سوالات

علی چراغی و مجتبی عبدالملکی

سوال ۱. تمام جواب‌های صحیح معادله دیوفانتی $x^۳+۲y^۳=۱$ را پیدا کنید. [۱]

راه حل ۱.۱ (مقدماتی). جواب‌های $x^۳+۱=۲y^۳$ را پیدا می‌کنیم. (جواب‌های معادله اصلی با $(x,y)\to(-x,y)$ داده می‌شوند). ابتدا فرض می‌کنیم $x\neq ۱$ و $y\neq ۰$. x باید فرد باشد و پس اعداد $x+۱$ و $x-۱$ زوج هستند و $u=\frac{x+۱}{۲}$ و $v=\frac{x-۱}{۲}$ اعداد صحیح نسبت به هم اول هستند. پس

$$(u+v)^۳+(u-v)^۳=۱+x^۳=۲y^۳\Leftrightarrow u(u^۲+۳v^۲)=y^۳$$

حال از آنجایی که $x\neq ۱$ و $y\neq ۰$، پس داریم $uvy\neq ۰$.

حالت اول. فرض می‌کنیم $(u,۳)=۱$. در این صورت داریم $(u,u^۲+۳v^۲)=۱$ پس $n,m\in\mathbb{Z}$ وجود دارند که

$$u=n^۳,\quad u^۲+۳v^۲=m^۳$$

پس $m^۳-n^۶=۳v^۲$ و پس

$$(m-n^۲)((m-n^۲)^۲+۳mn^۲)=۳v^۲$$

قرار دهید $t=m-n^۲$. پس از آنجایی که $(n,m)=۱$، پس $(t,n)=۱$ و از بالا داریم که

$$t(t^۲+۳tn^۲+۳n^۴)=۳v^۲$$

پس $t|۳$ و مثلا $t=۳t_۱$ و پس

$$t_۱(۹t_۱^۲+۹t_۱n^۲+۳n^۴)=v^۲$$

پس $v|۳$ و مثلا $v=۳v_۱$ و از آنجایی که $(n,۳)=۱$

$$(۹t_۱^۲+۹t_۱n^۲+۳n^۴,۹)=۳$$

پس از $۹|v^۲$، بدست می‌آوریم: $t_۱=۳t_۲$. پس از بالا

$$t_۲(۲۷t_۲^۲+۹t_۲n^۲+n^۴)=v_۱^۲$$

همچنین

$$(t_۲,۲۷t_۲^۲+۹t_۲n^۲+n^۴)=۱$$

پس $a,b\in\mathbb{Z}$ هستند که

$$۲۷a^۴+۹a^۲n^۲+n^۴=b^۲$$

همچنین از آنجا که فرض کرده‌ایم $x\neq ۱$ و $y\neq ۰$، داریم که b و $|n|$ اعداد طبیعی هستند. پس جواب‌هایی طبیعی از معادله دیوفانتی زیر را پیدا کرده‌ایم:

$$x^۴+۹x^۲y^۲+۲۷y^۴=z^۲ \qquad (۱)$$

(بعد از بررسی حالت دوم ثابت می‌کنیم این معادله جواب طبیعی ندارد)

حالت دوم. فرض کنید $u|۳$. از آنجایی که $(u,v)=۱$. پس $(v,۳)=۱$ و $u=۳u_۱$ پس از آنجایی که $u(u^۲+۳v^۲)=y^۳$ پس $y=۳y_۱$ و

$$u_۱(۳u_۱^۲+v^۲)=۳y_۱^۳$$

[۱] ما سه راه حل برای این مسئله ارائه می‌دهیم که یکی مقدماتی، دومی با استفاده از نظریه جبری اعداد و سومی با استفاده از هندسه حسابی است.

پس از $(v,3)=1$ نتیجه می‌گیریم که $3|u_1$. پس $u_1=3u_2$ و

$$u_2(27u_2^2+v^2)=y_1^3$$

اما $(u_2,v)=1$ و پس

$$(u_2,27u_2^2+v^2)=1$$

پس $a,b\in\mathbb{Z}$ نسبت به هم اول هستند که

$$u_2=a^3,\quad 27u_2^2+v^2=b^3$$

همچنین $(b,3)=1$. پس داریم

$$27a^6+v^2=b^3$$

قرار می‌دهیم $t=b-3a^2$. پس داریم $(t,3)=1$ و همچنین

$$t(t^2+9a^2t+27a^4)=v^2$$

ولی چون $(a,b)=1$، پس $(a,t)=1$ و از $(t,3)=1$ بدست می‌آوریم که

$$(t,t^2+9a^2t+27a^4)=1$$

پس $a_1,b_1\in\mathbb{Z}$ هستند که

$$t=a_1^2,\quad t^2+9a^2t+27a^4=b_1^2$$

و پس

$$a_1^4+9a^2a_1^2+27a^4=b_1^2$$

همچنین a_1 یا a نمی‌توانند صفر باشند به دلیل فرض $x\neq 1$ و $y\neq 0$. پس دوباره بدست می‌آوریم که $x^4+9x^2y^2+27y^4=z^2$ جواب طبیعی دارد.

قبل این که ثابت کنیم این معادله جواب طبیعی ندارد، واضح است که حالت $x=1$ یا $y=0$ جواب‌های $(-1,1)$ و $(1,0)$ از معادله اصلی را می‌دهند.

اثبات حل ناپذیری (۱) : فرض کنید (x,y,z) یک جواب طبیعی با کوچکترین z باشد. در این صورت به وضوح باید داشته باشیم $(x,y,z)=1$ همچنین با یک بررسی ساده، باید x فرد و y زوج باشد و $(x,3)=1$ و $(x,z)=1$. حال قرار دهید $y=2y_1$، پس معادله (۱) را به شکل زیر می‌توان نوشت:

$$27y_1^4=(\frac{z+x^2}{2}+9y_1^2)(\frac{z-x^2}{2}-9y_1^2)$$

حال فرض کنید d ب.م.م. دو عبارت سمت راست باشد. در این صورت:

$$d^2|27y_1^4\Rightarrow d|9y_1^2\Rightarrow d|(x^2,z)=1\Rightarrow d=1$$

و پس یا

$$\frac{z+x^2}{2}+9y_1^2=27a^4,\quad \frac{z-x^2}{2}-9y_1^2=b^4,\quad y_1=ab \qquad (2)$$

یا

$$\frac{z+x^2}{2}+9y_1^2=a^4,\quad \frac{z-x^2}{2}-9y_1^2=27b^4,\quad y_1=ab \qquad (3)$$

(۲) نتیجه می‌دهد

$$x^2+18a^2b^2=27a^4-b^4\Rightarrow 3|b^4+1$$

که غیرممکن است. حال (۳) نتیجه می‌دهد که

$$x^2+18a^2b^2=a^4-27b^4 \qquad (4)$$

که نتیجه می‌دهد a یا b زوج است. اگر a زوج باشد $a^4\overset{8}{\equiv}4$ که غیرممکن است. پس b زوج است و

$$27b^4=(\frac{a^2+x}{2}-\frac{9}{2}b^2)(\frac{a^2-x}{2}-\frac{9}{2}b^2)$$

مانند قبل می‌توان نتیجه گرفت که دو عبارت سمت راست نسبت به هم اول هستند. حال اگر علامت هر دو عبارت سمت راست منفی باشد، داریم $a^2<9b^2$ که تناقض با (۴) است. پس هر دو مثبت هستند و $m,n\in\mathbb{Z}$ وجود دارند که:

$$\frac{a^2\pm x}{2}-\frac{9}{2}b^2=m^4,\quad \frac{a^2\mp x}{2}-\frac{9}{2}b^2=27n^4,\quad b=mn$$

پس

$$a^2=m^4+9m^2n^2+27n^4$$

که

$$a \leq y_1 < y < z$$

که با فرض مینیمم بودن z در تناقض است. پس معادله‌ی (۱) جواب طبیعی ندارد.

راه حل ۲.۱ (نظریه جبری اعداد). داریم $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(x+\sqrt[3]{2}y) = x^3+2y^3 = 1$. پس $x+\sqrt[3]{2}y$ باید در $\mathbb{Q}(\sqrt[3]{2})$ یکه[۲] باشد. حال از آنجایی که $\mathbb{Q}(\sqrt[3]{2})$، دو نشاندن[۳] مختلط دارد و یک نشاندن حقیقی دارد، پس طبق قضیه یکه دیریکله[۴]، رتبه[۵] گروه یکه‌ها ۱ است. پس

$$U(\mathbb{Q}(\sqrt[3]{2})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

(چون تنها ریشه‌های واحد موجود در آن ± 1 هستند) . همچنین می‌توان به سادگی دید که $\sqrt[3]{2}-1$ یک یکه اساسی[۶] است و پس هر یکه‌ای به شکل $\pm(\sqrt[3]{2}-1)^n$ است. پس باید داشته باشیم $\pm(\sqrt[3]{2}-1)^n = x+y\sqrt[3]{2}$، ولی به سادگی می‌توان چک کرد که اگر

$$\pm(\sqrt[3]{2}-1)^n = a_n + b_n\sqrt[3]{2} + c_n\sqrt[3]{4}$$

آنگاه $c_n \neq 0$ برای n صحیح به جز ۰،۱ و پس تنها جواب‌ها در بین $\pm(\sqrt[3]{2}-1)$ و ± 1 هستند که با چک کردن نُرم این‌ها، تنها دو جواب $(-1,1)$ و $(1,0)$ را بدست می‌آوریم.

راه حل ۳.۱ (هندسه حسابی [۷]). با یک تغییر متغیر تعریف شده روی اعداد گویا، می‌توان این معادله را به خم بیضوی

$$E : y^2 = x^3 - 27$$

تبدیل کرد و سپس می‌توان با نرم افزار *PARI/GP* (یا روش‌های الگوریتمی دیگر) بدست آورد که $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. پس E تنها دو جواب گویا دارد که به همان دو جواب صحیح $(1,0)$ و $(-1,1)$ از معادله اصلی تناظر داده می‌شوند.

سوال ۲. فرض کنید G یک گروه حل پذیر متناهی از مرتبه n باشد. ثابت کنید تابع دوسویی (نه لزوما هوموفیسم) $f : G \to C_n$ وجود دارد به طوری که $o(g)|o(f(g))$ (C_n گروه دوری مرتبه n و $o(g)$ مرتبه‌ی عنصر g است.)

حدس ۱.۲. این خاصیت برای همه گروه‌های متناهی G درست است.

راه حل ۱.۲. اولا یک گروه ساده‌ی حل پذیر لزوما باید آبلی باشد (چون $G' = \{1\}$) و پس باید $\mathbb{Z}/p\mathbb{Z}$ باشد برای p اولی و سوال برای آن واضح می‌شود. حال استقرا روی مرتبه‌ی G می‌زنیم. برای $n = 1$ واضح است. حال فرض کنید برای گروه‌های حل پذیر از مرتبه‌ی کمتر از n درست باشد. از بالا می‌توانیم فرض کنیم گروه G ساده نیست و N زیرگروه نرمال مینیمال نابدیهی ای از آن باشد. در این صورت می‌دانیم که این زیرگروه نرمال به شکل $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$ است برای p اولی (مثلا قضیه ۳،۳،۱۵ از کتاب رابینسون[۸])

G/N حل پذیر و متناهی با مرتبه‌ی کم‌تر از n است پس می‌توان تابع $\sigma : G/N \to C_{|G/N|}$ را پیدا کرد به طوری که $o(\bar{g})|o(\sigma(\bar{g}))$. با استفاده از σ می‌خواهیم تابع دوسویی موردنظر را بسازیم. داریم $C_{|G/N|} \cong \frac{C_{|G|}}{C_{|N|}}$ پس می‌توان تابع σ را بشکل $\sigma : G/N \to \frac{C_{|G|}}{C_{|N|}}$ در نظر گرفت.

حال فرض کنید $g \in G$ عنصری دلخواه باشد بطوری که $\sigma(\bar{g}) = \bar{c} \in \frac{C_{|G|}}{C_{|N|}}$. می‌خواهیم تابعی دوسویی $f_{gN} : gN \to cC_{|N|}$ را تعریف کنیم. ابتدا مرتبه‌ی اعضای دو زیرمجموعه‌ی gN و $cC_{|N|}$ را بررسی می‌کنیم.

از آنجا که مرتبه‌ی هر عضو N ، ۱ یا p است، پس برای هر $n \in N$ ، $o(\bar{g})|o(gn)|po(\bar{g})$ و پس یا $o(gn) = o(\bar{g})$ یا $o(gn) = po(\bar{g})$

[۲] unit
[۳] embedding
[۴] Dirichlet's unit theorem
[۵] rank
[۶] fundamental unit
[۷] Arithmetic Geometry
[۸] Robinson, D. J. S., A Course in the Theory of Groups

برای $cC_{|N|}$ دو حالت داریم:

حالت اول. $p|o(\bar{c})$ که در این صورت به سادگی مشاهده می‌شود که مرتبه‌ی هر عنصر $cC_{|N|}$ باید $o(\bar{c})|N|$ باشد.

در واقع اگر $C_{|N|} = \langle x \rangle$ و مرتبه‌ی عنصری از $cC_{|N|}$ مثل cx^k ، $o(\bar{c})|N|$ نباشد، باید برای $k' \in \mathbb{Z}$ ی داشته باشیم: در این‌جا

$$\begin{aligned} &(cx^k)^{o(\bar{c})} = x^{pk'} \\ &\Rightarrow ((cx^k)^{\frac{o(\bar{c})}{p}} x^{-k'})^p = 1 \\ &\Rightarrow (cx^k)^{\frac{o(\bar{c})}{p}} x^{-k'} \in N \\ &\Rightarrow (c)^{\frac{o(\bar{c})}{p}} \in N \end{aligned}$$

که متناقض با تعریف $o(\bar{c})$ است. پس در این حالت می‌توان هر عنصر $gn \in gN$ را به هر عنصر دلخواهی از $cC_{|N|}$ تصویر کرد و داریم

$$o(gn)|o(f_{gN}(gn))$$

حالت دوم. $p \nmid o(\bar{c})$ که در این صورت مرتبه‌ی هر عنصر $cC_{|N|}$ به شکل $o(\bar{c})p^r$ است که $p^r \mid |N|$ و مرتبه‌ی دقیقا یک عنصر از $cC_{|N|}$ ، $o(\bar{c})$ است. در واقع برای هر $a \in cC_{|N|}$ $a^{o(\bar{c})} \in C_{|N|}$ و همگی این‌ها به عناصر متفاوتی از $C_{|N|}$ نگاشته می‌شوند، چون اگر $a \neq b$ عناصری از $cC_{|N|}$ باشند و $a^{o(\bar{c})} = b^{o(\bar{c})}$ ، آنگاه $(ab^{-1})^{o(\bar{c})} = 1$ ولی $ab^{-1} \in C_{|N|}$ پس باید $p|o(ab^{-1})|o(\bar{c})$ که متناقض با فرض است. پس $a^{o(\bar{c})}$ به عناصر متفاوتی نگاشته شده و پس دقیقا یک عنصر از مرتبه‌ی $o(\bar{c})$ در $cC_{|N|}$ وجود دارد. در این حالت داریم $o(\bar{g})|o(\bar{c})$ و پس $p \nmid o(\bar{g})$. حال ثابت می‌کنیم عنصر $gn \in gN$ وجود دارد به طوری که $p \nmid o(gn)$. در واقع اگر $p \nmid o(g)$ که کار تمام است، در غیر این صورت $g^{o(\bar{g})} = n \in N$ و چون $|N| = p^k$ برای k ای، پس عضو $n' \in N$ وجود دارد که $(n')^{o(\bar{g})} = n$ پس:

$$g^{o(\bar{g})} = (n')^{o(\bar{g})} \Rightarrow (g(n')^{-1})^{o(\bar{g})} = 1$$

و پس عنصر $g(n')^{-1}$ خاصیت مورد نظر را دارد.

$$(p \nmid o(g(n')^{-1}) = o(\bar{g}))$$

در این صورت $g(n')^{-1}$ را به عضو یکتای $cC_{|N|}$ از مرتبه‌ی $o(\bar{c})$ تصویر می‌کنیم و بقیه را به شکل دلخواه (به طوری که f_{gN} دوسویی شود) به $cC_{|N|}$ تصویر می‌کنیم.

در این صورت تابع $f : G \to C_{|G|}$ را به صورتی تعریف می‌کنیم که $f|_{gN} = f_{gN}$ (برای g های در یک مجموعه از نماینده‌های G/N) پس کار تمام است.

سوال ۳. فرض کنید G گروهی آبلی باشد. ثابت کنید توسیع گالوای $K/\mathbb{Q}$ وجود دارد به طوری که $G \cong \mathrm{Gal}(K/\mathbb{Q})$

حدس ۱.۳. (مسئله وارون گالوا[9]) این خاصیت برای هر گروه متناهی G درست است.

این حدس توسط شفروویچ[10] برای گروه‌های حل پذیر متناهی ثابت شده است.

راه حل ۱.۳. فرض کنید ζ_n یک ریشه‌ی nام واحد اولیه باشد. اولا $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ در واقع اگر $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ آنگاه σ باید ζ_n را به یک ریشه‌ی nام واحد ببرد زیرا

$$\sigma(\zeta_n)^n = \sigma(\zeta_n^n) = \sigma(1) = 1$$

پس مثلا $\sigma : \zeta_n \mapsto \zeta_n^i$ که $gcd(i,n) = 1$ (چون باید وارون پذیر باشد) . اگر عمل σ روی ζ_n معلوم باشد آنگاه روی $\mathbb{Q}(\zeta_n)$ مشخص می‌شود. پس همه‌ی اتومورفیسم‌ها به شکل بالا هستند که پس ایزومورفیسم بالا بدست می‌آید.

حال طبق قضیه اساسی نظریه گروه‌های آبلی متناهی تولید:

$$G \cong C_{n_1} \times C_{n_2} \cdots \times C_{n_k}$$

که C_n گروه دوری مرتبه n است و $n_1|n_2|\cdots|n_k$.

حال طبق قضیه دیریکله برای تصاعدهای حسابی، اعداد اول $p_i (1 \leq i \leq k)$ وجود دارند که $p_i \overset{n_i}{\equiv} 1$. حال قرار دهید $n = p_1 p_2 \cdots p_k$

[9] Inverse Galois Problem

[10] I. Shafarevich

در این صورت

$$\begin{aligned} &Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ &\cong (\mathbb{Z}/n\mathbb{Z})^* \\ &\cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \mathbb{Z}/(p_2-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_k-1)\mathbb{Z} \end{aligned}$$

پس از آنجا که $n_i | p_i - 1$ ، پس یک زیرگروه H_i از $\mathbb{Z}/(p_i-1)\mathbb{Z}$ وجود دارد که:

$$\frac{\mathbb{Z}/(p_i-1)\mathbb{Z}}{H_i} \cong \mathbb{Z}/n_i\mathbb{Z}$$

پس

$$\frac{(\mathbb{Z}/n\mathbb{Z})^*}{H_1 \times H_2 \times \cdots \times H_k} \cong G$$

همچنین شناخته شده است که $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ گالوا است (می‌توانید به سادگی این موضوع را چک کنید) پس از آنجایی که $H_1 \times H_2 \times \cdots \times H_k$ در $(\mathbb{Z}/n\mathbb{Z})^*$ نرمال است، توسیع گالوای $K/\mathbb{Q}$ وجود دارد که $Gal(K/\mathbb{Q}) \cong G$.

سوال ۴. گراف K_n که روی هر رأس آن یک عدد حقیقی و روی هر یال آن یک لیست سه تایی از اعداد حقیقی مختلف قرار داده شده، به ما داده شده است(لیست قرار داده شده بر روی یال‌های مختلف می‌تواند یکسان یا متفاوت باشد). ثابت کنید که می‌توان از لیست هر کدام از یال‌ها یک عدد را انتخاب کرد که در نهایت رنگ هر دو رأس مجاور فرق کند. اگر w_v عدد روی رأس v و l_{uv} عدد انتخاب شده برای یال uv باشد آنگاه رنگ رأس v برابر است با:

$$\text{color}(v) = W_v + \sum_{u \in N(v)} l_{uv}$$

راه حل ۱.۴. با استقرا روی تعداد رئوس از n به $n+2$ حکم را ثابت می‌کنیم:

برای $n = 1, n = 4$ حکم را خودتان ثابت کنید ؛)

فرض کنید حکم برای n برقرار است حکم را برای $n+2$ ثابت می‌کنیم:

هر حالت انتخاب اعداد روی رئوس را یک رنگ آمیزی می‌نامیم و در هر رنگ آمیزی به ازای هر دوتایی مرتب از رئوس مانند u و v مقدار $f(u,v)$ را برابر با $\text{color}(u) - \text{color}(v)$ تعریف می‌کنیم،حال به ازای تمام رنگ آمیزی‌های ممکن مقدار ماکسیمم برای $f(u,v)$ را در نظر بگیرید و یکی از رنگ آمیزی‌های متناظر با این مقدار ماکسیمم و دو رأس متناظر u و v را در نظر بگیرید(بدیهی است در این حالت از تمام یال‌های متصل به u به جز یال uv مقدار ماکیسممشان از لیست سه تایی و از تمام یال‌های متصل به v به جز uv مقدار مینیممشان از لیست سه تایی روی این یال‌ها انتخاب شده‌اند، در ضمن مقدار انتخاب شده از روی یال uv بر مقدار $f(u,v)$ تاثیری ندارد.)

حال دو رأس u, v را در نظر گرفته و از تمام یال‌های متصل به u به جز یال uv مقدار ماکیسممشان از لیست سه تایی و از تمام یال‌های متصل به v به جز uv مقدار مینیممشان از لیست سه تایی روی این یال‌ها انتخاب می‌کنیم و از یال uv مقدار وسطی از سه مقدار حقیقی روی uv را انتخاب می‌کنیم، اگر به ازای هر رأس به جز u و v مانند S اعداد روی یال‌های متصل بین u و v و s را به برچسب روی s اضافه کنیم، با توجه به فرض استقرا داریم حکم برای $n-2$ رأس دیگر به جز u, v با اعداد جدید روی برچسب هایشان برقرار است بنابراین یک انتخاب برای اعداد روی یال هایشان داریم به طوری که رنگ تمام رئوس به جز u و v با هم متمایز شوند و کافی است در این حالت کافی است ثابت کنیم رنگ u و v از سایر رئوس متمایز است .(بدیهی است رنگ u و v به ازای $n > 0$ از هم متمایزند.)

بنا بر تقارن فرض کنید رنگ یک رأس مانند t با عدد u یکی باشد داریم در این رنگ آمیزی $f(s,v) = f(u,v)$ از طرفی اگر در همین رنگ آمیزی از برچسب روی uv عدد مینیمم را انتخاب کنیم آنگاه $f(s,v) > f(u,v)$ که متناقض با فرض بیشینه بودن $f(u,v)$ است به طرز مشابه در این رنگ آمیزی رنگ هیچ رأسی با رنگ v هم یکی نیست.

سوال ۵. گراف دو بخشی $G = (X, Y)$ که روی هر رأس آن یک لیست دو تایی از اعداد طبیعی متمایز و روی هر یال آن مجموعه‌ی $\{1, 2\}$ قرار داده شده، به ما داده شده است. ثابت کنید که می‌توان از لیست هر کدام از یال‌ها یک عدد و از لیست هر کدام از رأس‌ها نیز یک عدد را انتخاب کرد که در نهایت رنگ هر دو رأس مجاور فرق کند. اگر W_v عدد انتخاب شده برای رأس v و l_{uv} عدد انتخاب

شده برای یال uv باشد آنگاه رنگ رأس v برابر است با:

$$\text{color}(v) = W_v + \sum_{u \in N(v)} l_{uv}$$

راه حل ۱.۵. حکم را برای یک گراف همبند ثابت می‌کنیم:
مجموع اعداد انتخاب شده روی هر رأس و یال‌های مجاور آن را عدد متناظر با آن رأس در نظر بگیرید. در ادامه ابتدا الگوریتمی را برای به دست آوردن ترتیبی از انتخاب اعداد لیست ها ارائه می‌دهیم،سپس ثابت می‌کنیم با انجام الگوریتم حکم مسئله اثبات می‌شود و در انتها ثابت می‌کنیم تعداد مراحل الگوریتم متناهی است .
در ابتدا از هر یک از برچسب‌ها بزرگترین را انتخاب می‌کنیم، یکی از رئوسی را که عدد متناظر با آن در بین عدد متناظر با سایر رئوس بیشینه است را در نظر بگیرید و فرض کنید در بخش اول گراف دو بخشی قرار دارد، همچنین M را برابر با عدد متناظر با آن قرار دهید.
حال در مرحله i ام ($i \leq M$) اعمال زیر را انجام می‌دهیم:
اگر $i \overset{۲}{\equiv} m, ۱ \leq m \leq ۲$ باشد تمامی رئوسی از گراف را که در بخش m ام قرار دارند و عدد متناظر آن‌ها در این مرحله (پس از اعمال تغییرات مرحله قبل در صورت وجود) برابر با $M - i + ۱$ است را در مجموعه A_i و همچنین تمام رئوسی از بخش دیگر را که بین آن‌ها و مجموعه A_i حداقل یک یال وجود دارد و نیز عدد متناظر آن‌ها برابر با $M - i + ۱$ است را در بخش B_i قرار می‌دهیم. سپس تمامی رئوسی را که عضو مجموعه B_i هستند و نیز حداقل یک یال به رأسی با عدد متناظر کمتر از $M - i + ۱$ در این مرحله دارند را در مجموعه C_i و سایر رئوس B_i را در D_i قرار می‌دهیم و اعضای مجموعه D_i را نقره‌ای می‌کنیم.
سپس اعداد انتخاب شده از لیست روی تمام رئوس D_i را به مقدار مینیمم از دو عدد لیستش تغییر می‌دهیم، همچنین از هر یک از رئوس مجموعه C_i یک یال که به رأسی با عدد متناظر کمتر از عدد متناظر این رأس متصل است را انتخاب کرده و عدد روی آن یال را از یک به صفر تغییر می‌دهیم (به ازای هر i امکان دارد تعدادی از مجموعه‌های A_i, B_i, C_i, D_i تهی باشند که اشکالی در الگوریتم به وجود نمی‌آورند).
حال ثابت می‌کنیم پس از انجام الگوریتم فوق عدد متناظر هر رأس با عدد متناظر تمامی رئوس مجاورش متفاوت است.
با توجه به همبندی گراف با اندکی تأمل می‌توان دریافت که هر رأس U یا به ازای یک i در مجموعه A_i آمده‌است یا به ازای یک i در مجموعه D_i قرار گرفته است حال برای هر دو حالت حکم را ثابت می‌کنیم:
۱ــ رأس U به ازای یک i در مجموعه D_i قرار گرفته باشد: تمامی یال‌های خارج شده از رأس U به رئوس با عدد متناظر بزرگتر متصل هستند زیرا در مرحله iام رأس U یالی به رأسی با عدد کمتر از $M - i + ۱$ ندارد و از طرفی بعد از انجام عمل این مرحله عدد روی این رأس از $M - i + ۱$ کمتر خواهد شد.
۲ــ رأس U به ازای یک i در مجموعه A_i قرار گرفته باشد: پس از مرحله iام عدد متناظر رأس U تغییر نمی‌کند و همان $M - i + ۱$ خواهد ماند از طرفی تمام مجاورهای رأس U یا یک رأس نقره‌ای هستند که بنا بر ۱ نمی‌توانند با عدد متناظرشان با عدد متناظر رأس U برابر شود یا عضو یک A_j هستند که j باید زوجیتش با i متفاوت باشد و عدد متناظرشان برابر است با $M - i + ۱$ که این هم با عدد متناظر رأس U متفاوت است.
در ضمن از آنجا که M عددی متناهی است تعداد مراحل متناهی است.
اگر گراف ناهمبند بود ما حکم را برای هر مولفه همبندی ثابت کرده‌ایم و بنابراین برای گراف کلی نیز حکم را ثابت کرده این زیرا دو مولفه همبندی مجزا رأس مجاور ندارند.

سوال ۶. فرض کنید که $A \in M_n(\mathbb{C})$ و داشته باشیم: $Tr(A) = ۰$ آیا می‌توان نتیجه گرفت که A پوچ توان است؟ $Tr(A^۲) = \cdots = Tr(A^n) = ۰$

راه حل ۱.۶. اگر ویژه مقدارهای ماتریس A را با $\lambda_۱, \lambda_۲, \ldots, \lambda_n$ نمایش دهیم، آنگاه ویژه مقادیر ماتریس A^k برابر $\lambda_۱^k, \lambda_۲^k, \ldots, \lambda_n^k$ است. بنابراین از فرض مسئله می‌توان نتیجه گرفت که:

$$\lambda_۱^k + \lambda_۲^k + \cdots + \lambda_n^k = ۰$$

حال با استفاده از اتحادهای نیوتن هر تابع متقارن بر حسب $\lambda_۱, \lambda_۲, \ldots, \lambda_n$ را می‌توانیم بر حسب $\lambda_۱^i + \lambda_۲^i + \cdots + \lambda_n^i$ برای $i =$

$۱, ۲, \ldots, n$ بنویسیم، بنابراین تمام ضرایب چند جمله‌ای مشخصه ماتریس A (به جز ضریب جمله با بزرگترین درجه) باید صفر باشند، بنابراین A پوچ توان است.

سوال ۷. فرض کنید $(A_i, B_i), ۱ \leq i \leq h$ یک خانواده از زوج مرتب‌ها از مجموعه‌هایی از اعداد صحیح باشند به طوری که $\forall i, |A_i| = k, |B_i| = l, A_i \cap B_i = \emptyset$ و $(A_i \cap B_j) \cup (A_j \cap B_i) \neq \emptyset$ آنگاه ثابت کنید:

$$h \leq \frac{(k+l)^{k+l}}{k^k l^l}$$

راه حل ۱.۷. مجموعه M را به صورت مقابل تعریف می‌کنیم:

$$M = \{\forall x | \exists i, x \in A_i \vee x \in B_i\}$$

حال هر یک از اعضای M را به احتمال $\frac{k}{k+l}$ آبی و به احتمال $\frac{l}{k+l}$ قرمز می کنیم.

K_i را برابر با این پیشامد تعریف می کنیم که تمام اعضای A_i آبی و تمام اعضای B_i به رنگ قرمز باشند.

$$P(K_i \cap K_j) = ۰$$

زیرا اگر قرار باشد $A_i \cap B_j \neq \emptyset$ آنگاه A_i و B_j باید یک عضو مشترک و همرنگ داشته باشند و اگر $B_i \cap A_j \neq \emptyset$ آنگاه A_j و B_i باید یک عضو مشترک و همرنگ داشته باشند.

$$P(K_i) = \left(\frac{k}{k+l}\right)^k \times \left(\frac{l}{k+l}\right)^l$$

$$p(\cup k_i) \leq ۱$$

$$P(K_i \cap K_j) = ۰ \Rightarrow P(\cup K_i) = \cup P(K_i)$$

$$\cup P(K_i) = h \times P(K_۱) = h \times \left(\left(\frac{k}{k+l}\right)^k \times \left(\frac{l}{k+l}\right)^l\right)$$

$$= p(\cup k_i) \leq ۱ \Rightarrow h \leq \frac{(k+l)^{k+l}}{k^k \times l^l}$$

سوال ۸. فرض کنید F یک مجموعه متناهی از رشته‌های دودویی با طول متناهی باشد به طوری که هیچ رشته‌ای از این مجموعه پیشوند رشته‌ی دیگری در دنباله نیست، حال N_i را تعداد رشته‌های با طول i در این دنباله در نظر بگیرید، ثابت کنید:

$$\sum_i \frac{N_i}{۲^i} \leq ۱$$

راه حل ۱.۸. فرض کنید $a_۱, a_۲, \ldots, a_m$ رشته‌های ما باشند و $L(a_i)$ را برابر با طول رشته a_i تعریف می‌کنیم می‌دانیم یک m به اندازه کافی بزرگ وجود دارد که از طول تمام رشته‌ها بزرگ‌تر باشد حال از تمام رشته‌های به طول m یکی را با احتمال برابر انتخاب می‌کنیم.

$P(A_i)$ را برابر با احتمال این پیشامد تعریف می‌کنیم که یک دنباله دودویی با رشته a_i شروع شود.

$$P(a_i) = \frac{۱}{۲^{L(a_i)}}$$

از طرفی داریم: $P(a_i \cap a_j) = ۰$ زیرا اگر دنباله‌ای با a_i شروع شود دیگر نمی‌تواند با a_j شروع شود.

حال داریم:

$$P(\cup a_i) \leq ۱$$

$$P(a_i \cap a_j) = \emptyset \Rightarrow P(\cup_i a_i) = \sim_i P(a_i) = \sum_i \frac{۱}{۲^{L(a_i)}}$$

$$= \sum_i \frac{N_i}{۲^i} \Rightarrow \sum \frac{N_i}{۲^i} \leq ۱$$

سوال ۹. فرض کنید F یک مجموعه متناهی از رشته‌های دودویی با طول متناهی باشد به طوری که هیچ رشته‌ای را نمی‌توان به دو صورت متفاوت با اعضای F به زیر رشته‌ها افراز کرد، حال N_i را تعداد رشته‌های با طول i در این دنباله در نظر بگیرید، ثابت کنید:

$$\sum_i \frac{N_i}{۲^i} \leq ۱$$

راه حل ۱.۹. X را مجموعه تمام a_i ها در نظر می‌گیریم داریم:

$$\left(\sum_X \frac{۱}{۲^{L(a_i)}}\right)^k = \left(\sum_X \frac{۱}{۲^{L(a_i)}}\right)\left(\sum_X \frac{۱}{۲^{L(a_i)}}\right)\cdots\left(\sum_X \frac{۱}{۲^{L(a_i)}}\right)$$

حال x^k را مجموعه تمام رشته‌هایی که از کنار هم گذاشتن k کلمه پشت سر هم تشکیل می‌شود در نظر بگیرید, مجموع فوق را می‌توان به این صورت هم نوشت:

$$\sum_{X^k} \frac{۱}{۲^{L(b_i)}}$$

که b_i ها همه کلماتی است که از به هم پیوستن k تا a_i به دست می آید

از طرفی از آنجا که هر رشته به طور یکتا قابل تجزیه است داریم مجموع فوق کمتر مساوی

$$\sum_{X^k} \frac{۱}{۲^{L(b_i)}} \leq \sum_L n_L \frac{۱}{۲^L}$$

است که در آن n_L برابر تمام رشته‌های k کلمه‌ای به طول L است و همچنین داریم :

$$n_L \leq ۲^L, L \leq K \times L_{max}$$

بنابراین داریم

$$\sum_{X^k} \frac{۱}{۲^{L(b_i)}} \leq \sum_{K\times L_{max}} \left(۲^L \times \frac{۱}{۲^L}\right) = K \times L_{max}$$

بنابراین:

$$\left(\sum \frac{۱}{۲^{L(a_i)}}\right)^k \leq K \times L_{max}$$

وبه همین ترتیب داریم:

$$\sum \frac{۱}{۲^{L(a_i)}} \leq (K \times L_{max})^{۱/k}$$

که با میل دادن k به بینهایت سمت راست عبارت به وضوح به ۱ میل می‌کند و حکم ثابت شد.

سوال ۱۰. ثابت کنید برای هر مجموعه X متشکل از $۴k^۲$ عدد متمایز به پیمانه یک عدد اول p، یک عدد a موجود است به طوری که مجموعه $\{ax(modp), x \in X\}$ با هر بازه به طول حداقل $\frac{p}{K}$ اشتراک ناتهی دارد.

راه حل ۱۰.۱۰. ابتدا مجموعه‌های A_i را به صورت زیر تعریف می‌کنیم:

$$A_i = \left\{\frac{(i-۱)p}{۲k} + ۱, \ldots, \frac{ip}{۲k}\right\}$$

بدیهی است که اگر a, b وجود داشته باشند به طوری که مجموعه: $aX + b = \{ax + b; x \in X\}$ هر یک از A_iها را حکم اشتراک ناتهی دارد سوال ثابت شده است. حال a, b را به صورت تصادفی و با احتمال برابر از مجموعه $\{۰, ۱, \ldots, p-۱\}$ انتخاب می‌کنیم. و متغیر تصادفی Y_i را به صورت زیر تعریف می‌کنیم:

$$Y_i = |\{aX + b\} \cap A_i|$$

همچنین متغییر تصادفی $Y(i,j)$ را به ازای $۱ \leq j \leq \frac{p}{۲k}$ به این صورت است که اگر $\frac{i-۱}{۲k} + j \in aX + b$ آنگاه $Y(i,j) = ۱$ در غیر صورت $Y(i,j) = ۰$ آنگاه داریم:

$$E[Y_{(i,j)}] = \frac{۴k^۲}{p}, VAR[Y_{(i,j)}] \leq E[Y_{(i,j)}] = \frac{۴k^۲}{p}$$

همچنین: $Y_i = \sum_{j=۱}^{\frac{p}{۲k}} Y_{(i,j)}$ به همین ترتیب:

$$E[Y_i] = \sum_{j=۱}^{\frac{p}{۲k}} E[Y_{(i,j)}],$$

$$VAR[Y_i] \leq \sum_{j=۱}^{\frac{p}{۲k}} VAR[Y_{(i,j)}] + \sum COV[Y_{(i,j)}Y_{(i,l)}]$$

$$COV[Y_{(i,j)}Y_{(i,l)}] = E[Y_{(i,j)}Y_{(i,l)}] - E[Y_{(i,j)}]E[Y_{(i,l)}] = E[Y_{(i,j)}Y_{(i,l)}] - \frac{(۴k)^۲}{p^۲}$$

برای محاسبه $E[Y_{(i,j)}Y_{(i,l)}]$ تعداد حالاتی که هر دو $Y_{(i,j)}, Y_{(i,l)}$ مخالف صفر هستند را بر کل حالات a, b تقسیم می‌کنیم از طرفی برای هر m, n متمایز داریم تعداد جواب‌های $aX_m + b = \left(\frac{(i-۱)p}{۲k} + j\right)$ و $aX_n + b = \left(\frac{(i-۱)p}{۲k} + l\right)$ دقیقا یکی است

بنابراین:

$$E\big[Y_{(i,j)}Y_{(i,l)}\big] \le \frac{\binom{۴k^۲}{۲}}{p^۲} < \left(\frac{۴K^۲}{P}\right)^۲$$

$$\Rightarrow COV\big[Y_{(i,j)}Y_{(i,l)}\big] < ۰$$

$$\Rightarrow VAR[Y_i] < \sum_{j=۱}^{\frac{p}{۲k}} VAR\big[Y_{(i,j)}\big] \ < \sum_{j=۱}^{\frac{p}{۲k}} E\big[Y_{(i,j)}\big]$$

بنابراین

$$E[Y_i] = ۲k, VAR[Y_i] < ۲k$$

بنابراین طبق نامساوی چبیشف داریم:

$$P(Y_i = ۰) < p\Big(|Y_i - ۲k| \ge ; \sqrt{۲k} \times \sqrt{۲k}\Big) \le \frac{۱}{۲k}$$

از طرفی داریم:

$$p(\cup(Y_i = ۰)) \le \cup P(Y_i = ۰) < (۲k) \times \frac{۱}{۲k} = ۱$$

بنابراین حالتی وجود دارد که هیچ یک از Y_jها صفر نشوند.