به نام خدا

راهنمایی مجموعه تمارین نظریه اعداد جلسه چهارم دوره تابستانی ۱۴۰۱

مبحث تابع ν_p و لم دوخط

۱. اگر n عددی فرد باشد، طبق لم دوخط و با توجه به اینکه توان هیچ عامل اولی در n بیشتر از یک نیست، می‌توان بیان کرد که برای هر عامل اول $x+y$ داریم :

$$3\nu_p(x+y) = \nu_p\left((x+y)^3\right) \leq \nu_p(x^n+y^n) = \nu_p(x+y) + \nu_p(n)$$

از این نامساوی به تناقض برسید. برای n زوج دقت کنید $x+y \mid (x+y)^3 \mid x^n+y^n$ و این رابطه عاد کردن را برای مقادیر زوج n نقض کنید.

۲. دقت کنید چون $y+1 \mid y^p+1$ و y^p+1 توانی از p است، $y+1$ نیز نمی‌تواند عامل اولی به غیر از p داشته باشد و بنابراین $y+1$ نیز توانی از p است. فرض کنید $y=p^t$ و با استفاده از لم دوخط و نامساوی به تناقض برسید.

۳. پاسخ مسئله مثبت است. ابتدا به عنوان یک لم ثابت کنید برای هر $a,b,n \in \mathbb{N}$ به طوری که $\gcd(a,b)=1$ و همچنین $a^n-b^n \nmid n(a-b)$، می‌توان نتیجه گرفت a^n-b^n عامل اولی دارد که $a-b$ را عاد نمی‌کند. حال عدد خواسته شده را به صورت استقرایی بسازید : فرض کنید n_i عددی فرد و خالی از مربع باشد به طوری که $2^{n_i}+1$ دقیقا i عامل اول داشته باشد. فرض کنید p عامل اول دلخواهی از n_i باشد. بدیهیست که pn_i نیز در شرط مسئله صادق خواهد بود.حال طبق لم می‌توان نتیجه گرفت $2^{pn_i}+1$ عامل اولی دارد که در $2^{n_i}+1$ موجود نبوده است. سعی کنید با اضافه کردن این عامل اول به pn_i گام استقرایی را کامل کنید. به عنوان تعمیمی از این مسئله، می‌توانید مسئله زیر را اثبات کنید :
اگر $a,b,s \in \mathbb{N}$ و $\gcd(a,b)=1$ و $a+b$ توانی از ۲ نباشد، آنگاه نامتناهی $n \in \mathbb{N}$ با دقیقا s عامل اول متمایز موجود است به طوری که $n \mid a^n+b^n$.

۴. طبق لم استفاده شده در راه حل سوال قبل، مسئله بدیهی بنظر می‌رسد اما دقت کنید که در این مسئله شرط اول بودن x,y نسبت به هم وجود ندارد. برای حل این مشکل، فرض کنید $\gcd(x,y)=d$ و همچنین $x=da, y=db, \gcd(a,b)=1$. حال با بازنویسی عبارت داده شده در فرض مسئله داریم : $2^{m-1}d^p(a^p+b^p) = d^m(a+b)^m$. اما حال در مقایسه توان‌های d به یک نامساوی بین m,p نیاز داریم. با نامساوی هولدر (و یا به استقرا) ثابت کنید $\frac{x^p+y^p}{2} \geq \left(\frac{x+y}{2}\right)^p$ و از این نتیجه بگیرید $m \geq p$. بنابراین داریم : $2^{m-1}(a^p+b^p) = d^{m-p}(a+b)^m$. حال با استفاده از لم دوخط نتیجه بگیرید $a+b$ نمی‌تواند عامل اول فرد داشته باشد. با تکمیل جزئیات مسئله اثبات را کامل کنید.

۵. فرض کنید $\gcd(x,y,z)=1$, $a=\frac{x}{z}, b=\frac{y}{z}$. آنگاه طبق فرض مسئله برای نامتناهی $n \in \mathbb{N}$ داریم : $z^n \mid x^n-y^n$. حال فرض کنید $x,y \notin \mathbb{Z}$. این معادل است با اینکه $z \neq 1$. حال فرض کنید p عامل اولی از z باشد. اگر p فرد باشد. با استفاده از لم دوخط برای نامتناهی $n \in \mathbb{N}$ داریم :

$$n \leq n\nu_p(z) = \nu_p(z^n) \leq \nu_p(x^n-y^n) = \nu_p(x-y) + \nu_p(n) \leq \nu_p(x-y) + \log_p(n)$$

و از این نامساوی به تناقض برسید. برای حالت $p=2$ به طریق مشابه و با استفاده از لم دوخط به تناقض رسیده و اثبات مسئله را کامل کنید.

۶. اگر n عددی زوج باشد، عامل اول فردی از $k+1$ در نظر بگیرید و آن را p بنامید. به عنوان یک لم ثابت کنید اگر $p \mid x+y$ آنگاه $p^k \mid x^{p^k}+y^{p^k}$. حال با جفت کردن اعداد $1,\cdots,k$ به زوج‌هایی با مجموع $k+1$ مسئله را حل کنید. برای حالتی که k عددی فرد است، عاملی اول از k انتخاب کنید و سعی کنید اثبات را مانند حالت قبل و با اندکی تغییر کامل کنید.

۷. ابتدا با بررسی‌های ابتدایی ثابت کنید $p \nmid xy$. در نتیجه واضح است $x \neq y$. فرض کنید $x^{p-1}+y=p^\alpha, x+y^{p-1}=p^\beta$. بدون کم شدن از کلیت مسئله فرض کنید $\alpha > \beta$. با استفاده از قضیه کوچک فرما نشان دهید $p \mid x+1, p \mid y+1, p \mid x-y$. از طرف دیگر با استفاده از فرض مسئله خواهیم داشت : $xp^\alpha - yp^\beta = x^p+xy-xy-y^p = x^p-y^p$. با استفاده از لم دوخط نشان دهید $\beta = 1+\nu_p(x-y)$. با استفاده از این نتیجه نشان دهید $\nu_p(y+1)=\nu_p(x-y)$. در نهایت از نامساوی زیر مقادیر ممکن را تعیین کنید :

$$p^{\nu_p(x-y)+1} = p^\beta = y^{p-1}+x > y^{p-1} \geq \left(p^{\nu_p(x-y)}-1\right)^{p-1}$$

۸. ادعا می‌کنیم معادله مذکور متناهی جواب دارد اگر و فقط اگر $a+b=3$ و یا a,b اعدادی نسبت به هم اول باشند که مجموع آنها توانی از ۲ است. ابتدا فرض کنید $a+b=3$ یا معادلاً $(a,b)=(1,2)$. در این حالت کوچکترین عامل اول n را p بنامید و ثابت کنید $p=3$. با استفاده از لم دوخط ثابت کنید $\nu_3(n)=1$ و بنابراین $n=3m, 3 \nmid m$. مجدداً فرض کنید $m \neq 1$ و کوچکترین عامل اول m را در نظر بگیرید و ثابت کنید $m=7$ و به تناقض برسید و این قسمت از ادعا اثبات می‌شود. به عنوان حالت دوم فرض کنید $\gcd(a,b)=d>1$. ثابت کنید $n=d^k$ برای هر $k \in \mathbb{N}$ به اندازه کافی بزرگ در معادله صادق است و این قسمت از ادعا نیز ثابت می‌شود. برای قسمت بعد، فرض کنید $\gcd(a,b)=1$ و $a+b$ توانی از ۲ باشد. ابتدا ثابت کنید n نمی‌تواند زوج باشد. در غیر این صورت مثل حالت اول، فرض کنید p کوچکترین عامل اول فرد n باشد. طبق شرط مسئله داریم : $p \mid a^{2n}-b^{2n}$. آنگاه ثابت کنید $p \mid a+b$ و این با شرط توان دو بودن $a+b$ در تناقض است. به عنوان قسمت پایانی ادعا، اثبات می‌کنیم اگر $\gcd(a,b)=1$ و $a+b \neq 3$ عامل اول فردی مثل p داشته باشد، آنگاه دنباله‌ای نامتناهی از اعداد موجود است که در شرط مسئله صادق باشند. ابتدا ثابت کنید $n=p$ در شرط مسئله صادق است و سپس دنباله‌ای از اعداد اول متمایز مانند $p_0,p_1,\cdots,p_n$ در نظر بگیرید به طوری که برای هر $i \leq n$ مقدار $n=p_0\cdots p_i$ در شرط مسئله صدق کند. با استفاده از لم دوخط و قضیه زیگموندی ثابت کنید همواره می‌توان عامل اول جدیدی به دنباله اضافه کرد که شرط دنباله برقرار بماند و اثبات ادعا تکمیل می‌شود.

۹. ثابت کنید S_k متناهیست اگر و تنها اگر k توانی از ۲ باشد. ابتدا فرض کنید k توانی از ۲ باشد. مجدداً مانند راه حل سوال ۸، کوچکترین عامل اول فرد n را در نظر بگیرید و آن را p بنامید. از فرض مسئله داریم $p \mid a^n+b^n$. با استفاده از لم دوخط و با توجه به اینکه $\gcd(2n,p-1)=2$ اثبات کنید $p \mid a^2+b^2$ و یا $p \mid a+b$. بنابراین S_k متناهیست. در حالتی که k عامل اول فردی مانند p داشته باشد، به کمک لم دوخط اثبات کنید نامتناهی جواب به صورت $n=p^t$ موجود است.

۱۰. ابتدا فرض کنید $p \leq n$ عددی اول باشد و $p \mid a_i - a_j$. با استفاده از شرط مسئله ثابت کنید $p \mid a_i, p \mid a_j$. با استفاده از این نتیجه ثابت کنید حداکثر $p-1$ عدد از مجموعه $a_1, \cdots, a_n$ بر p بخش‌پذیر نیستند و بنابراین حداقل $n-(p-1)$ عدد از این مجموعه بر p بخش‌پذیرند. همه این اعداد را از دنباله خارج کرده و همه آنها را بر p تقسیم کنید. ثابت کنید دنباله جدید مجددا در شرط مسئله صادق است و با استدلالی مشابه نتیجه بگیرید حداقل $n-2(p-1)$ عضو از دنباله جدید بر p بخش پذیرند. توجه کنید این نشان می‌دهد که حداقل $n-2(p-1)$ عضو از دنباله اولیه (مجموعه $a_1, \cdots, a_n$) بر p^2 بخش‌پذیر بوده‌اند. با تکرار این استدلال و با استفاده از ایده شمارش پلکانی نتیجه بگیرید $\nu_p(a_1 \cdots a_n) \geq (n-(p-1)) + (n-2(p-1)) + \cdots + \left(n - \lfloor \frac{n}{p-1} \rfloor p - 1\right)$. به عنوان یک لم ثابت کنید برای هر $p \leq \sqrt{n}$ داریم : $p^{\frac{n^2}{3p}} \leq \left(n - \lfloor \frac{n}{p-1} \rfloor p - 1\right) + \cdots + (n-2(p-1)) + (n-(p-1))$. با ضرب تمام این نامساوی‌ها در یکدیگر می‌توان نتیجه گرفت : $\prod_{\substack{p \leq \sqrt{n} \\ p \in \mathbb{P}}} p^{\frac{n^2}{3p}} \leq a_1 \cdots a_n < {a_n}^n$. از فرض اولیه مسئله نتیجه بگیرید $a_n \leq 2a_1$. بنابراین داریم : $\prod_{\substack{p \leq \sqrt{n} \\ p \in \mathbb{P}}} p^{\frac{n}{3p}} \leq \frac{1}{2} a_1$. در نهایت کافیست ثابت کنیم $c \in \mathbb{R}^+$ موجود است که داشته باشیم : $\prod_{\substack{p \leq \sqrt{n} \\ p \in \mathbb{P}}} p^{\frac{1}{p}} > n^c$. نتیجه بگیرید کافیست نشان دهیم $\forall n \in \mathbb{N} : 8^{-\frac{1}{n}}$ $c \in \mathbb{R}^+$ موجود است که $\prod_{\substack{p \leq n \\ p \in \mathbb{P}}} p^{\frac{1}{p}} > n^c$.

۱۱. به استقرا روی $\nu_p(n)$ عمل می‌کنیم. داریم : $\frac{x^n - y^n}{x-y} = \frac{x^n - y^n}{x^{\frac{n}{p}} - y^{\frac{n}{p}}} \cdot \frac{x^{\frac{n}{p}} - y^{\frac{n}{p}}}{x-y}$. با اعمال فرض استقرا و نوشتن دو کسر اخیر به صورت ترکیب خطی و باز کردن حاصل‌ضرب بدست آمده، حکم استقرا اثبات شده و اثبات کامل خواهد شد. همچنین واضح است که می‌توان پیمانه همنهشتی را به $p^{\nu_p(n)}$ تقلیل داد و در این صورت درستی لم دوخط نتیجه می‌شود.

۱۲. برای حل مسئله ابتدا کوچکترین عدد اول و یا توان عدد اول که از همه مقادیر a_i بزرگتر است را در نظر گرفته و آن را p^α بنامید که در آن $p \in \mathbb{P}, \alpha \in \mathbb{N}$ و کرانی برای مجموع a_i ها ارائه دهید. سپس دو طرف حکم مسئله را بر k دلخواه که عددی اول و یا توانی از عدد اول است تقسیم کنید. فرض کنید $1 \leq i \leq n$ وجود داشته باشد که حکم مسئله به ازای آن برقرار نباشد و در واقع داشته باشیم : $a_1 + \cdots + a_n \geq 1 + \lfloor a_i \rfloor$. در نتیجه برای هر k مناسب داریم : $\sum_{\substack{1 \leq j \leq n \\ j \neq i}} \lfloor \frac{a_j}{k} \rfloor < \left(\{\frac{a_1}{k}\} + \cdots + \{\frac{a_n}{k}\}\right) - \frac{1}{k}$. حال فرض کنید این رابطه برای هر اندیس برقرار باشد و به تناقض برسید. سپس فرض کنید برای دو اندیس متفاوت همزمان برقرار نباشد و ثابت کنید تمام a_i ها با هم برابرند.

۱۳. فرض کنید $k \in \mathbb{N}$ عددی ثابت باشد. تعریف کنید $a_n = (k)! + (2k)! + \cdots + (nk)!$. به عنوان حکم قوی‌تر، ثابت می‌کنیم دنباله $\{a_i\}_{i=1}^{\infty}$ نامتناهی عامل اول دارد. فرض کنید اینطور نباشد و S مجموعه متناهی عوامل اول این دنباله باشد. ابتدا ثابت کنید برای هر $p \in \mathbb{S}$، دنباله $\{\nu_p(a_i)\}_{i=1}^{\infty}$ کراندار نیست اگر و فقط اگر برای هر $n \in \mathbb{N}$ داشته باشیم : $\nu_p(((n+1)k)!) \geq \nu_p((nk)!)$. حال این نتیجه را بهبود بخشیده و ثابت کنید در صورتی که $\nu_p(a_n) \geq \nu_p(((n+1)k)!)$ برقرار باشد، داریم $\nu_p(a_n) = \nu_p(((n+1)k)!)$. نتیجه بگیرید از جایی به بعد توان تمام عوامل اول دنباله یا ثابت خواهند بود و یا برابر با توان همان عامل اول در $((n+1)k)!$ خواهد بود. سپس با استفاده از یک نامساوی به تناقض برسید و ثابت کنید دنباله $\{a_i\}_{i=1}^{\infty}$ باید یک عامل اول دیگر نیز داشته باشد.

تمرینات اضافه

۱. فرض خلف کنید که $k > \pi(n)$. دقت کنید $a_i \nmid \prod_{\substack{1 \leq j \leq k \\ j \neq i}} a_j \iff {a_i}^2 \nmid \prod_{1 \leq j \leq k} a_j \iff \exists p_i \in \mathbb{P} : 2\nu_{p_i}(a_i) > \sum_{1 \leq j \leq k} \nu_{p_i}(a_j)$. هر عدد از a_i ها را به p_i مربوطه متناظر کنید. طبق اصل لانه کبوتری، اندیس های $i \neq j$ وجود دارند به طوری که $p_i = p_j$. بنابراین می‌توان نتیجه گرفت :

$$\exists p \in \mathbb{P} \quad , \quad 2\nu_p(a_i) > \sum_{1 \leq s \leq k} \nu_p(a_s) \quad , \quad 2\nu_p(a_j) > \sum_{1 \leq s \leq k} \nu_p(a_s)$$

و از این رابطه به تناقض برسید.

۲. ابتدا ثابت کنید $b \geq a$. سپس فرض خلف کرده و نتیجه بگیرید $b > a$. سپس با استفاده از فرض مسئله ثابت کنید کافیست مسئله را در حالت $a \leq \frac{b}{2}$ حل کنیم. برای حل این حالت، از قضیه‌ای منتسب به شور و سیلوستر که تعمیم قضیه مشهور چیبشف است استفاده می‌کنیم. به عنوان یک لم این قضیه را بیان و اثبات می‌کنیم : برای هر $b \geq 2a$، مقدار $\binom{b}{a}$ عامل اولی بزرگتر از a دارد. در صورت صحیح بودن این لم، نتیجه می‌شود $b(b-1)\cdots(b-a+1)$ عامل اولی مثل p دارد که $p > a$. از رابطه $p \mid b(b-1)\cdots(b-a+1)$ همچنین نتیجه می‌شود که باقیمانده b در تقسیم بر p از $a-1$ بیشتر نیست. اما چون $p > a$ برقرار است، باقیمانده a در تقسیم بر p دقیقا برابر با a است و این با فرض مسئله در تناقض است که با نقض فرض خلف، اثبات مسئله را کامل می‌کند.
حال لم به کار رفته در مسئله را اثبات می‌کنیم : فرض خلف کنید که تمام عوامل اول $\binom{b}{a} = \frac{b(b-1)\cdots(b-a+1)}{a(a-1)\cdots 1}$ کمتر و یا مساوی با a باشند. حال فرض کنید برای هر $p \in \mathbb{P}, k \in \mathbb{N}$ مقادیر $B(p^k), A(p^k)$ به ترتیب برابر با تعداد پرانتز هایی از مخرج و صورت کسر اخیر باشند که بر p^k بخش‌پذیرند. ابتدا مقادیر $B(p^k), A(p^k)$ را بر حسب توابع مقدماتی محاسبه کنید و نتیجه بگیرید $B(p^k) - A(p^k)$ همواره برابر با ۰ یا ۱ است. همچنین ثابت کنید $A(p) = B(p)$. همچنین بدیهیست که برای هر $p > a$ و هر $k \in \mathbb{N}$ داریم : $A(p^k) = B(p^k) = 0$. بنابراین می‌توان نتیجه گرفت : $\binom{b}{a} = \prod_{\substack{p \in \mathbb{P} \\ p \leq a}} p^{B(p)-A(p)+B(p^2)-A(p^2)+\cdots}$. اما طبق نتایج اخیر، این مجموع محدود است. بزرگترین مقدار $k \in \mathbb{N}$ که $B(p^k) \neq 0$ را با $r(p)$ نمایش دهید.

$$\implies B(p) - A(p) + B(p^2) - A(p^2) + \cdots = B(p^2) - A(p^2) + \cdots + B(p^{r(p)}) - A(p^{r(p)}) \leq r(p) - 1$$

$$\implies \binom{b}{a} \mid \prod_{\substack{p\in\mathbb{P}\\ p\le a}} p^{r(p)-1} \iff \frac{b(b-1)\cdots(b-a+1)}{\prod_{\substack{p\in\mathbb{P}\\ p\le a}} p^{r(p)}} \mid \frac{a(a-1)\cdots 1}{\prod_{\substack{p\in\mathbb{P}\\ p\le a}} p} \implies \frac{b(b-1)\cdots(b-a+1)}{\prod_{\substack{p\in\mathbb{P}\\ p\le a}} p^{r(p)}} \le \frac{a(a-1)\cdots 1}{\prod_{\substack{p\in\mathbb{P}\\ p\le a}} p}$$

حال با استفاده از نامساوی و با توجه به اینکه $b \ge 2a$ به تناقض برسید.

۳. برای قسمت الف، توجه کنید $\frac{p}{i(p-i)} = \frac{1}{p-i} + \frac{1}{i}$. بنابراین صرفا کافیست ثابت کنیم صورت ساده شده کسر $\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}$ بر p بخش‌پذیر است. از طرفی این معادل است با اینکه ثابت کنیم $\sum_{i=1}^{\frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} \in \mathbb{Z}$ $p \mid$. با استفاده از وارون‌های ضربی اعداد موجود در مخرج و همچنین قضیه ویلسون این حکم را ثابت کنید. در قسمت ب ابتدا به عنوان یک لم بسیار پر کاربرد ثابت کنید برای هر $t \in \mathbb{N}$، اعداد صحیح $a_0, \cdots, a_t$ موجودند به طوری که برای هر $n \in \mathbb{N}$ داشته باشیم : $n^t = \sum_{i=0}^{t} a_i \binom{n}{i}$. این لم به کمک استقرای ریاضی قابل اثبات است اما حتی می‌توان ثابت کرد برای هر $1 \le i \le t$ داریم : $a_i = \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} j^t$.

حال به کمک این لم قسمت ب مسئله را اثبات می‌کنیم. دقت کنید برای هر $1 \le i \le p-1$ می‌دانیم $\frac{1}{i^2} \overset{p}{\equiv} i^{p-3} \implies i^2 \cdot i^{p-3} \overset{p}{\equiv} 1$. بنابراین مسئله در واقع معادل با این است که ثابت کنیم $p \mid \sum_{i=1}^{p-1} i^{p-3}$. حال با استفاده از لم بیان شده، فرض کنید $a_0, \cdots, a_{p-3} \in \mathbb{Z}$ اعدادی صحیح باشند به طوری که برای هر $n \in \mathbb{N}$ داشته باشیم : $n^{p-3} = \sum_{i=0}^{p-3} a_i \binom{n}{i}$. مقدار $\sum_{i=1}^{p-1} i^{p-3}$ را محاسبه کرده و با استفاده از اتحادهای ترکیبیاتی حکم قسمت ب را نتیجه بگیرید. برای قسمت ج دقت کنید داریم : $\sum_{i=1}^{\frac{p-1}{2}} ((p-1)!)^3 \frac{3i^2 p}{i^3(p-i)^3} \overset{p^2}{\equiv} \sum_{i=1}^{\frac{p-1}{2}} ((p-1)!)^3 \frac{i^3+(p-i)^3}{i^3(p-i)^3} = \sum_{i=1}^{p-1} \frac{((p-1)!)^3}{i^3} \mid p^2 \iff \sum_{i=1}^{p-1} \frac{1}{i^3} \mid p^2$. اما این مجموع به وضوح بر p بخش‌پذیر است. بنابراین کافیست ثابت کنیم : $\sum_{i=1}^{\frac{p-1}{2}} \frac{3}{i^4} = \sum_{i=1}^{\frac{p-1}{2}} \frac{3i^2}{i^6} \overset{p}{\equiv} \sum_{i=1}^{\frac{p-1}{2}} (-1)^3 \frac{3i^2}{i^3(-i)^3} \overset{p}{\equiv} \sum_{i=1}^{\frac{p-1}{2}} ((p-1)!)^3 \frac{3i^2}{i^3(p-i)^3} \mid p$.

برای تکمیل اثبات، مشابه اثبات حالت‌های قبل می‌دانیم $\sum_{i=1}^{\frac{p-1}{2}} \frac{((p-1)!)^4}{i^4} \mid p \iff \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^4} \mid p$. حال سعی کنید مشابه قسمت ب راه حل را تکمیل کنید.

در نهایت برای قسمت د با ایده‌ای مشابه قسمت‌های قبل شروع به حل مسئله می‌کنیم :

$$2\sum_{k=1}^{p-1} \frac{1}{k^u} = \sum_{k=1}^{p-1} \frac{1}{k^u} + \sum_{k=1}^{p-1} \frac{1}{k^u} = \sum_{k=1}^{p-1} \frac{1}{k^u} + \sum_{k=1}^{p-1} \frac{1}{(p-k)^u} = \sum_{k=1}^{p-1} \left(\frac{1}{k^u} + \frac{1}{(p-k)^u} \right) = \sum_{k=1}^{p-1} \frac{k^u + (p-k)^u}{k^u (p-k)^u}$$

اما حال از فرد بودن u می‌توان نتیجه گرفت :

$$2\sum_{k=1}^{p-1} \frac{1}{k^u} = \sum_{k=1}^{p-1} \frac{k^u + \left(p^u - up^{u-1}k \pm \cdots + upk^{u-1} - k^u\right)}{k^u (p-k)^u} = \sum_{k=1}^{p-1} \frac{p^u - up^{u-1}k \pm \cdots + upk^{u-1}}{k^u (p-k)^u}$$

$$= p\sum_{k=1}^{p-1} \frac{p^{u-1} - up^{u-2}k \pm \cdots + uk^{u-1}}{k^u (p-k)^u}$$

و بنابراین کافیست ثابت کنیم : $\sum_{k=1}^{p-1} \frac{p^{u-1} - up^{u-2}k \pm \cdots + uk^{u-1}}{k^u (p-k)^u} \mid p$. حال با محاسبات به پیمانه p و استفاده از قضیه فرما و ویلسون نشان دهید :

$$\sum_{k=1}^{p-1} \frac{p^{u-1} - up^{u-2}k \pm \cdots + uk^{u-1}}{k^u (p-k)^u} \overset{p}{\equiv} \sum_{k=1}^{p-1} \frac{uk^{u-1}}{(-1)^u k^{2u}} \overset{p}{\equiv} \frac{u}{(-1)^u} \sum_{k=1}^{p-1} k^{-u-1}$$

در نهایت به عنوان یک لم ثابت کنید برای هر $p \in \mathbb{P}$ که عددی اول و فرد است و هر $n \in \mathbb{N}$ به طوری که $1 \le n \le p-2$ داریم : $\sum_{i=1}^{p-1} i^n \mid p$.
برای اثبات این لم می‌توانید از ایده قسمت ب استفاده کنید و یا به کمک اتحاد نیوتن ، استقرای ریاضی و یا ابزارهای دیگری مانند ریشه اولیه آن را اثبات کنید.