راهنمایی مجموعه تمارین نظریه اعداد جلسه پنجم دوره تابستانی ۱۴۰۱

مبحث مرتبه و قضایای مربوطه

۱. فرض کنید p_i عامل اول دلخواهی از n_i باشد. طبق فرض مسئله $p_i \mid 2^{n_{i+1}}-1 \implies \mathrm{Ord}_{p_i}(2) \mid n_{i+1}$. حال کافیست با یک رویکرد اکسترمالی روی کوچکترین عامل اول بین تمام مقادیر n_i به تناقض برسید و نتیجه بگیرید هیچ یک از n_i ها نمی‌تواند عامل اولی داشته باشد.

۲. ابتدا در جهت ساده‌سازی حکم، سعی می‌کنیم رابطه خواسته شده را به دو رابطه عاد کردن بر p, q تبدیل کنیم. در این جهت با استفاده از قضیه فرما نتیجه بگیرید $p = 3 \iff p \mid 5^p - 2^p$. حالتی که در آن p و یا q برابر با ۳ هستند را حل کنید. در حالت دیگر، باید داشته باشیم : $q \mid 5^p - 2^p \quad , \quad p \mid 5^q - 2^q$.
حال فرض کنید p^*, q^* وارون‌های ضربی ۲ به پیمانه p, q باشند. می‌توان نوشت : $p \mid 5^q(q^*)^q - 2^q(q^*)^q \overset{p}{\equiv} 5^q(q^*)^q - 1 = (5q^*)^q - 1$ و به طور کاملا مشابه $q \mid (5p^*)^p - 1$. حال با استفاده از اطلاعات بدست‌آمده درباره $\mathrm{Ord}_q(5p^*), \mathrm{Ord}_p(5q^*)$ به تناقض رسیده و اثبات را کامل کنید.

۳. با بررسی‌های مقدماتی آغاز به حل مسئله می‌کنیم. از فرض مسئله داریم :

$$p^\alpha \mid a^{2n}-1, p^\alpha \mid a^{2m}-1 \implies \mathrm{Ord}_{p^\alpha}(a) \mid 2m, \mathrm{Ord}_{p^\alpha}(a) \mid 2n \implies \mathrm{Ord}_{p^\alpha}(a) \mid 2\gcd(m,n) \implies p^\alpha \mid a^{2\gcd(m,n)}-1$$

از این نتیجه بگیرید که مگر در حالت $p = 2, \alpha = 1$، در باقی حالات می‌توان نتیجه گرفت $p^\alpha \mid a^{\gcd(m,n)} - 1$. از اینجا حدس می‌زنیم که پاسخ مسئله $a^{\gcd(m,n)} - 1$ باشد. دقت کنید که تا الان ثابت کرده‌ایم برای هر $p \in \mathbb{P}$ (به جز یک حالت خاص که به صورت جداگانه بررسی می‌شود) می توان نتیجه گرفت : $\nu_p(a^{\gcd(m,n)} - 1) \geq \nu_p\left(\gcd\left(a^m - 1, a^n - 1\right)\right)$. حال به طور مشابه ثابت کنید $\nu_p(a^{\gcd(m,n)} - 1) \leq \nu_p\left(\gcd\left(a^m - 1, a^n - 1\right)\right)$ و با استفاده از این دو نتیجه، اثبات حکم را کامل کنید. به عنوان تمرین سعی کنید این تمرین را با کمک الگوریتم اقلیدس ثابت کنید. همچنین سعی کنید این حکم را تعمیم دهید.

۴. حکم را به استقرا اثبات کنید. فرض کنید $m_0 \in \mathbb{N}$ موجود باشد که $2^n \mid 5^{m_0}+3$ اما $2^{n+1} \nmid 5^{m_0}+3$. در نتیجه داریم : $5^{m_0}+3 \overset{2^{n+1}}{\equiv} 2^n$. با جاگذاری این نتیجه در معادله داریم : $5^m+3 \overset{2^{n+1}}{\equiv} 2^n - 5^{m_0} + 5^m$. در نهایت کافیست مقدار $m \in \mathbb{N}$ را بیابید به طوری که $2^{n+1} \mid 5^m + 3$. $5^{m-m_0} - 1 \overset{2^{n+1}}{\equiv} 5^m - 5^{m_0} \overset{2^{n+1}}{\equiv} 2^n$.

۵. فرض کنید $p \in \mathbb{P}$ دارای این خاصیت باشد که $p \mid 2^{2^n} + 1$. با استفاده از خواص $\mathrm{Ord}_p(2)$ نتیجه بگیرید $p \geq 2^{n+1} + 1$. $p \overset{2^{n+1}}{\equiv} -1 \implies$. حال اگر p عاملی از $P(n)$ نیز باشد، باید داشته باشیم : $P(n) \geq p \geq 2^{n+1} + 1$. از این نامساوی به تناقض رسیده و اثبات را کامل کنید.

۶. از خواص مرتبه می‌دانیم چون $m \mid n$، آنگاه $\mathrm{Ord}_n(a) \mid \mathrm{Ord}_m(a)$. پس در واقع حکم مسئله معادل با این است که $\frac{\mathrm{Ord}_m(a)}{\mathrm{Ord}_n(a)} = \frac{m}{\gcd(m, a^{\mathrm{Ord}_n(a)}-1)}$. ابتدا به عنوان صورتی ضعیف‌تر از مسئله (اثبات صورت ضعیف‌تر مسئله و سپس استفاده از آن به عنوان ابزار کمکی را به عنوان یک ابزار کاربردی در ریاضیات به یاد داشته باشید) ثابت می کنیم : $\frac{\mathrm{Ord}_m(a)}{\mathrm{Ord}_n(a)} \mid \frac{m}{\gcd(m, a^{\mathrm{Ord}_n(a)}-1)}$. این رابطه معادل با این است که برای هر $p \in \mathbb{P}$ داشته باشیم :

$$\nu_p(m) - \min\{\nu_p(m), \nu_p(a^{\mathrm{Ord}_n(a)} - 1)\} \leq \nu_p(\mathrm{Ord}_m(a)) - \nu_p(\mathrm{Ord}_n(a))$$

اما دقت کنید اگر $\nu_p(m) \leq \nu_p(a^{\mathrm{Ord}_n(a)} - 1)$، آنگاه کافیست داشته باشیم : $\nu_p(\mathrm{Ord}_m(a)) \geq \nu_p(\mathrm{Ord}_n(a))$. اما این با توجه به رابطه عاد کردن ابتدای حل بدیهیست. در حالت دیگر داریم : $\nu_p(m) > \nu_p(a^{\mathrm{Ord}_n(a)} - 1)$. در این حالت با استفاده از لم دوخط و خواص مرتبه خواهیم داشت :

$$\nu_p\left(\frac{\mathrm{Ord}_m(a)}{\mathrm{Ord}_n(a)}\right) = \nu_p(a^{\mathrm{Ord}_n(a)\cdot \frac{\mathrm{Ord}_m(a)}{\mathrm{Ord}_n(a)}}-1) - \nu_p(a^{\mathrm{Ord}_n(a)}-1) \nu_p(a^{\mathrm{Ord}_m(a)}-1) - \nu_p(a^{\mathrm{Ord}_n(a)}-1) \nu_p(m) - \nu_p(a^{\mathrm{Ord}_n(a)}-1)$$

حال که این حکم ضعیف‌تر اثبات شده است، کافیست نشان دهیم : $\frac{m}{\gcd(m, a^{\mathrm{Ord}_n(a)}-1)} \mid \frac{\mathrm{Ord}_m(a)}{\mathrm{Ord}_n(a)}$. به طریق مشابه این رابطه را ثابت کرده و اثبات را کامل کنید.

۷. ابتدا با بررسی‌های مقدماتی شروع می‌کنیم : $p \mid q^r+1 \implies p \mid q^{2r}-1 \mid \mathrm{Ord}_p(q) \mid 2r, \mathrm{Ord}_p(q) \mid p-1 \implies \mathrm{Ord}_p(q) \mid \gcd(2r, p-1)$.
این رابطه نشان می‌دهد که یا $\mathrm{Ord}_p(q) = 2$ و یا $r \mid p - 1$ و یا $\mathrm{Ord}_p(q) = 1$. معادلاً می‌توان نوشت یا $r < p$ و یا $q \leq p$ و یا $p = 2$. حال با در نظر گرفتن این نتیجه برای هر سه معادله و با استفاده از رویکرد اکسترمالی به تناقض برسید و ثابت کنید تنها پاسخ‌های مسئله جایگشت‌های دوری مجموعه $\{2, 5, 3\}$ هستند.

۸. ابتدا به عنوان یک لم با استفاده از خواص مرتبه ثابت کنید اگر $a \in \mathbb{N}$ عددی بزرگتر از ۱ بوده و $p, q \in \mathbb{P}$ اعدادی اول باشند به نحوی که $q \mid \frac{a^p-1}{a-1}$ برقرار باشد، آنگاه $p = q$ و یا $q \overset{p}{\equiv} 1$. با استفاده از این نتیجه و لم شور حل مسئله را کامل کنید. به عنوان تعمیم این حکم، می‌توانید با استدلالی نسبتاً مشابه، ثابت کنید برای هر $n \in \mathbb{N}$، نامتناهی عدد اول به فرم $kn + 1$ وجود دارد. این قضیه (که حالت خاص قضیه دیریشله در تصاعدهای حسابی است) به دیریشله ضعیف نیز معروف است.

۹. فرض کنید $2^{2^n} + 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ تجزیه یکتای $2^{2^n} + 1$ به عوامل اول باشد. از لم بیان شده در راه حل سوال ۵ می‌دانیم تمام p_i ها به فرم $q_i 2^{n+1} + 1$ هستند که در آن q_i عددی طبیعیست. حال برای به دست آوردن کرانی برای مجموع q_i ها، سعی می‌کنیم در استفاده از بسط دوجمله‌ای نیوتن، جملات با توان بالاتر از ۱ به وجود نیاید. برای این کار، دو طرف تساوی را به پیمانه 2^{2n+2} در نظر بگیرید. داریم : $\sum_{i=1}^{k}(\alpha_i q_i 2^{n+1} + 1) + 1 \overset{2^{2n+2}}{\equiv} 1$ و در نتیجه $2^{n+1} \mid \sum_{i=1}^{k} \alpha_i q_i$. حال فرض کنید $\max\{q_i\}_{i=1}^k = q_{\max}$. بنابراین $q_{\max} \sum_{i=1}^{k} \alpha_i \geq 2^{n+1}$. در نهایت یک کران بالا برای $\sum_{i=1}^{k} \alpha_i$ بیابید و اثبات مسئله را کامل کنید.

۱۰. مشابه روند مسئله قبل، ابتدا دقت کنید $\nu_p\left((p-1)^p+1\right)=2$. سپس فرض کنید $q_i \neq p$. با استفاده از خواص مرتبه نتیجه بگیرید $\mathrm{Ord}_{{q_i}^{\alpha_i}}(p-1)$ برابر با 2 یا $2p$ است. حالت اول را با بررسی‌های مقدماتی رد کنید. نتیجه بگیرید $2p \mid \varphi({q_i}^{\alpha_i})$. حال فرض کنید برای هر $1 \le i \le n$، (به استثنا $q_i = p$) داشته باشیم : $q_i = 2pk_i + 1$ و تساوی داده شده را بازنویسی کنید. دو طرف تساوی را به پیمانه p^4 در نظر گرفته و حکم را نتیجه بگیرید.

۱۱. با استفاده از ایده‌ای مشابه سوال قبل، سعی کنید با بررسی‌های اولیه اطلاعات کافی درباره q_i ها به دست آورید و سپس دو طرف تساوی را به پیمانه p^2 در نظر بگیرید و با کامل کردن جزئیات راه حل اثبات این مسئله را کامل کنید.

۱۲. ابتدا با استفاده از بررسی‌های اولیه، می‌دانیم اگر q عامل اولی از 2^p-1 باشد، آنگاه $q \overset{p}{\equiv} 1$. حال فرض کنید $2^p - 1 = {q_1}^{\alpha_1}\cdots{q_k}^{\alpha_k}$ تجزیه یکتای 2^p-1 به عوامل اول باشد. همچنین فرض کنید $q_i = pa_i + 1$. بنابراین $2^p - 1 = \prod_{i=1}^{k}(pm_i+1)$. مشابه مسائل اخیر، برای ارائه کران درباره بزرگترین عامل اول 2^p-1 ابتدا دو طرف تساوی را به پیمانه p^2 در نظر گرفته و نتیجه بگیرید $p \mid \sum_{i=1}^{k} a_i\alpha_i$ و بنابراین اگر قرار دهید $q_{\max} = \max\{q_i\}_{i=1}^{k}$ آنگاه $a_{\max} > \frac{p}{\alpha_1+\cdots+\alpha_k}$. در نهایت ثابت کنید تمام a_i ها بزرگتر و یا مساوی با ۶ هستند و با استفاده از نتایج حاصل شده اثبات را کامل کنید.

۱۳. ابتدا مشهود است که به عنوان اولین گام برای شروع به حل مسئله، تغییر متغیر $a=p+q, b=p-q$ در جهت ساده‌سازی محاسبات مفید است. در این صورت عبارت داده شده در مسئله به رابطه $a^ab^b-1 \mid a^bb^a-a$ تبدیل می‌شود. نتیجه بگیرید که این معادل است با اینکه $a^bb^a-1 \mid a^{a-b}-b^{a-b}=a^{2q}-b^{2q}$. حال چون $\gcd(b, a^bb^a-1)=1$، فرض کنید b^* وارون ضربی b به پیمانه a^bb^a-1 باشد. در این صورت $a^bb^a-1 \mid (ab^*)^{2q}-1$. با استفاده از خواص مرتبه نتیجه می‌شود اگر $r\in\mathbb{P}$ عامل اولی از a^bb^a-1 باشد آنگاه $\mathrm{Ord}_r(ab^*)$ برابر با یکی از اعداد $1,2,q,2q$ است. با حالت‌بندی مسئله سعی کنید اثبات را کامل کنید و نتیجه بگیرید تنها جواب ممکن مسئله زوج $(p,q)=(3,2)$ خواهد بود.

۱۴. با استفاده از قضیه زیگموندی نشان دهید برای هر $a\ge 2, n\ge 7$ عدد $p\in\mathbb{P}$ موجود است به نحوی که $\mathrm{Ord}_p(a)=n$ و با استفاده از این نتیجه اثبات را کامل کنید.

۱۵. ابتدا برای شروع فرض کنید $p,q\in\mathbb{P}$ اعدادی اول و دلخواه باشند به طوری که $\gcd(q,a)=\gcd(q,b)=1$ و همچنین $q \mid a^p-b$. در این صورت از خواص مرتبه می‌توان نتیجه گرفت $\mathrm{Ord}_q(b)$ برابر با $\mathrm{Ord}_q(a)$ و یا $p\,\mathrm{Ord}_q(a)$ است. حال فرض کنید فقط متناهی q موجود باشد که در حالت اول صدق کند. برای هر q دیگر باید داشته باشیم: $q-1 \mid \mathrm{Ord}_q(b)=p\,\mathrm{Ord}_q(a) \mid p$. ابتدا ثابت کنید دنباله $\{a^p-b \mid \forall p\in\mathbb{P}\}$ نامتناهی عامل اول دارد. همچنین ثابت کنید اگر $q\in\mathbb{P}$ عددی اول باشد که نسبت به a,b اول است نامتناهی جمله از دنباله موجود است که بر q بخش‌پذیر نباشد. سپس نتیجه بگیرید اگر متناهی عدد اول با خواص داده شده در صورت مسئله موجود باشد، می‌توان $c,d\in\mathbb{N}$ طبیعی و بیشتر از ۱ را پیدا کرد به طوری که برای هر عامل اول $p,q\in\mathbb{P}$ به طوری که $q \mid c^p-d$ داشته باشیم $q \mid c-d$ و یا $q-1 \mid p$. حال نتیجه بگیرید به ازای هر عامل اول q از مجموعه $\{c^p-d \mid \forall p\in\mathbb{P}\}$ به طوری که $q \mid c-d$ برقرار باشد، توان q در اعضای این دنباله کمتر یا مساوی با $\nu_q(c-d)$ است. در نتیجه هر عضو از این مجموعه را می‌توان به صورت حاصل‌ضرب یک مقسوم علیه از $c-d$ و یک عدد طبیعی که تمام عوامل اول آن به فرم $kp+1$ هستند نوشت. با تکمیل جزئیات راه حل اثبات را کامل کنید.

۱۶. فرض کنید $q \overset{p}{\equiv} 1$. در این صورت اگر $n\in\mathbb{N}$ موجود باشد به طوری که $q \mid n^p-p$، آنگاه داریم : $q \mid n^{q-1}-p^{\frac{q-1}{p}} \overset{q}{\equiv} 1-p^{\frac{q-1}{p}} \implies \mathrm{Ord}_q(p) \mid \frac{q-1}{p}$. حال به عنوان یک لم ثابت کنید $q\in\mathbb{P}$ موجود است به طوری که $q \mid \frac{p^p-1}{p-1}$ و $p^2 \nmid q-1$ و نتیجه بگیرید این عدد اول در شرط فوق صدق نمی‌کند و اثبات را کامل کنید.

۱۷. ابتدا با استفاده از خواص مرتبه ثابت کنید برای $p\in\mathbb{P}$ به اندازه کافی بزرگ، a^p-1 عامل اولی بزرگتر از k دارد. سپس واضح است که برای هر مقدار $n\in\mathbb{N}$ به اندازه کافی بزرگ، مقدار a^n-1 عامل اولی بزرگتر از k خواهد داشت. حالتی را در نظر بگیرید که تمام عوامل اول n از مقدار ثابتی (فرضاً t) کمتر باشند. در این صورت توان عوامل اول کمتر از k در مقدار a^n-1 را با استفاده از لم دوخط محدود کنید و با تکمیل استدلال، اثبات قضیه را کامل کنید. (توجه کنید درستی حکم با قضیه زیگموندی بدیهیست)

۱۸. ابتدا به عنوان یک لم ثابت کنید برای هر $p\in\mathbb{P}, a\in\mathbb{Z}$ به طوری که $\gcd(p,a)=1$ برقرار باشد و هر $k\in\mathbb{N}$ داریم : $\mathrm{Ord}_p(a^k)=\frac{\mathrm{Ord}_p(a)}{\gcd(k,\mathrm{Ord}_p(a))}$. بنا بر شرط اول بدیهیست که $f(1)=1$. حال با جاگذاری $n=1$ در شرط دوم داریم : $\mathrm{Ord}_p(a)=\mathrm{Ord}_p(f(a))$. (برای هر $p\nmid a$) همچنین مجدداً مطابق شرط اول بدیهیست که برای هر $p\in\mathbb{P}$ داریم : $f(p)=p^k$. با جاگذاری در شرط دوم داریم : $\forall p,q\in\mathbb{P}, p\neq q \implies \mathrm{Ord}_q(p)=\mathrm{Ord}_q(p^k)$. اما طبق لم بیان شده در آغاز راه حل، این معادل با این است که $\gcd(k,\mathrm{Ord}_q(p))=1$. حال دقت کنید اگر $k\neq 1$ آنگاه طبق قضیه زیگموندی $q\in\mathbb{P}$ موجود است به طوری که $k \mid \mathrm{Ord}_q(p)$ که با نتیجه اخیر در تناقض است. بنابراین $\forall p\in\mathbb{P} \implies f(p)=p$. حال در شرط دوم مقدار a را برابر عددی اول قرار دهید. آنگاه داریم : $\mathrm{Ord}_p(q^b)=\mathrm{Ord}_p(q^{f(b)})$. مجدداً با استفاده از لم مذکور نتیجه بگیرید : $\gcd(b,\mathrm{Ord}_p(q))=\gcd(f(b),\mathrm{Ord}_p(q))$. حال فرض کنید $f(b)\neq b$ و سپس عامل اولی را در نظر بگیرید که در تجزیه یکتای $b, f(b)$ به عوامل اول، توان متفاوتی داشته باشد و با مجدداً با استفاده از قضیه زیگموندی به تناقض برسید.

تمرینات اضافه

۱. ابتدا مانند هر مسئله دیگری با بررسی‌های اولیه شروع به حل می‌کنیم. فرض کنید q عامل اول دلخواهی از n باشد. حال از برهان خلف استفاده کنید و دقت کنید فرض خلف معادل با این است که هر عامل اول از n نسبت به $m^{n-1}-1$ اول باشد. بنابراین برای هر $q \mid n$ خواهیم داشت : $q \mid m^{p(n-1)}-1, q\nmid m^{n-1}-1$. از این دو رابطه نتیجه بگیرید که $q-1 \mid \mathrm{Ord}_q(p) \mid p$. بنابراین هر عامل اول از n به فرم $kp+1$ است و در نتیجه n خود عددی به فرم $kp+1$ خواهد بود. با جاگذاری این رابطه در فرض مسئله داریم : $kp+1 \mid n^{kp^2}-1, \gcd(kp+1, m^{kp}-1)=1$. مجدداً عامل اولی از $kp+1$ در نظر بگیرید (مثل q) و با روندی مشابه ثابت کنید $q \overset{p^2}{\equiv} 1$. سپس اثبات کنید که هر بار می‌توان همین استدلال را تکرار کرد و در نتیجه $\nu_p(n-1)$ باید از هر عدد طبیعی بزرگتر است و بنابراین $n=1$ که تناقض است.

۲. ابتدا حالتی را در نظر بگیرید که $p \geq 3$. از رابطه $n^p+1 \geq p^n+1$ نتیجه بگیرید $p \geq n \geq 3$. در نهایت دقت کنید چون n باید فرد باشد داریم : $p+1 \mid p^n+1$ و بنابراین $p+1 \mid n^p+1 \implies p+1 \mid n^{2p}-1 \implies \mathrm{Ord}_{p+1}(n) \mid 2p$. بنا بر دو نتیجه اخیر، مقدار $\mathrm{Ord}_{p+1}(n)$ برابر با 2 و یا $2p$ است. اما در حالت دوم داریم : $2p \mid \varphi(p+1) < 2p$ که به وضوح تناقض است. در نتیجه $\mathrm{Ord}_{p+1}(n) = 2 \implies n^2 \overset{p+1}{\equiv} 1$. با استفاده از این رابطه و فرض اولیه مسئله نتیجه بگیرید $p+1 \mid n+1$ که با نتیجه $n \leq p$ تنها جواب $n = p$ را به دست می‌دهد. در نهایت با بررسی حالت $p = 2$ اثبات را کامل کنید.

۳. ابتدا با تغییر صورت مسئله داریم : $\nu_p(ca^n-db^n) = \nu_p(\frac{c}{d}\cdot\frac{a^n}{b^n}-1) = \nu_p(\frac{c}{d}-(\frac{b}{a})^n))$. بنابراین کافیست ثابت کنیم اگر دنباله $\{v_p(\frac{c}{d}-(\frac{b}{a})^n) \mid n \in \mathbb{N}\}$ کراندار بوده و تماماً صفر نباشد، اعضای ناصفر آن با یکدیگر برابرند. فرض خلف کنید که $\alpha, \beta \in \mathbb{N}$ موجود باشند که $m = \nu_p(\frac{c}{d}-(\frac{b}{a})^\alpha) > \nu_p(\frac{c}{d}-(\frac{b}{a})^\beta) > 0$. حال فرض کنید $t \in \mathbb{N}$ موجود باشد به طوری که $\nu_p(1-(\frac{b}{a})^t) = m$. در این وضعیت $\frac{c}{d}-(\frac{b}{a})^\alpha, (\frac{b}{a})^{tk}-1$ که در آن $k \in \mathbb{N}$ عددی طبیعی و نسبت به p اول است، هر دو دارای این خاصیت هستند که توان عامل اول p در آنها برابر با m است و در صورتی که بتوان ضرایب p^m در آنها را به دست آورد، می‌توان ثابت کرد جمله $(\frac{c}{d}-(\frac{b}{a})^\alpha)+(\frac{b}{a})^\alpha\cdot(1-(\frac{b}{a})^{tk}) = \frac{c}{d}-(\frac{b}{a})^{\alpha+tk}$ در دنباله موجود است به طوری که توان p در آن حداقل $m+1$ باشد که با حکم مسئله در تناقض است.

برای تکمیل اثبات دقت کنید طبق مسئله شماره ۱۱ مجموعه سوالات لم دوخط داریم : $\frac{1-(\frac{b}{a})^{tk}}{1-(\frac{b}{a})^t} \overset{p^m}{\equiv} k$ و از این نتیجه بگیرید اگر $1-(\frac{b}{a})^t$ به فرم sp^m باشد که در آن $\gcd(s,p) = 1$، در این صورت $1-(\frac{b}{a})^{tk} \overset{p^{m+1}}{\equiv} ksp^m$. از طرفی فرض کنید $\frac{c}{d}-(\frac{b}{a})^\alpha = rp^m$ که مجددا $\gcd(r,p) = 1$ و نتیجه می‌شود که $\frac{c}{d}-(\frac{b}{a})^{\alpha+tk} = p^m(r+ks(\frac{b}{a})^\alpha)$ که با انتخاب مناسب k بدیهتاً می‌تواند بر p^{m+1} بخش‌پذیر باشد که یک تناقض است. برای تکمیل اثبات صرفا کافیست ثابت کنیم $t \in \mathbb{N}$ موجود است به طوری که $\nu_p(1-(\frac{b}{a})^t) = m$ برقرار باشد. برای اثبات این حکم ثابت کنید $m \geq \nu_p(1-(\frac{b}{a})^{\mathrm{Ord}_p(\frac{b}{a})})$ و سپس با استفاده از لم دوخط این گزاره را نتیجه بگیرید و اثبات را کامل کنید.