پک دوم نظریه اعداد گروه ببعی، مبحث لم دو خط و p-adic order

آرین همتی مهنوش عظیمیان ارشیا صادقی

منابع رنگی شده لینک های قابل کلیک هستند

چکیده

نظریه مقدماتی اعداد از لحاظ تکنیک‌ها و راهبردهای حل مسئله به دو دسته اصلی تقسیم می‌شود. دسته اول که مبتنی بر قضیه اساسی تقسیم است، حساب پیمانه‌ای (Modular Arithmetic) نامیده می‌شود و درباره سیستم های معادلات همنهشتی و خواص آنها بحث می‌کند. در مقابل، دسته دوم که مبتنی بر قضیه اساسی حساب است، تئوری بخش پذیری (Divisibility Theory) نامیده می‌شود و اساساً درباره روابط عاد کردن، عوامل اول و تجزیه اعداد صحیح بحث می‌کند. در این بین، روابط ν_p در نظریه اعداد اتصالی میان این دو بخش به ظاهر مجزا ایجاد می‌کند که منجر به ایجاد ابزاری قوی در حل مسائل نظریه اعداد می‌شود. در این پک با تعریف و خواص تابع ν_p در نظریه اعداد بیشتر آشنا خواهیم شد و سپس لم معروفی به نام لم دو خط (LTE) را بیان می‌کنیم که کاربرد بسیار موثری در نظریه مقدماتی اعداد دارد.

۱ قضیه اساسی حساب و تجزیه یکتا به عوامل اول

تعریف. اعداد اول : به هر عدد طبیعی مثل $n > 1$ که بر هیچ یک از اعداد مجموعه $\{2, 3, \cdots, n-1\}$ بخش پذیر نباشد، عدد اول می‌گوییم. مجموعه اعداد اول را با $\mathbb{P}$ نمایش می‌دهیم. هر عدد غیر اول بزرگتر از یک را مرکب می‌نامیم.

قضیه ۱. برای هر عدد طبیعی $n > 1$ عدد اول $p \in \mathbb{P}$ موجود است که n بر p بخش پذیر باشد. همچنین در این صورت، p را یک عامل اول از n می‌نامیم.

اثبات. از استقرای قوی روی n استفاده می‌کنیم. حکم برای هر $n \in \mathbb{P}$ واضح است، زیرا اگر n اول باشد، با توجه به اینکه $n \mid n$ نتیجه می‌گیریم n عددی اول است که n بر آن بخش پذیر است که حکم را ثابت می‌کند. در غیر این صورت، فرض کنید k عددی مرکب باشد. بنا بر فرض استقرا، درستی حکم برای مقادیر $n = 2, 3, \cdots, k-1$ واضح است و می‌خواهیم درستی حکم را برای $n = k$ اثبات کنیم. طبق تعریف عدد مرکب، n باید مقسوم علیهی در بازه $[2, k-1]$ داشته باشد. این مقسوم علیه را d بنامید. آنگاه طبق فرض استقرا، d عاملی اول مثل p خواهد داشت و داریم : $p \mid d \mid k$ که نشان می‌دهد p اولی وجود دارد که n بر آن بخش پذیر است و بنابراین اثبات کامل است.

قضیه ۲. قضیه اساسی حساب : هر عدد طبیعی $n > 1$ برابر با حاصل‌ضرب تعدادی متناهی از اعداد اول است. نمایش n به صورت حاصل‌ضرب تعدادی عدد اول را به شکل $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ نشان می‌دهیم و آن را تجزیه n به عوامل اول می‌نامیم.

اثبات. مجددا از استقرای قوی استفاده می‌کنیم. حکم برای مقادیر $n \in \mathbb{P}$ بدیهیست. حال فرض کنید k عددی مرکب باشد. فرض کنید حکم برای تمامی مقادیر $n = 2, 3, \cdots, k-1$ صادق باشد. آنگاه درستی حکم را برای $n = k$ اثبات می‌کنیم. دقت کنید طبق قضیه یک، n عاملی اول مثل p دارد. آنگاه داریم : $n = p \cdot (\frac{n}{p})$ که در آن $1 < \frac{n}{p} < n$. بنا بر فرض استقرای قوی، $\frac{n}{p}$ برابر با حاصل‌ضرب تعدادی عدد اول است. فرض کنید $\frac{n}{p} = \prod_{i=1}^{m} p_i$ (p_i ها لزوماً متمایز نیستند). آنگاه خواهیم داشت :

$n = p \cdot (\frac{n}{p}) = p \cdot \prod_{i=1}^{m} p_i$ و بنابراین n هم به صورت حاصل‌ضرب تعدادی عدد اول قابل نمایش است و حکم اثبات می‌شود.

اکنون که ثابت کردیم اعداد صحیح قابل تجزیه به عوامل اول هستند، قضیه اساسی حساب را کامل کرده و اثبات می‌کنیم هر عدد صحیح ناصفر تجزیه ای یکتا به عوامل اول دارد.

قضیه ۳. تجزیه هر عدد طبیعی به اعداد اول، صرف نظر از ترتیب اعداد اول یکتاست. به عبارتی اگر دو تجزیه از عدد طبیعی n به عوامل اول وجود داشته باشد، آنگاه در این دو تجزیه مجموعه عوامل اول یکسانند و همچنین تکرر هر عامل اول در این دو تجزیه همواره برابر است. این قضیه نشان می‌دهد که تجزیه $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ که در آن $p_1 < p_2 < \cdots < p_m$ یکتاست. به این نمایش از تجزیه n به عوامل اول، تجزیه استاندارد گفته می‌شود.

اثبات. فرض کنید $p_1^{\alpha_1} \cdots p_m^{\alpha_m}, q_1^{\beta_1} \cdots q_r^{\beta_r}$ دو تجزیه استاندارد از عدد طبیعی n باشند. برای اثبات حکم کافیست ثابت کنیم $\{p_1, \cdots, p_m\} = \{q_1, \cdots, q_r\}$ و همچنین $\forall i \in \mathbb{N} \implies \alpha_i = \beta_i$. برای اثبات حکم اول توجه کنید : $\forall 1 \leq i \leq m :$ $p_i \mid n \implies p_i \in \{q_1, \cdots, q_r\}$ و همچنین داریم : $\forall 1 \leq j \leq r : q_j \mid n \implies q_j \in \{p_1, \cdots, p_m\}$. بنابراین داریم :

$$\{p_1, \cdots, p_m\} \subseteq \{q_1, \cdots, q_r\} \quad , \quad \{q_1, \cdots, q_r\} \subseteq \{p_1, \cdots, p_m\} \implies \{p_1, \cdots, p_m\} = \{q_1, \cdots, q_r\}$$

برای اثبات حکم دوم از استقرا روی مقدار $M = \max(\alpha_1 + \cdots + \alpha_m, \beta_1 + \cdots + \beta_r)$ استفاده می‌کنیم. به عنوان پایه استقرا واضح است که حکم برای $M = 1$ بدیهیست زیرا تنها یک عامل اول با توان یک وجود دارد و بنابراین $\alpha_1 = \beta_1 = 1$. حال فرض کنید حکم برای $M = M_0$ صحیح باشد و حکم را برای $M = M_0 + 1$ اثبات می‌کنیم. با توجه به اینکه $\alpha_1, \beta_1 \geq 1$ واضح است که داریم :

$$p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m} = n = q_1^{\beta_1 - 1} \cdots q_r^{\beta_r}$$

که در آن همه توان ها اعداد نامنفی هستند. (ممکن است $\alpha_1 - 1$ یا $\beta_1 - 1$ برابر با صفر باشند) در این شرایط داریم :

$$M = \max(\alpha_1 - 1 + \cdots + \alpha_m, \beta_1 - 1 + \cdots + \beta_r) = \max(\alpha_1 + \cdots + \alpha_m, \beta_1 + \cdots + \beta_r) - 1 = M_0 + 1 - 1 = M_0$$

اما درستی حکم برای $M = M_0$ (دقت کنید با توجه به حکم اول $m = r$) : از فرض استقرا واضح است، در نتیجه خواهیم داشت

$$\alpha_1 - 1 = \beta_1 - 1 \quad , \quad \alpha_2 = \beta_2 \quad \cdots \quad \alpha_m = \beta_r$$

که مستقیما نتیجه می‌دهد :

$$\alpha_1 = \beta_1 \quad , \quad \alpha_2 = \beta_2 \quad \cdots \quad \alpha_m = \beta_r$$

که حکم استقرا را اثبات می‌کند و اثبات این قضیه نیز کامل است.

۲ تابع ν_p (p-adic order)

تعریف. برای هر عدد طبیعی n و عدد اول p بزرگترین مقدار صحیح k که در دو رابطه $p^k \mid n, p^{k+1} \nmid n$ صدق کند را $\nu_p(n)$ می‌نامیم. برای هر عدد طبیعی n اگر تجزیه یکتای n به عوامل اول به شکل $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ باشد، آنگاه برای هر $1 \leq i \leq m$ داریم : $\nu_{p_i}(n) = \alpha_i$ و برای هر عدد اول دیگر خواهیم داشت : $\nu_p(n) = 0$.

توجه کنید طبق تعریف تابع ν_p اگر هر عدد صحیح مثل k این خاصیت را داشته باشد که $p^{k+1} \mid n$ آنگاه $\nu_p(n) > k$. همچنین مجدداً طبق تعریف، برای هر عدد صحیح k اگر داشته باشیم $p^k \nmid n$ آنگاه $\nu_p(n) < k$. در ادامه با خواص این تابع پرکاربرد در نظریه مقدماتی اعداد آشنا خواهیم شد.

قضیه ۴. خواص زیر را برای تابع ν_p اثبات کنید.

۱. $\forall n \in \mathbb{N}, k \in \mathbb{Z} : p^{k+1} \mid n \implies \nu_p(n) > k$.

۲. $\forall n \in \mathbb{N}, k \in \mathbb{Z} : p^k \nmid n \implies \nu_p(n) < k$.

۳. $\forall n \in \mathbb{N}, p \in \mathbb{P} \implies \nu_p(n) \geq 0$.

۴. $\forall n \in \mathbb{N}, p \in \mathbb{P} : \quad p \mid n \iff \nu_p(n) \geq 1$.

۵. $\forall n\in\mathbb{N}, p\in\mathbb{P}, \alpha\in\mathbb{N}: \quad p^\alpha | n \iff \nu_p(n)\geq\alpha$.

۶. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p(mn)=\nu_p(m)+\nu_p(n)$.

۷. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p(\frac{m}{n})=\nu_p(m)-\nu_p(n)$.

۸. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p(m^n)=n\nu_p(m)$.

۹. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p(\sqrt[n]{m})=\frac{\nu_p(m)}{n}$.

۱۰. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies n\mid\nu_p(m^n)$.

۱۱. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p(m+n)\geq\min(\nu_p(m),\nu_p(n))$.

۱۲. $\forall n,m\in\mathbb{N} \implies m=n \iff \{\forall p\in\mathbb{P}:\nu_p(m)=\nu_p(n)\}$.

۱۳. $\forall n,m\in\mathbb{N} \implies m\mid n \iff \{\forall p\in\mathbb{P}:\nu_p(m)\leq\nu_p(n)\}$.

۱۴. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p\big(\gcd(m,n)\big)=\min\big(\nu_p(m),\nu_p(n)\big)$.

۱۵. $\forall n,m\in\mathbb{N}, p\in\mathbb{P} \implies \nu_p\big(\operatorname{lcm}(m,n)\big)=\max\big(\nu_p(m),\nu_p(n)\big)$.

اثبات.

۱. **طبق تعریف بدیهیست.**

۲. **طبق تعریف بدیهیست.**

۳. **با قرار دادن** $k=-1$ **در رابطه اول داریم :** $p^{-1+1}=p^0=1\mid n \implies \nu_p(n)>-1 \implies \nu_p(n)\geq 0$.

۴. **با قرار دادن** $k=0$ **در رابطه اول داریم :** $p^{0+1}=p^1=p\mid n \implies \nu_p(n)>0 \implies \nu_p(n)\geq 1$. **اثبات عکس این رابطه با توجه به تعریف** ν_p **بدیهیست.**

۵. **با قرار دادن** $k=\alpha-1$ **در رابطه اول داریم :** $p^{\alpha-1+1}=p^\alpha\mid n \implies \nu_p(n)>\alpha-1 \implies \nu_p(n)\geq\alpha$. **اثبات عکس این رابطه با توجه به تعریف** ν_p **بدیهیست.**

۶. **با توجه به تعریف** ν_p **داریم :**

$$p^{\nu_p(n)}\mid n, p^{\nu_p(m)}\mid m \implies p^{\nu_p(n)+\nu_p(m)}\mid mn$$

بنابراین طبق قضیه پنج داریم : $\nu_p(mn)\geq\nu_p\left(p^{\nu_p(n)+\nu_p(m)}\right)=\nu_p(n)+\nu_p(m)$. **حال فرض کنید داشته باشیم :** $\nu_p(mn)>\nu_p(n)+\nu_p(m) \iff \nu_p(mn)\geq\nu_p(n)+\nu_p(m)+1$. **طبق قضیه پنج داریم :**

$$\nu_p(mn)\geq\nu_p(n)+\nu_p(m)+1 \implies p^{\nu_p(n)+\nu_p(m)+1}\mid mn \implies p^{\nu_p(n)+1}\mid n \quad \text{یا} \quad p^{\nu_p(m)+1}\mid m$$

اما می‌دانیم هر دوی این روابط با توجه به تعریف $\nu_p(m),\nu_p(n)$ **نادرستند و بنابراین** $\nu_p(mn)=\nu_p(m)+\nu_p(n)$.

۷. **از رابطه ششم داریم :** $\nu_p(m)=\nu_p(n\cdot\frac{m}{n})=\nu_p(n)+\nu_p(\frac{m}{n}) \implies \nu_p(\frac{m}{n})=\nu_p(m)-\nu_p(n)$.

۸. **با استفاده از استقرا و رابطه ششم بدیهیست.**

۹. **با توجه به رابطه شماره هشت داریم :** $\nu_p(m)=\nu_p\big((\sqrt[n]{m})^n\big)=n\cdot\nu_p(\sqrt[n]{m}) \implies \nu_p(\sqrt[n]{m})=\frac{\nu_p(m)}{n}$.

۱۰. **از رابطه شماره هشت بدیهیست.**

۱۱. فرض کنید $\alpha = \nu_p(n), \beta = \nu_p(m)$. بدون کم شدن از کلیت مسئله فرض کنید $\alpha \geq \beta$. آنگاه داریم :
$p^\beta \mid m, p^\beta \mid p^\alpha \mid n \implies p^\beta \mid m+n$ و بنا بر قضیه پنج داریم : $\nu_p(m+n) \geq \nu_p(p^\beta) = \beta$ که حکم این رابطه را اثبات می‌کند. (به عنوان تمرین، حالت تساوی این نامساوی را بررسی کنید)

۱۲. با توجه به قضیه سوم (تجزیه یکتا) بدیهیست.

۱۳. می‌دانیم $\nu_p(n) \geq \nu_p(m) \iff \nu_p(n) - \nu_p(m) = \nu(k) \geq 0 \iff \exists\, k \in \mathbb{Z} : n = mk \implies m \mid n$.

۱۴. قرار دهید $\gcd(m,n) = d$. با توجه به تعریف ب.م.م داریم :

$$d \mid m, d \mid n \implies \nu_p(m) \geq \nu_p(d), \nu_p(n) \geq \nu_p(d) \implies \min(\nu_p(m), \nu_p(n)) \geq \nu_p(d)$$

حال اگر داشته باشیم $\min(\nu_p(m), \nu_p(n)) > \nu_p(d)$ آنگاه قرار دهید $d' = pd$. حال داریم :

$$\nu_p(d') = \nu_p(p) + \nu_p(d) = 1 + \nu_p(d) \implies \min(\nu_p(m), \nu_p(n)) \geq \nu_p(d')$$

و بنابراین $d' > d$ یک مقسوم علیه مشترک از m, n است. اما این با تعریف ب.م.م به عنوان "بزرگترین" مقسوم علیه مشترک متناقض است و بنابراین باید داشته باشیم : $\min(\nu_p(m), \nu_p(n)) = \nu_p(d)$ که این بخش را اثبات می‌کند.

۱۵. مشابه اثبات رابطه قبل قرار می‌دهیم $\operatorname{lcm}(m,n) = d$. با توجه به تعریف ک.م.م داریم :

$$m \mid d, n \mid d \implies \nu_p(m) \leq \nu_p(d), \nu_p(n) \leq \nu_p(d) \implies \min(\nu_p(m), \nu_p(n)) \leq \nu_p(d)$$

حال اگر داشته باشیم $\min(\nu_p(m), \nu_p(n)) < \nu_p(d)$ آنگاه قرار دهید $d' = \frac{d}{p}$. حال داریم :

$$\nu_p(d') = \nu_p(d) - \nu_p(p) = \nu_p(d) - 1 \implies \min(\nu_p(m), \nu_p(n)) \leq \nu_p(d')$$

و بنابراین $d' < d$ یک مضرب مشترک از m, n است. اما این با تعریف ک.م.م به عنوان "کوچکترین" مضرب مشترک متناقض است و بنابراین باید داشته باشیم : $\min(\nu_p(m), \nu_p(n)) = \nu_p(d)$ که این بخش را نیز اثبات می‌کند.

مثال ۱. فرض کنید $a, b \in \mathbb{N}$ اعدادی طبیعی هستند که $a > b$ و همچنین $ab(a-b) \mid a^3 + ab + b^3$. ثابت کنید ab مکعب کامل یک عدد صحیح است.

راه حل. عدد اول دلخواه $p \mid ab$ را در نظر بگیرید. ابتدا فرض کنید $\nu_p(a) = \nu_p(b) = k$. در این صورت طبق موارد قضیه قبل داریم

$$\nu_p(ab(a-b)) = \nu_p(a) + \nu_p(b) + \nu_p(a-b) = 2k + \nu_p(a-b) \geq 3k$$

$$\nu_p(a^3) = \nu_p(b^3) = 3k \quad , \quad \nu_p(ab) = 2k \implies \nu_p(a^3 + ab + b^3) = 2k$$

اما طبق رابطه عاد کردن ابتدای مسئله، باید داشته باشیم $2k = \nu_p(a^3 + ab + b^3) \geq \nu_p(ab(a-b)) = 3k$ که بدلیل ناصفر بودن k یک تناقض است. حال که $\nu_p(a), \nu_p(b)$ نمی‌توانند با هم برابر باشند، بدون کم شدن از کلیت مسئله فرض کنید $\nu_p(a) > \nu_p(b)$. در این صورت مجددا داریم :

$$\nu_p(ab(a-b)) = \nu_p(a) + \nu_p(b) + \nu_p(a-b) = \nu_p(a) + 2\nu_p(b) \implies \nu_p(a^3 + ab + b^3) \geq \nu_p(a) + 2\nu_p(b)$$

اما حال می‌دانیم $\nu_p(a^3) > \nu_p(b^3) \implies \nu_p(a^3 + b^3) = 3\nu_p(b)$. از طرفی $\nu_p(ab) = \nu_p(a) + \nu_p(b)$. حال بدیهیست که داریم $\nu_p(ab) < \nu_p(a^3)$. اگر همچنین داشته باشیم $\nu_p(ab) \neq \nu_p(b^3)$ آنگاه طبق قضیه قبل داریم : $\nu_p(a^3 + ab + b^3) = \min(\nu_p(b^3), \nu_p(ab))$. اما می‌دانیم هر دوی این مقادیر از $\nu_p(a) + 2\nu_p(b)$ اکیداً کوچکترند که متناقض با رابطه عاد کردن اولیه مسئله است. بنابراین نتیجه می‌گیریم $\nu_p(ab) = \nu_p(b^3) = 3\nu_p(b)$ و در نتیجه $3 \mid \nu_p(ab)$ که اثبات مسئله را کامل می‌کند.

مثال ۲. فرض کنید $a, b, c \in \mathbb{N}$ اعدادی طبیعی باشند به طوری که $\frac{ab}{c} + \frac{ac}{b} + \frac{bc}{a} \in \mathbb{N}$. ثابت کنید $\frac{ab}{c}, \frac{ac}{b}, \frac{bc}{a} \in \mathbb{N}$.

راه حل.

$$\frac{ab}{c} + \frac{ac}{b} + \frac{bc}{a} = \frac{a^2b^2 + a^2c^2 + b^2c^2}{abc} \in \mathbb{N} \iff abc \mid a^2b^2 + a^2c^2 + b^2c^2$$

عدد اول دلخواه $p \mid abc$ را در نظر بگیرید. بدون کم شدن از کلیت مسئله فرض کنید $\nu_p(a) \geq \nu_p(b) \geq \nu_p(c)$. برای اثبات حکم کافیست نشان دهیم $\nu_p(b) + \nu_p(c) \geq \nu_p(a)$. (چرا؟) فرض کنید این نامساوی نادرست باشد و داشته باشیم $\nu_p(b) + \nu_p(c) < \nu_p(a)$. در این صورت داریم :

$$\nu_p(a^2b^2) = 2\nu_p(a) + 2\nu_p(b) > 4\nu_p(b) + 2\nu_p(c) \geq 2\nu_p(b) + 2\nu_p(c) = \nu_p(b^2c^2)$$

$$\nu_p(a^2c^2) = 2\nu_p(a) + 2\nu_p(c) > 2\nu_p(b) + 4\nu_p(c) \geq 2\nu_p(b) + 2\nu_p(c) = \nu_p(b^2c^2)$$

$$\nu_p(a^2b^2) > \nu_p(b^2c^2) \quad , \quad \nu_p(a^2c^2) > \nu_p(b^2c^2) \implies \nu_p(a^2b^2 + a^2c^2) > \nu_p(b^2c^2)$$

$$\implies \nu_p(abc) \leq \nu_p(a^2b^2 + a^2c^2 + b^2c^2) = \nu_p(b^2c^2) \implies 2\nu_p(b) + 2\nu_p(c) \geq \nu_p(a) + \nu_p(b) + \nu_p(c)$$

$$\iff \nu_p(b) + \nu_p(c) \geq \nu_p(a)$$

که با فرض خلف در تناقض است. بنابراین فرض خلف باطل بوده و اثبات مسئله کامل است.

مثال ۳. تمام $x, y \in \mathbb{N}$ را بیابید که داشته باشیم $y > x$ و ثانیاً $x^{x+y} = y^{y-x}$.

راه حل.

$$\forall p \in \mathbb{P} : p \mid x \iff p \mid y$$

$$\forall p \in \mathbb{P}, p \mid xy : \quad (x+y)\nu_p(x) = (y-x)\nu_p(y) \quad , \quad x + y > y - x \implies \nu_p(y) > \nu_p(x)$$

$$\forall p \in \mathbb{P}, p \mid xy : \nu_p(y) > \nu_p(x) \implies x \mid y \implies \exists k \in \mathbb{N} : y = kx$$

$$\implies x^{x+xk} = (xk)^{xk-x} \iff (x^2)^x = (k^{k-1})^x, x \neq 0 \implies x^2 = k^{k-1}$$

بنابراین k عددی فرد است : $\exists t \in \mathbb{N} : k = 2t + 1$ و در نهایت داریم :

$$x^2 = (2t+1)^{2t} \iff x = (2t+1)^t \implies y = kx = (2t+1)x = (2t+1) \cdot (2t+1)^t = (2t+1)^{t+1}$$

و بنابراین جواب مسئله همه زوج های $(x, y) = \left((2t+1)^t, (2t+1)^{t+1}\right)$ است که در آن $t \in \mathbb{N}$ عدد طبیعی دلخواه است.

حال که با خواص این تابع به طور کامل آشنا شدید، کاملا وجه ارتباط این تابع بین دو بخش پیمانه ای و بخش پذیری در نظریه اعداد مشهود خواهد بود. با استفاده از این ابزار قدرتمند، روابط ضربی موجود در عبارات نظریه اعدادی تبدیل به روابط جمعی روی توان های عبارات خواهند شد که کار با عبارات و خواص آنها را بسیار ملموس تر و ساده تر خواهد کرد. در ادامه با یکی از ابزارهای قدرتمند در استفاده از تابع ν_p آشنا خواهید شد.

همانطور که احتمالا تا الان متوجه شدید، نقطه ضعف این ابزار قدرتمند در عباراتیست که در آنها جمع به کار رفته است. در عبارات ضربی با استفاده از خواص ارائه داده شده می‌توان مقدار دقیق ν_p را محاسبه کرد اما در عبارات حاوی جمع تنها رابطه یازده است که یک کران برای این تابع در اختیار ما می‌گذارد. در ادامه با قضیه‌ای به نام لم دو خط (Lifting The Exponents) آشنا خواهید شد که تا حدی امکان دسترسی تابع ν_p به عبارات جمعی را برای ما ممکن می‌سازد. صورت اصلی این قضیه به شرح زیر است :

۳ لم دو خط (Lifting The Exponents lemma)

قضیه ۵. برای هر عدد اول فرد p و $a,b\in\mathbb{Z}$ ، اگر داشته باشیم $p\nmid ab, p\mid a-b$ آنگاه برای هر عدد طبیعی k خواهیم داشت :

$$\nu_p(a^k-b^k)=\nu_p(a-b)+\nu_p(k)$$

اثبات. برای اثبات حکم، از استقرا روی $\nu_p(k)$ استفاده می‌کنیم. به عنوان پایه استقرا دقت کنید اگر $p\nmid k \iff \nu_p(k)=0$ آنگاه داریم :

$$\nu_p(k)=\nu_p(a^k-b^k)-\nu_p(a-b)=\nu_p(\frac{a^k-b^k}{a-b})=\nu_p(a^{k-1}+a^{k-2}b+\cdots+b^{k-1})$$

اما داشتیم $a\overset{p}{\equiv} b$ بنابراین $a^{k-1}+a^{k-2}b+\cdots+b^{k-1}\overset{p}{\equiv}a^{k-1}+a^{k-1}+\cdots+a^{k-1}=ka^{k-1}$ اما با توجه به مفروضات داریم : $p\nmid k, p\nmid a$ و در نتیجه $\nu_p(ka^{k-1})=0$ و بنابراین $\nu_p(a^{k-1}+a^{k-2}b+\cdots+b^{k-1})=0$ که حکم را در این حالت ثابت می‌کند. حال فرض کنید حکم برای $\nu_p(k)=n_0$ صادق باشد. برای $\nu_p(k)=n_0+1$ ابتدا قرار دهید $k=pk'$ و بنابراین داریم : $\nu_p(k')=n_0$. از طرفی : $a^k-b^k=a^{pk'}-b^{pk'}=(a^p)^{k'}-(b^p)^{k'}$. حال نشان می‌دهیم شرایط استفاده از فرض استقرا برقرار است : به وضوح a^p,b^p همچنان نسبت به p اولند. در رابطه با شرط دوم، طبق قضیه کوچک فرما داریم : $a^p\overset{p}{\equiv}a, b^p\overset{p}{\equiv}b \implies a^p-b^p\overset{p}{\equiv}a-b\overset{p}{\equiv}0$ و بنابراین کماکان $p\mid a^p-b^p$. از طرفی $\nu_p(k')=n_0$. پس همه شرایط استفاده از فرض استقرا فراهم است. با توجه به فرض استقرا داریم :

$$\nu_p\Big((a^p)^{k'}-(b^p)^{k'}\Big)=\nu_p(a^p-b^p)+\nu_p(k')=\nu_p(a-b)+\nu_p(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})+\nu_p(k')$$

پس کافیست ثابت کنیم $\nu_p(k)=\nu_p(pk')=1+\nu_p(k')=\nu_p(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})+\nu_p(k')$ که معادل است با اینکه $\nu_p(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})=1$. ابتدا دقت کنید مجدداً طبق فرض همنهشتی a,b به پیمانه p داریم : $a^{p-1}+a^{p-2}b+\cdots+b^{p-1}\overset{p}{\equiv}pa^{p-1}\overset{p}{\equiv}0$ و بنابراین $\nu_p(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})\geq 1$. حال ثابت می‌کنیم اعداد $a^{p-1},a^{p-2}b,\cdots,b^{p-1}$ یا همگی به پیمانه p^2 همنهشتند و یا دو به دو به پیمانه p^2 ناهمنهشتند :

$$a^ib^{p-i-1}\overset{p}{\equiv}a^jb^{p-j-1}\xrightarrow{\text{WLOG } i\geqslant j} a^{i-j}\overset{p}{\equiv}b^{i-j}\iff p\mid a^{i-j}-b^{i-j}$$

اما با توجه به اینکه $1\leq i-j<p$ و در نتیجه $p\nmid i-j$، با توجه به فرض استقرا که در اول ثابت کردیم نتیجه می‌گیریم اگر $p^2\mid a-b$ آنگاه همه اعضا به پیمانه p^2 همنهشتند و در غیر این صورت هر دو عضوی به پیمانه p^2 ناهمنهشتند. در حالت اول :

$$a^{p-1}+a^{p-2}b+\cdots+b^{p-1}\overset{p^2}{\equiv}pa^{p-1}\implies\nu_p(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})=1$$

در حالت دیگر نیز دقت کنید اعضا همگی به پیمانه p همچنان همنهشتند. بنابراین مجموعه اعضای $a^{p-1},a^{p-2}b,\cdots,b^{p-1}$ به پیمانه p^2 همنهشت با مجموعه $i,p+i,\cdots+p(p-1)+i$ خواهد بود که i در آن عددی بین صفر و p است. آنگاه داریم :

$$a^{p-1}+a^{p-2}b+\cdots+b^{p-1}\overset{p^2}{\equiv}(i)+(p+i)+\cdots+(p(p-1)+i)=p\cdot\frac{p(p-1)}{2}+pi=p(\frac{p(p-1)}{2}+i)$$

اما با توجه به فرد بودن p داریم : $p\mid\frac{p(p-1)}{2}$ و در نتیجه $p\nmid\frac{p(p-1)}{2}+i$ و مجدداً $\nu_p(a^{p-1}+a^{p-2}b+\cdots+b^{p-1})=1$ که اثبات قضیه را کامل می‌کند.

قضیه ۶. برای هر $p \in \mathbb{P}$ فرد و $a, c \in \mathbb{Z}$ ، اگر داشته باشیم $p \nmid ac, p \mid a+c$ آنگاه برای هر عدد طبیعی و فرد k داریم :

$$\nu_p(a^k + c^k) = \nu_p(a+c) + \nu_p(k)$$

اثبات. در صورت فرد بودن k، این قضیه حالت خاصی از قضیه چهار است، هنگامی که $b = -c$ و اثبات به پایان می‌رسد.

همانطور که مشاهده کردید، لم دو خط تنها برای p های اول قابل استفاده است و در حالت $p = 2$ کمی پیچیده تر خواهد بود. به عنوان تمرین، چهار لم زیر را برای $p = 2$ اثبات می‌کنیم :

قضیه ۷. اگر $a, b \in \mathbb{N}$ اعدادی صحیح و فرد باشند و $n \in \mathbb{N}$ آنگاه داریم :

۱. اگر n فرد باشد آنگاه : $\nu_2(a^n - b^n) = \nu_2(a-b)$.

۲. اگر n زوج باشد آنگاه $\nu_2(a^n - b^n) = \nu_2(a^2 - b^2) + \nu_2(\frac{n}{2})$.

۳. اگر a, b اعدادی فرد باشند و $a \overset{4}{\equiv} b$ آنگاه $\nu_2(a^n - b^n) = \nu_2(a-b) + \nu_2(n)$.

۴. اگر a, b اعدادی فرد باشند و $a \overset{4}{\not\equiv} b$ آنگاه $\nu_2(a^n - b^n) = \nu_2(a+b) + \nu_2(n)$.

اثبات.

۱. حکم معادل است با اینکه $0 = \nu_2(a^n - b^n) - \nu_2(a-b) = \nu_2(\frac{a^n - b^n}{a-b}) = \nu_2(a^{n-1} + ba^{n-2} + \cdots + b^{n-1})$ که با توجه به فرد بودن تعداد جملات (n) و فرد بودن هر جمله (به دلیل فرد بودن a, b) واضح است و اثبات این بخش کامل می‌شود.

۲. حکم را به استقرا روی $\nu_2(n)$ ثابت می‌کنیم. درستی حکم برای $n = 2$ بدیهیست. (چرا؟) از زوج بودن n داریم : $\nu_2(a^n - b^n) = \nu_2\left((a^2)^{\frac{n}{2}} - (b^2)^{\frac{n}{2}}\right) = \nu_2(a^2 - b^2) + \nu_2(\frac{n}{2})$. بنابراین :

$$\nu_2(\frac{n}{2}) = \nu_2\left((a^2)^{\frac{n}{2}} - (b^2)^{\frac{n}{2}}\right) - \nu_2(a^2 - b^2) = \nu_2\left(\frac{(a^2)^{\frac{n}{2}} - (b^2)^{\frac{n}{2}}}{a^2 - b^2}\right)$$

حال اگر $\frac{n}{2}$ زوج باشد، طبق فرض استقرا داریم :

$$\nu_2\left((a^2)^{\frac{n}{2}} - (b^2)^{\frac{n}{2}}\right) = \nu_2(a^4 - b^4) + \nu(\frac{n}{4}) = \nu_2(a^2 - b^2) + \nu_2(a^2 + b^2) + \nu(\frac{n}{2}) - 1$$

$$\iff \nu_2(\frac{n}{2}) = \nu_2\left((a^2)^{\frac{n}{2}} - (b^2)^{\frac{n}{2}}\right) - \nu_2(a^2 - b^2) = \nu_2(a^2 + b^2) + \nu(\frac{n}{2}) - 1 \iff \nu_2(a^2 + b^2) = 1$$

که این هم بدیهیست، زیرا برای a, b فرد، همواره $4 \nmid a^2 + b^2$. اما اگر n فرد باشد طبق قسمت اول داریم :

$$\nu_2(\frac{n}{2}) = \nu_2\left((a^2)^{\frac{n}{2}} - (b^2)^{\frac{n}{2}}\right) - \nu_2(a^2 - b^2) = 0$$

که با توجه به فرد بودن $\frac{n}{2}$ بدیهیست و اثبات این بخش کامل است.

۳. با حالت بندی روی زوجیت n و استفاده از قسمت اول و دوم، اثبات این قسمت بدیهیست.

۴. با حالت بندی روی زوجیت n و استفاده از قسمت اول و دوم، اثبات این قسمت بدیهیست.

در ادامه به تعدادی از لم ها و تعمیم های معروف و پرکاربرد لم دو خط اشاره می کنیم :

مثال ۴. فرض کنید $a, b \in \mathbb{Z}$ اعدادی صحیح و نسبت به هم اول و $n \in \mathbb{N}$ عددی طبیعی باشد به طوری که داشته باشیم $a^n - b^n \nmid n(a-b)$. آنگاه $a^n - b^n$ عامل اولی دارد که $a-b$ را عاد نمی‌کند.

راه حل. فرض خلف می‌کنیم که عوامل اول $a^n - b^n$ همگی از عوامل اول $a-b$ باشند. آنگاه برای هر عامل اول p از $a^n - b^n$، چون این عدد عامل اول $a-b$ نیز هست و همچنین چون p نمی‌تواند عامل اولی از a یا b باشد (چرا؟) طبق لم دو خط خواهیم داشت : $\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n) = \nu_p(n(a-b))$. پس عوامل اول $a^n - b^n$ زیرمجموعه عوامل اول $n(a-b)$ است و توان های عوامل اول مشترک این دو عیناً یکسانند و بنابراین $a^n - b^n \mid n(a-b)$ خواهد بود که حکم را ثابت می‌کند.

مثال ۵. برای هر $n \in \mathbb{N}$ و $a, b \in \mathbb{Z}$ ثابت کنید : $\gcd\left(\frac{a^n-b^n}{a-b}, a-b\right) = \gcd\left(n(\gcd(a,b)^{n-1}, a-b\right)$.

راه حل. کافیست ثابت کنیم برای هر $p \in \mathbb{P}$ داریم : $\nu_p(LHS) = \nu_p(RHS)$. داریم : برای محاسبه ν_p تنها در عبارت $\frac{a^n-b^n}{a-b}$ به مشکل خواهیم خورد که بنظر می‌رسد این مشکل توسط لم دو خط قابل حل باشد اما با دقت بیشتر متوجه می‌شویم که شرط $p \nmid ab$ در این سوال برقرار نیست. بنابراین باید به نحوی عوامل مشترک a, b را از سوال خارج کنیم. تنها حالت مشکل زا، حالتیست که $p \mid a, p \mid b$. در غیر این صورت مانعی برای استفاده از لم دو خط وجود ندارد. لذا فرض می کنیم همینطور باشد و $p \mid a, p \mid b$. همچنین فرض کنید $a = p^s \cdot c, b = p^t \cdot d$ که در آن بدون کم شدن از کلیت مسئله $s \geq t$ و $\gcd(p, cd) = 1$. در این صورت داریم :

$$\gcd\left(\frac{p^{ns}c^n - p^{nt}d^n}{p^s c - p^t d}, p^s c - p^t d\right) = \gcd\left(n(\gcd(p^s c, p^s d)^{n-1}, p^s c - p^s d\right)$$

$$\implies \gcd\left(p^{(n-2)t} \cdot \frac{(p^{(s-t)}c)^n - d^n}{p^(s-t)c - d}, p^(s-t)c - d\right) = \gcd\left(np^{(n-2)t} \cdot \gcd(c,d)^{n-1}, p^{s-t}c - d\right)$$

دقت کنید s, t می‌توانند صفر باشند پس این فرم، حالتی که $\gcd(a,b) = 1$ را هم پوشش می‌دهد. دو حالت را در نظر می‌گیریم :

$$i)\ \ s \neq t \implies \nu_p(p^{s-t}c - d) = 0 \implies \nu_p(RHS) = \nu_p(LHS) = 0 \quad \blacksquare$$

$$ii)\ \ s = q \implies \gcd\left(p^{(n-2)t} \cdot \frac{c^n - d^n}{c-d}, c-d\right) = \gcd\left(np^{(n-2)t} \cdot \gcd(c,d)^{n-1}, c-d\right)$$

در این حالت اگر $p \nmid c - d$ آنگاه مشابه حالت قبل داریم : $\nu_p(LHS) = \nu_p(RHS) = 0$ و مسئله حل می‌شود. در غیر این صورت داریم :

$$\nu_p(LHS) = \nu_p\left(\gcd\left(p^{(n-2)t} \cdot \frac{c^n - d^n}{c-d}, c-d\right)\right) = \min\left(\nu_p(p^{(n-2)t} \cdot \frac{c^n - d^n}{c-d}), \nu_p(c-d)\right)$$

$$\overset{\text{LTE}}{\implies} \nu_p(LHS) = \min\left((n-2)t + \nu_p(n), \nu_p(c-d)\right)$$

$$\nu_p(RHS) = \nu_p\left(\gcd\left(np^{(n-2)t} \cdot \gcd(c,d)^{n-1}, c-d\right)\right) = \min\left(\nu_p(n) + (n-2)t, \nu_p(c-d)\right)$$

$$\implies \nu_p(LHS) = \nu_p(RHS)$$

که اثبات را کامل می‌کند.

مثال ۶. **تعمیمی جزئی از لم دو خط :** برای هر عدد اول فرد $p \in \mathbb{P}, x \in \mathbb{Z}$ اگر داشته باشیم $p \mid x-1, \nu_p(n)=\alpha$ آنگاه :

$$\frac{x^n-1}{x-1} \overset{p^{\alpha+1}}{\equiv} n$$

راه حل. حکم را به استقرا روی $\nu_p(n)$ ثابت می‌کنیم. به عنوان پایه استقرا برای $\nu_p(n)=0$ داریم : (توجه کنید $x \overset{p}{\equiv} 1$)

$$\frac{x^n-1}{x-1} = 1+x+x^2+\cdots+x^{n-1} \overset{p}{\equiv} 1+1+\cdots+1 = n$$

که اثبات پایه استقرا را کامل می‌کند.حال فرض کنید حکم برای $\alpha=k$ برقرار باشد که $k \geq 0$. آنگاه $b \in \mathbb{N}$ وجود دارد به طوری که داشته باشیم $n=bp^k$. اثبات می‌کنیم حکم برای $n=bp^k+1$ نیز درست است. بنا بر فرض استقرا عدد صحیح m موجود است به طوری که داشته باشیم $\sum_{i=0}^{bp^k-1} x^i = mp^{k+1}+bp^k$. خواهیم داشت :

$$\sum_{i=0}^{bp^{k+1}-1} x^i - bp^{k+1} = \sum_{j=0}^{p-1} x^{j(bp^k)} \left(\sum_{i=0}^{bp^k-1} x^i\right) - bp^{k+1} = \sum_{j=0}^{p-1} x^{j(bp^k)} \left(mp^{k+1}+bp^k\right) - bp^{k+1}$$

$$= mp^{k+1}\sum_{j=0}^{p-1} x^{j(bp^k)} + bp^k\sum_{j=0}^{p-1} x^{j(bp^k)} - bp^{k+1} = mp^{k+1}\sum_{j=0}^{p-1} x^{j(bp^k)} + bp^k\left(\sum_{j=0}^{p-1} x^{j(bp^k)} - p\right)$$

از طرفی از بسط دوجمله‌ای نیوتن داریم :

$$\sum_{j=0}^{p-1} x^{j(bp^k)} \overset{p^2}{\equiv} \sum_{j=0}^{p-1}(cp+1)^{j(bp^k)} \overset{p^2}{\equiv} \sum_{j=0}^{p-1}\left(\sum_{i=0}^{j(bp^k)} \binom{j(bp^k)}{i}(cp)^i\right) \overset{p^2}{\equiv} \sum_{j=0}^{p-1}(1+j(bp^k)(cp))$$

$$\overset{p^2}{\equiv} \sum_{j=0}^{p-1} 1 + bcp^{k+1}\sum_{j=0}^{p-1} j \overset{p^2}{\equiv} p + bcp^{k+1}\left(\frac{p(p-1)}{2}\right) \overset{p^2}{\equiv} p + bcp^{k+2}\left(\frac{p-1}{2}\right) \overset{p^2}{\equiv} p$$

با استفاده از دو نتیجه اخیر به رابطه زیر می‌رسیم که حکم استقرا را ثابت می‌کند :

$$\sum_{i=0}^{bp^{k+1}-1} x^i - bp^{k+1} \overset{p^{k+2}}{\equiv} 0$$

مثال ۷. فرض کنید $a \in \mathbb{N}$ عددی طبیعی باشد. همچنین فرض کنید برای هر $n \in \mathbb{N}$ می‌دانیم $4(a^n+1)$ مکعب کامل یک عدد طبیعی است. ثابت کنید $a=1$.

راه حل. فرض کنید $a+1$ یک عامل اول فرد مثل p داشته باشد. آنگاه به وضوح شرایط لم دو خط برقرار است و طبق این لم برای مقادیر فرد n داریم :

$$3 \mid \nu_p(4(a^n+1)) = \nu_p(a^n+1) = \nu_p(a+1)+\nu_p(n)$$

اما واضح است که به ازای یکی از مقادیر $n=p, n=p^2$ این رابطه نادرست است. (چرا؟) پس کافیست حالتی را در نظر بگیریم که در آن $a=2^k-1$. در این صورت داریم $a^2+1=2^{2k}-2^{k+1}+2=2(2^{2k-1}-2^k+1)$. اما اگر $2^{2k-1}-2^k+1$ عامل اولی داشته باشد، از آنجا که عددی فرد است عامل اول فرد دارد. از طرفی اگر عدد a در شرایط مسئله صدق کند، a^2 نیز باید در شرایط مسئله صادق باشد (چرا؟) و بنابراین a^2+1 هم نباید عامل اول فرد داشته باشد و در نتیجه $2^{2k-1}-2^k+1=1$ که تنها مقدار $k=1$ نتیجه می‌دهد و بنابراین $a=1$ و اثبات کامل است.

مثال ۸. بزرگترین مقدار صحیح k را بیابید به طوری که داشته باشیم :

$$A = 1990^{1991^{1992}} + 1992^{1991^{1990}} \quad , \quad 1991^k \mid A$$

راه حل.

$$1991 = 11 \times 181 \quad , \quad 1990^{1991^{1992}} + 1992^{1991^{1990}} = (1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}$$

$$1991 \nmid 1992 \quad , \quad 1991 \nmid 1990 \quad , \quad 1992 \overset{1991}{\equiv} 1, 1990^{1991^2} \overset{1991}{\equiv} -1 \implies 1991 \mid 1992 + 1990^{1991^2}$$

$$\overset{\text{LTE}}{\implies} \nu_{11}\left((1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}\right) = \nu_{11}\left((1990^{1991^2}+1)+1991\right) + \nu_{11}(1991^{1990})$$

$$\nu_{11}(1991) = 1 \quad , \quad \nu_{11}(1990^{1991^2}+1) = \nu_{11}(1991) + \nu_{11}(1991^2) = 3 \quad \implies \nu_{11}\left((1990^{1991^2}+1)+1991\right) = 1$$

$$\implies \nu_{11}\left((1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}\right) = 1 + 1990 = 1991$$

$$\overset{\text{LTE}}{\implies} \nu_{181}\left((1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}\right) = \nu_{181}\left((1990^{1991^2}+1)+1991\right) + +\nu_{181}(1991^{1990})$$

$$\nu_{181}(1991) = 1 \quad , \quad \nu_{181}(1990^{1991^2}+1) = \nu_{181}(1991)+\nu_{181}(1991^2) = 3 \quad \implies \nu_{181}\left((1990^{1991^2}+1)+1991\right) = 1$$

$$\implies \nu_{181}\left((1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}\right) = 1 + 1990 = 1991$$

از طرفی بزرگترین k خواسته شده در واقع برابر با $\min(\nu_{11}(A), \nu_{181}(A))$ است و بنابراین $k = 1991$ و حل مسئله به پایان می‌رسد.

مثال ۹. فرض کنید $a, b \in \mathbb{N}$ اعدادی طبیعی باشند و داشته باشیم $a \mid b^2, b^2 \mid a^3, a^3 \mid b^4, \ldots$ ثابت کنید $a = b$.

راه حل. عدد اول دلخواه p را در نظر بگیرید. طبق روابط موجود در قضیه چهارم داریم :

$$\forall p \in \mathbb{P}, n \overset{4}{\equiv} 1 : \nu_p(b^{n+1}) \geq \nu_p(a^n) \implies (n+1)\nu_p(b) \geq n\nu_p(a) \implies n \overset{4}{\equiv} 1 : 1 + \frac{1}{n} = \frac{n+1}{n} \geq \frac{\nu_p(a)}{\nu_p(b)}$$

اما بدیهیست که داریم $\lim_{n\to\infty} 1 + \frac{1}{n} = 1$. به عبارت دیگر، با افزایش مقدار طبیعی n، مقدار حقیقی $1 + \frac{1}{n}$ از هر مقدار حقیقی بیشتر از یک‌ای کمتر می‌شود. بنابراین مقدار $\frac{\nu_p(a)}{\nu_p(b)}$ از ۱ تجاوز نمی‌کند. بنابراین برای هر عدد اول p داریم : $\nu_p(a) \leq \nu_p(b)$.
در نتیجه از قضیه چهارم نتیجه می‌شود $a \mid b$.
به همین ترتیب و به طریق مشابه داریم :

$$\forall p \in \mathbb{P}, n \overset{4}{\equiv} 3 : \nu_p(a^{n+1}) \geq \nu_p(b^n) \implies (n+1)\nu_p(a) \geq n\nu_p(b) \implies n \overset{4}{\equiv} 3 : 1 + \frac{1}{n} = \frac{n+1}{n} \geq \frac{\nu_p(b)}{\nu_p(a)}$$

اما بدیهیست که داریم $\lim_{n\to\infty} 1 + \frac{1}{n} = 1$. به عبارت دیگر، با افزایش مقدار طبیعی n، مقدار حقیقی $1 + \frac{1}{n}$ از هر مقدار حقیقی بیشتر از یک‌ای کمتر می‌شود. بنابراین مقدار $\frac{\nu_p(b)}{\nu_p(a)}$ از ۱ تجاوز نمی‌کند. بنابراین برای هر عدد اول p داریم : $\nu_p(b) \leq \nu_p(a)$.
در نتیجه از قضیه چهارم نتیجه می‌شود $b \mid a$.
در نتیجه داریم $a \mid b, b \mid a$ که نتیجه می‌دهد $a = b$ و اثبات را کامل می‌کند.

مثال ۱۰. **فرض کنید $a, b, c \in \mathbb{Q}^+$ اعدادی گویا باشند به طوری که داشته باشیم $abc = 1$. اگر اعداد $x, y, z \in \mathbb{N}$ موجود باشند به طوری که $a^x + b^y + c^z \in \mathbb{N}$ آنگاه ثابت کنید صورت فرم ساده شده a^x, b^y, c^z مربع کامل است. سپس اثبات کنید صورت فرم ساده شده کسرهای اعداد گویای a, b, c هر یک توانی کامل از یک عدد صحیح هستند.**

راه حل. فرض کنید $a = \frac{p_1}{q_1}$، $b = \frac{p_2}{q_2}$، $c = \frac{p_2}{q_2}$ که در آن $p_1, p_2, p_3, q_1, q_2, q_3$ همگی اعدادی طبیعی هستند و همچنین $\gcd(p_1, q_1) = \gcd(p_2, q_2) = \gcd(p_3, q_3) = 1$. آنگاه طبق فرض مسئله داریم :

$$\frac{{p_1}^x}{{q_1}^x} + \frac{{p_2}^y}{{q_2}^y} + \frac{{p_3}^z}{{q_3}^z} \in \mathbb{N} \iff {q_1}^x {q_2}^y {q_3}^z \mid {p_1}^x {q_2}^y {q_3}^z + {q_1}^x {p_2}^y {q_3}^z + {q_1}^x {q_2}^y {p_3}^z$$

حال چون از فرض مسئله داریم $abc = 1$، نتیجه می‌شود $p_1p_2p_3 = q_1q_2q_3$. هر عامل اول از هر یک از اعداد حال یک عامل اول دلخواه از ${q_1}^x {q_2}^y {q_3}^z$ مثل p در نظر بگیرید. ثابت می‌کنیم از $\nu_p({q_1}^x) = \nu_p({q_2}^y) = \nu_p({q_3}^z)$ دو تا برابرند و سومی برابر با صفر است. بدون کم شدن از کلیت مسئله فرض کنید $\nu_p({q_1}^x) \geq \nu_p({q_2}^y) \geq \nu_p({q_3}^z)$. (دقت کنید $\nu_p(p_1) = \nu_p(p_2) = \nu_p(p_3) = 0$)

$$\nu_p({q_1}^x {q_2}^y {p_3}^z) \geq \nu_p({q_1}^x {p_2}^y {q_3}^z) \geq \nu_p({p_1}^x {q_2}^y {q_3}^z)$$

حال بدیهیست چون $\nu_p({q_1}^x {q_2}^y {p_3}^z) \geq \nu_p({p_1}^x {q_2}^y {q_3}^z), \nu_p({q_1}^x {p_2}^y {q_3}^z) \geq \nu_p({p_1}^x {q_2}^y {q_3}^z)$ بنابراین همواره داریم :

$$\nu_p({q_1}^x {q_2}^y {p_3}^z) + \nu_p({q_1}^x {p_2}^y {q_3}^z) \geq \nu_p({p_1}^x {q_2}^y {q_3}^z)$$

اما اگر تساوی در این نامساوی رخ ندهد، طبق قضیه ۴ داریم :

$$\nu_p({q_1}^x {q_2}^y {q_3}^z) \leq \nu_p({q_1}^x {q_2}^y {p_3}^z) + \nu_p({q_1}^x {p_2}^y {q_3}^z) + \nu_p({p_1}^x {q_2}^y {q_3}^z) = \nu_p({p_1}^x {q_2}^y {q_3}^z) = \nu_p({q_2}^y {q_3}^z)$$

$$\implies \nu_p({q_1}^x) = 0 \implies \nu_p({q_2}^y) = \nu_p({q_3}^z) = 0 \implies p \nmid {q_1}^x {q_2}^y {q_3}^z$$

که به وضوح یک تناقض است. بنابراین داریم :

$$\nu_p({q_1}^x {q_2}^y {p_3}^z) + \nu_p({q_1}^x {p_2}^y {q_3}^z) = \nu_p({p_1}^x {q_2}^y {q_3}^z)$$

از طرفی از قضیه ۴ می‌دانیم :

$$\nu_p({q_1}^x {q_2}^y {p_3}^z) + \nu_p({q_1}^x {p_2}^y {q_3}^z) \geq \min(\nu_p({q_1}^x {q_2}^y {p_3}^z) + \nu_p({q_1}^x {p_2}^y {q_3}^z)) = \nu_p({q_1}^x {p_2}^y {q_3}^z)$$

بنابراین داریم :

$$\nu_p({p_1}^x {q_2}^y {q_3}^z) \geq \nu_p({q_1}^x {p_2}^y {q_3}^z)$$

همچنین از فرضی که بدون کم شدن از کلیت مسئله انجام دادیم داریم :

$$\nu_p({p_1}^x {q_2}^y {q_3}^z) \leq \nu_p({q_1}^x {p_2}^y {q_3}^z)$$

$$\implies \nu_p({p_1}^x {q_2}^y {q_3}^z) = \nu_p({q_1}^x {p_2}^y {q_3}^z) \implies \nu_p({q_1}^x) = \nu_p({q_2}^y)$$

حال دقت کنید $p \mid {q_1}^x$، $p \mid {q_2}^y$ و همچنین داشتیم $\gcd(p_1, q_1) = \gcd(p_2, q_2) = \gcd(p_3, q_3) = 1$ بنابراین نتیجه می‌شود : $p \nmid {p_1}^x$، $p \nmid {p_2}^y$. از طرفی از ابتدای مسئله داشتیم $p_1p_2p_3 = q_1q_2q_3$. در نتیجه $p \nmid q_3 \implies p \mid p_3 \implies p \mid q_1q_2q_3 \mid p_1p_2p_3$.
در نهایت داریم : $\nu_p({q_3}^z) = 0 \quad , \quad \nu_p({q_1}^x) = \nu_p({q_2}^y)$ که اثبات ادعا را کامل می‌کند. همچنین نتیجه می‌شود $\nu_p({p_3}^z) = \nu_p({q_1}^x) + \nu_p({q_2}^y) = 2\nu_p({q_1}^x)$ و بنابراین از آنجا که هر عامل اول p_1, p_2, p_3 عامل اول ${q_1}^x {q_2}^y {p_3}^z$ نیز هست، نتیجه می‌شود توان همه عوامل اول ${p_1}^x {p_2}^y {p_3}^z$ زوج هستند و بنابراین صورت اعداد گویای a^x, b^y, c^z در حالت ساده شده مربع کاملند که اثبات قسمت اول را کامل می‌کند.

برای اثبات قسمت دوم دقت کنید طبق نتایج قسمت قبل اگر p عامل اولی از (بدون کم شدن از کلیت مسئله) p_1 باشد آنگاه $p \mid p_1p_2p_3 \mid q_1q_2q_3$ و در نتیجه یکی از اعداد q_1, q_2, q_3 بر p بخش‌پذیر است. اما q_1 نمی‌تواند بر p بخش‌پذیر باشد. در نتیجه $\nu_p(q_1) = 0$ و طبق قسمت قبل

$$y\nu_p(q_2) = \nu_p({q_2}^y) = \nu_p({q_3}^z) = z\nu_p(q_3) \implies \frac{y}{\gcd(y,z)}\nu_p(q_2) = \frac{z}{\gcd(y,z)}\nu_p(q_3)$$

بنابراین $k \in \mathbb{N}$ موجود است که داشته باشیم : (چرا؟)

$$\nu_p(q_2) = k \cdot \frac{z}{\gcd(y,z)} \quad , \quad \nu_p(q_3) = k \cdot \frac{y}{\gcd(y,z)} \implies \nu_p(q_2) + \nu_p(q_3) = k \cdot \frac{y+z}{\gcd(y,z)}$$

همچنین از آنجا که $p_1p_2p_3 = q_1q_2q_3$ و p_2, p_3, q_1 نسبت به p اول هستند نتیجه می‌گیریم : $\nu_p(p_1) = \nu_p(q_2) + \nu_p(q_3)$ و در نتیجه :

$$\nu_p(q_2) + \nu_p(q_3) = k \cdot \frac{y+z}{\gcd(y,z)} = -\nu_p(p_1) \implies \frac{y+z}{\gcd(y,z)} \mid \nu_p(p_1) \quad , \quad \frac{y+z}{\gcd(y,z)} > 1$$

بنابراین p_1 توان $\frac{y+z}{\gcd(y,z)}$ اُم کامل است. با تکرار این کار برای p_2, p_3 اثبات مسئله کامل می‌شود.

تمرین‌های تکمیلی

۱. تمام اعداد طبیعی m, n را بیابید به طوری که $m^m = n^{n^n}$. (Iran MO 2014)

۲. فرض کنید $a > k$ اعدادی طبیعی باشند و همچنین $r_1 < r_2 < \cdots < r_n$ و $s_1 < s_2 < \cdots < s_n$ دنباله هایی از اعداد طبیعی باشند به طوری که :

$$(a^{r_1} + k)(a^{r_2} + k) \cdots (a^{r_n} + k) = (a^{s_1} + k)(a^{s_2} + k) \cdots (a^{s_n} + k)$$

ثابت کنید $\forall 1 \le i \le n : r_i = s_i$. (Iran MO 2018)

۳. تمام جفت های (k, n) از اعداد طبیعی را بیابید به طوری که داشته باشیم : $k! = (2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-1})$. (IMO 2019)

۴. ثابت کنید اعداد طبیعی $a_1, a_2, \cdots, a_{2018}$ موجود نیستند به طوری که اعداد

$$(a_1)^{2018} + a_2, (a_2)^{2018} + a_3, \cdots, (a_{2018})^{2018} + a_1$$

همگی توان های صحیح ۵ باشند. (Indian TST 2019)

۵. تمام اعداد صحیح k را بیابید به طوری که نامتناهی $n \in \mathbb{N}$ وجود داشته باشد که داشته باشیم $n + k \nmid \binom{2n}{n}$. (China MO 2015)

۶. فرض کنید $p \in \mathbb{P}$ عددی اول و فرد باشد و همچنین $m > 1, n$ اعدادی طبیعی باشند به طوری که $\frac{m^{pn}-1}{m^n-1}$ عددی اول باشد. آنگاه ثابت کنید $pn \mid (p-1)^n + 1$. (Turkey TST 2019)

۷. دنباله $\{a_n\}$ از اعداد طبیعی را مناسب می‌نامیم اگر به ازای هر $m, n \in \mathbb{N}$ که $m \neq n$ داشته باشیم :

$$\gcd(m, n) \mid {a_m}^2 + {a_n}^2 \quad , \quad \gcd(a_m, a_n) \mid m^2 + n^2$$

عدد طبیعی $b \in \mathbb{N}$ را kمناسب می‌نامیم هر گاه دنباله ی مناسب $\{a_n\}$ موجود باشد به طوری که $a_k = b$. آیا $k \in \mathbb{N}$ وجود دارد به طوری که دقیقا ۲۰۱۹ عدد kمناسب طبیعی موجود باشد؟ (China TST 2019)

۸. تمام اعداد طبیعی $m \ge 2$ را بیابید به طوری که برای هر $n \in \mathbb{N}$ که داشته باشیم $\frac{m}{3} \le n \le \frac{m}{2}$، رابطه $n \mid \binom{n}{m-2n}$ برقرار باشد. (IMO Shortlist 2012)

۹. فرض کنید $a \in \mathbb{N}$ عددی طبیعی باشد. برای هر $n \in \mathbb{N}$ تعریف میکنیم $a_n = 1 + a + \cdots + a^{n-1}$. فرض کنید $s, t \in \mathbb{N}$ دو عدد طبیعی متمایز باشند به طوری که اگر p عاملی اول از $s - t$ باشد آنگاه لزوما $p \mid a - 1$ برقرار باشد. ثابت کنید $\frac{a_s - a_t}{s - t} \in \mathbb{N}$. (Balkan MO Shortlist 2015)

۱۰. فرض کنید $x, y, m, n \in \mathbb{N}$ اعدادی طبیعی و بزرگتر از ۱ باشند به نحوی که داشته باشیم $\underbrace{x^{x^{\cdot^{\cdot^{x}}}}}_{m \text{ times}} = \underbrace{y^{y^{\cdot^{\cdot^{y}}}}}_{n \text{ times}}$. آیا لزوماً رابطه $m = n$ برقرار است؟ (European Mathematical Cup 2018)

۱۱. تمام جفت های (p, n) که در آنها $p \in \mathbb{P}$ عددی اول و $n \in \mathbb{N}$ عددی طبیعی است را بیابید به طوری که داشته باشیم :

$$n^{p-1} \mid (p-1)^n + 1$$

۱۲. برای هر $k \in \mathbb{N}, k > 1$، مجموعه S_k را مجموعه تمام سه تایی های (n, a, b) از اعداد طبیعی در نظر بگیرید که n عددی فرد باشد و a, b نیز اعدادی نسبت به هم اول باشند که $a + b = k$ و همچنین $n \mid a^n + b^n$ برقرار باشد. تمام مقادیر طبیعی k را بیابید به طوری که S_k مجموعه ای متناهی باشد. (Indian TST 2018)

۱۳. تمام سه تایی های (p, x, y) را بیابید به طوری که $p \in \mathbb{P}$ عددی اول باشد و $x, y \in \mathbb{N}$ اعدادی طبیعی باشند به طوری که $x^{p-1} + y, x + y^{p-1}$ هر دو توانی صحیح از p باشند. (IMO Shortlist 2014) فرض کنید $a_1, a_2, \cdots$ دنباله ای نامتناهی از اعداد طبیعی باشد. همچنین فرض کنید عدد طبیعی $N > 1$ موجود است به طوری که برای هر $n \ge N$ داریم :

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1} \in \mathbb{N}$$

ثابت کنید M طبیعی موجود است به طوری که برای هر $m \ge M$ داشته باشیم $a_m = a_{m+1}$. (IMO 2018)

۱۴. فرض کنید $a > b > 1$ اعدادی طبیعی باشند به طوری که b عددی فرد است. همچنین فرض کنید $n \in \mathbb{N}$ عددی طبیعی باشد. اگر $b^n \mid a^n - 1$ آنگاه ثابت کنید $a^b > \frac{3^n}{n}$. (China TST 2009)

۱۵. فرض کنید $m, n \in \mathbb{N}$ اعدادی طبیعی و فرد باشند که مجموعه عوامل اول یکسانی دارند. همچنین فرض کنید $m \mid n$. اگر $a \in \mathbb{N}$ عددی دلخواه باشد به طوری که $\gcd(a, m) = \gcd(a, n) = 1$، آنگاه ثابت کنید :

$$Ord_m(a) = Ord_n(a) \cdot \frac{m}{\gcd(m, a^{Ord_n(a)} - 1}$$

که در اینجا $Ord_x(y)$ برابر کوچکترین عدد طبیعی است به طوری که $y^{Ord_x(y)} \overset{x}{\equiv} 1$ برقرار باشد. (Indonesian TST 2022)