Prvočísla

3. PODZIMNÍ SÉRIE — VZOROVÉ ŘEŠENÍ

Úloha 1.

Dvojka slaví narozeniny a na oslavu si pozvala prvních osm lichých prvočísel (tedy 3, 5, 7, 11, 13, 17, 19 a 23). Pomozte dvojce rozesadit všech osm hostů okolo kulatého stolu tak, aby byl rozdíl každých dvou sousedních čísel celočíselnou mocninou dvojky. *(Martin Raška)*

ŘEŠENÍ:
Úloha má dvě možná řešení. Prvním řešením je cyklicky posloupnost

$$11 \quad 3 \quad 5 \quad 13 \quad 17 \quad 19 \quad 23 \quad 7,$$

kdy rozdíly mezi sousedními čísly jsou 8, 2, 8, 4, 2, 4, 16, 4. Druhým řešením je

$$5 \quad 3 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 7$$

s rozdíly mezi sousedními čísly 2, 8, 2, 4, 2, 4, 16, 2.

POZNÁMKY:
Naprostá většina řešení byla v pořádku a ve velké části z nich byly nalezeny i obě možnosti.

(Anna Marie Minarovičová)

Úloha 2.

Žirafa přinesla Michalovi přirozené číslo $n \geq 3$. Michal si poté pro všechna lichá prvočísla $p \leq n$ zapsal číslo $n - p$ a zjistil, že mu vychází samá prvočísla. Určete, která n mu mohla žirafa přinést.
(Magdaléna Mišinová)

ŘEŠENÍ:
Úloha má jediné riešenie $n = 10$, ktoré zadaniu vyhovuje, pretože prvočísla menšie alebo rovné 10 sú 3, 5 a 7 a platí $10 - 7 = 3$, $10 - 5 = 5$ a $10 - 3 = 7$. Všimnime si, že ak $n > 10$, potom si Michal určite zapísal čísla $n - 3$, $n - 5$ a $n - 7$. Pozrieme sa na ich zvyšky po delení 3. Platí

$$n - 3 \equiv n \pmod 3,$$
$$n - 5 \equiv n - 2 \pmod 3,$$
$$n - 7 \equiv n - 1 \pmod 3.$$

Keďže číslo n môže dávať po delení 3 jedine zvyšky 0, 1 a 2, jedno z čísel $n - 3$, $n - 5$ a $n - 7$ je určite deliteľné 3. Avšak pre $n > 10$ sú čísla $n - 3$, $n - 5$ a $n - 7$ väčšie ako 3, z čoho vyplýva, že ak je niektoré z nich deliteľné 3, už nejde o prvočíslo. Preto žiadne $n > 10$ nevyhovuje zadaniu.

Už nám stačí overiť iba $3 \leq n < 10$. Keďže si Michal zapísal $n - p$ pre všetky prvočísla $p \leq n$, tak ak by bolo n prvočíslo, tak by si pre $p = n$ zapísal aj $n - n = 0$, čo nie je prvočíslo, a preto $n \neq 3, 5, 7$. Ak by bolo n tvaru $p + 1$, potom $n - p = 1$, čo opäť nie je prvočíslo, z čoho vyplýva $n \neq 4, 6, 8$. Už nám stačí iba rozobrať prípad $n = 9$, ktorý nevyhovuje, pretože pre $p = 5$ platí $9 - 5 = 4$ a to nie je prvočíslo.

Zadaniu tak vyhovuje jedine $n = 10$.

Poznámky:
Väčšina riešení postupovala podobne ako vzorové riešenie. Niektoré riešienia išli tým smerom, že hľadali prvočísla, ktoré môžu odčítať od n tak, aby vyšlo číslo s poslednou cirfrou 5, ktoré je buď prvočíslo 5, alebo číslo deliteľné číslom 5. *(Michal Pecho)*

Úloha 3.

Ben, Peťo a Zdeněk si každý mysleli prvočíslo. Zjistili, že součin jejich myšlených čísel je devatenáctkrát větší než jejich součet. Určete, jaké všechny trojice prvočísel mohli mít na mysli.
(Marian Poljak)

Řešení:
Označme myšlená prvočísla p_1, p_2 a p_3. Na jejich pořadí nezáleží. Potom dostáváme ze zadání rovnost

$$p_1 \cdot p_2 \cdot p_3 = 19 \cdot (p_1 + p_2 + p_3).$$

Na levé straně je součin tří prvočísel, a jelikož číslo 19 dělí pravou stranu, musí jedno z těchto prvočísel být 19. Bez újmy na obecnosti $p_1 = 19$. Potom lze rovnici vydělit číslem 19 a upravit

$$\begin{aligned} p_2 \cdot p_3 &= 19 + p_2 + p_3, \\ p_2 \cdot p_3 - p_2 - p_3 + 1 &= 20, \\ (p_2 - 1)(p_3 - 1) &= 20. \end{aligned}$$

Stačí se tak podívat na možné rozklady čísla 20 na dva činitele. První možnost je $20 = 20 \cdot 1$, potom pro p_2, p_3 dostáváme hodnoty 21 a 2, kde ale 21 není prvočíslo. Další možnost je $20 = 10 \cdot 2$, potom pro p_2, p_3 dostáváme hodnoty 3 a 11, což jsou prvočísla. Získáváme tak jako možné řešení trojici prvočísel 19, 11 a 3. Poslední možnost rozložení na činitele je $20 = 5 \cdot 4$, pak ale dostáváme hodnoty 6 a 5, které opět nevyhovují, jelikož 6 není prvočíslo.

Jediné možné řešení tedy je, že si Ben, Peťo a Zdeněk myslí prvočísla 19, 11 a 3.

Poznámky:
Vetšina řešení postupovala obdobně jako to vzorové. Někteří řešitelé se po vydělení číslem 19 na rovnici dívali modulo 3, došli tak správně k závěru, že jedno z prvočísel je dělitelné číslem 3 a tím pádem mu musí být rovno. Většina řešení si odnesla plný počet bodů. Menší počet bodů si pak odnesla řešení, která sice uvedla výsledek, ale ne kompletní postup, a neukázala tak, že není žádné jiné vyhovující řešení. *(Klárka Grinerová)*

Úloha 4.

Nalezněte všechny trojice prvočísel p, q, r takové, že $p^4 + q^4 + r^4 - 3$ je také prvočíslo.
(Marian Poljak)

Řešení:
Nechť $s = p^4 + q^4 + r^4 - 3$, kde s je prvočíslo.

Nejprve se podívejme na paritu s. Jelikož $s \geq 2^4 + 2^4 + 2^4 - 3 = 45$, musí s být liché prvočíslo, jelikož jediné sudé prvočíslo je 2. To ovšem znamená, že $p^4 + q^4 + r^4$ musí být sudé, a tedy právě jedno, nebo všechna tři z prvočísel p, q, r musejí být sudá.

Dále se podívejme na $s \pmod 3$. Všechna čísla mohou dávat při dělení třemi pouze zbytky 0, 1, 2. Pro jejich čtvrté mocniny pak platí

$$\begin{aligned} 1^4 &\equiv 2^4 \equiv 1 \pmod 3, \\ 0^4 &\equiv 0 \pmod 3. \end{aligned}$$

Můžeme si všimnout, že čísla nedělitelná třemi, tedy čísla dávající zbytky 1, 2 po dělení třemi, mají po umocnění na čtvrtou zbytek 1. Čísla dávající zbytek 0 při dělení třemi mají po umocnění na čtvrtou opět zbytek 0. Předpokládejme, že žádné prvočíslo z p, q, r není 3. Potom ovšem

$$p^4 + q^4 + r^4 - 3 \equiv 1 + 1 + 1 - 3 \equiv 0 \pmod 3.$$

Toto by nemohlo nastat, pokud by s bylo prvočíslo, jelikož $s > 3$, tedy s nemůže být dělitelné třemi. Alespoň jedno z čísel p, q, r tedy musí být 3.

Nakonec se podívejme na $s \pmod 5$. Všechna čísla mohou dávat při dělení pěti pouze zbytky 0, 1, 2, 3, 4. Pro jejich čtvrté mocniny pak platí

$$1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod 5,$$
$$0^4 \equiv 0 \pmod 5.$$

Jak vidíme, všechna čísla se zbytky 1, 2, 3, 4 po dělení pěti dávají po umocnění na čtvrtou zbytek 1, zatímco čísla se zbytkem 0 dávají opět zbytek 0. Předpokládejme, že žádné prvočíslo z p, q, r není 5. Potom ovšem $p^4 + q^4 + r^4 - 3 \equiv 1 + 1 + 1 - 3 \equiv 0 \pmod 5$, což nemůže nastat, jelikož $s > 5$, tedy nemůže být prvočíslo. Alespoň jedno z čísel proto p, q, r musí být 5.

Jak jsme ukázali, alespoň jedno z p, q, r musí být rovno 2, 3, 5. To ověříme dosazením

$$s = p^4 + q^4 + r^4 - 3 = 2^4 + 3^4 + 5^4 - 3 = 719,$$

což je skutečně prvočíslo. Tudíž řešením je trojice $\{p, q, r\} = \{2, 3, 5\}$.

Poznámky:
Většina řešení byla správná. Někteří řešitelé odůvodnili množinu zbytků čtvrtých mocnin po dělení pěti či třemi použitím Malé Fermatovy věty, nebo si výraz upravili na

$$(p-1)(p+1)\left(p^2+1\right) + (q-1)(q+1)\left(q^2+1\right) + (r-1)(r+1)\left(r^2+1\right),$$

a pak řešili jeho dělitelnost. *(Vendula Onderková)*

Úloha 5.

Matouš vyrábí posloupnost přirozených čísel. Jako počáteční člen zvolí nějaké přirozené $a_1 \geq 2$ a poté opakuje následující kroky: jako p_n označí nejmenšího prvočíselného dělitele čísla a_n a následně spočte $a_{n+1} = a_n + \frac{a_n}{p_n}$. Dokažte, že ať už Matouš zvolil a_1 jakkoliv, od nějakého indexu K budou všechna $n \geq K$ splňovat $a_{n+3} = 3a_n$. *(Matěj Doležálek)*

Řešení:
Nejprve dokažme, že alespoň jedno číslo v posloupnosti je sudé, konkrétně a_1 nebo a_2. Pokud je a_1 liché, jsou lichá všechna prvočísla, která jej dělí, takže i p_1 a $\frac{a_1}{p_1}$ jsou lichá a $a_2 = a_1 + \frac{a_1}{p_1}$ je sudé. Alespoň jedno z čísel a_1, a_2 je tedy sudé.

Toto sudé číslo můžeme zapsat jako $a_m = 2^q b$, kde b a q jsou kladná celá čísla a b je navíc liché. Všichni prvočíselní dělitelé lichého čísla b jsou větší než 2, takže $p_m = 2$ a

$$a_{m+1} = 2^q b + 2^{q-1} b = 3 \cdot 2^{q-1} b.$$

Nejvyšší mocnina, ve které 2 dělí a_{m+1}, se tedy zmenší o 1. Opakováním tohoto kroku $(q-1)$-krát získáme člen posloupnosti a_K, který je dělitelný 2, ale už ne 4, tedy existuje liché přirozené číslo c takové, že $a_K = 2c$.

Dále dokažme, že pro $n \geq K$ platí $a_{n+3} = 3a_n$. Pro každé $a_i = 2c$, kde c je liché (tedy i pro a_K), platí následující:

2 je nejmenší prvočíslo, takže $p_i = 2$ a $a_{i+1} = 2c + c = 3c$. Liché c nemůže být dělitelné menším prvočíslem než 3, takže $p_{i+1} = 3$ a $a_{i+2} = 3c + c = 4c$. To je sudé, z čehož plyne $p_{i+2} = 2$ a $a_{i+3} = 4c + 2c = 6c$. Pro a_i dělitelné 2, ale ne 4 tedy platí

$$a_{i+1} = \frac{3}{2}a_i, \qquad a_{i+2} = 2a_i \qquad \text{a} \qquad a_{i+3} = 3a_i.$$

Speciálně je a_{i+3} opět dělitelné 2 ale ne 4, takže $a_{i+4} = \frac{9}{2}a_i = 3a_{i+1}$ a $a_{i+5} = 6a_i = 3a_{i+2}$. Dohromady tak dostáváme, že $a_{n+3} = 3a_n$ platí pro všechna $n \in \{i, i+1, i+2\}$.

Víme, že nějaké a_K je dělitelné 2 ale ne 4, takže indukcí stejná podmínka platí pro všechna a_{K+3l}, kde l je celé nezáporné číslo. Z předchozího odstavce díky tomu platí $a_{n+3} = 3a_n$ pro n ve tvarech $K + 3l$, $K + 3l + 1$ i $K + 3l + 2$, takže skutečně $a_{n+3} = 3a_n$ pro všechna $n \geq K$.

Poznámky:
Většina řešení byla správná a postupovala velmi podobně jako vzorové řešení, body jsem strhával většinou za důkazové nedostatky. *(Tomáš Flídr)*

Úloha 6.

Určete, pro která prvočísla p jsou $\frac{p+1}{2}$ i $\frac{p^2+1}{2}$ druhé mocniny celých čísel. *(Matěj Doležálek)*

Řešení:
Mějme taková a a b, že $\frac{p+1}{2} = a^2$ a $\frac{p^2+1}{2} = b^2$. BÚNO můžeme předpokládat, že a a b jsou nezáporná. To proto, že pokud $a < 0$, vezmeme místo něj nezáporné $-a$. Všimněme si, že musí platit $p > b > a$. První nerovnost plyne z $2p^2 > p^2 + 1 = 2b^2$ pro $p > 1$, druhá z $b^2 = \frac{p^2+1}{2} > \frac{p+1}{2} = a^2$, jelikož $p > 1$.

Úpravou rovností výše dostáváme $p + 1 = 2a^2$ a $p^2 + 1 = 2b^2$, jejich rozdílem pak je

$$\begin{aligned} p^2 + 1 - p - 1 &= 2b^2 - 2a^2, \\ p\,(p-1) &= 2\,(b+a)\,(b-a)\,. \end{aligned}$$

Jelikož p je prvočíslo, musí dělit jeden z činitelů na pravé straně.

Pokud $p \mid 2$, jistě $p = 2$ a $\frac{p+1}{2} = \frac{3}{2}$, což není druhá mocnina celého čísla. Tudíž $p = 2$ není možné. Z nerovností výše navíc plyne $p > b - a > 0$, tedy p nedělí $b - a$. Zbývá proto jediná možnost, a to $p \mid b + a$. Navíc z nerovností víme $2p > b + a$, tedy dokonce $p = b + a$. Z toho už plyne $p - 1 = 2b - 2a$.

Rozdílem posledních dvou rovností získáme $1 = 3a - b$, z čehož dostáváme $b = 3a - 1$ a následně $p = 4a - 1$.

Dosadíme-li do rovnosti definující a, získáme $\frac{(4a-1)+1}{2} = a^2$, tudíž $2a = a^2$, takže $a = 2$ nebo $a = 0$. V prvním případě snadno dopočteme $p = 7$, ve druhém $p = -1$, což zjevně není možné.

Zkouškou ještě ověříme, že $p = 7$ opravdu vyhovuje. Vskutku, $\frac{7+1}{2} = 2^2$ a $\frac{7^2+1}{2} = 5^2$. Je to tedy jediné řešení.

Poznámky:
Většina řešení postupovala podobně jako vzorové řešení, odečetla rovnice a pravou stranu rozložila na součin. Lišila se ovšem tím, jak elegantně zvládla dospět k samotnému výsledku. Dost lidí zapomnělo ověřit případ $p = 2$. Za to jsem body nestrhával, ale pozor na takové drobnosti.

Někteří řešitelé pouze vyzkoušeli několik malých prvočísel a prohlásili, že 7 vyhovuje. Úloha ovšem vyžaduje i důkaz, že je to opravdu jediná možnost. Proto jsem za samotný výsledek nedával žádné body. *(Václav Janáček)*

Úloha 7.

Venďa našla prvočíslo p a přirozené číslo $n \geq 2$ taková, že $p-1$ je násobkem n a zároveň je n^6-1 násobkem p. Dokažte, že alespoň jedno z čísel $p-n$ a $p+n$ muselo být druhou mocninou celého čísla. *(Marian Poljak)*

Řešení:
Zadání nám dává dvě podmínky

$$\begin{aligned} &n \mid p-1, \\ &p \mid n^6-1 = (n+1)(n-1)(n^2+n+1)(n^2-n+1). \end{aligned}$$

Číslo p si lze z první podmínky vyjádřit jako $p = nk+1$, kde $k \in \mathbb{N}$.

Z vlastnosti prvočísel víme, že dělí-li prvočíslo součin, pak alespoň jeden z činitelů musí být daným prvočíslem dělitelný, tedy

$$p \mid n+1 \qquad \vee \qquad p \mid n-1 \qquad \vee \qquad p \mid n^2+n+1 \qquad \vee \qquad p \mid n^2-n+1.$$

Pro $k=1$ dostáváme $p = n+1$, vidíme, že $p \mid n^6-1$ a $p-n = 1 = 1^2$. Pro $k>1$ dostáváme $p = nk+1 > n+1 > n-1$, tedy musí platit $p \mid n^2 \pm n + 1$. Navíc

$$nk+1 \mid n^2 \pm n + 1 \iff nk+1 \mid n^2 \pm n + 1 - nk - 1 = n(n \pm 1 - k),$$

kde prvočíslo $nk+1$ a číslo n jsou jistě nesoudělné, tedy dostáváme $nk+1 \mid n \pm 1 - k$.

Pro $n \pm 1 - k \neq 0$ musí platit $|n \pm 1 - k| \geq nk+1$. Z podmínky $nk+1 \mid n^2 \pm n + 1$ dostáváme, že

$$n^2 \pm n + 1 \geq nk+1 \iff n(n \pm 1) \geq nk \iff n \pm 1 \geq k,$$

tedy $0 \leq |n \pm 1 - k| = n \pm 1 - k$.

Tuto nerovnost pak dosadíme a získáme

$$|n \pm 1 - k| = n \pm 1 - k \geq nk+1 \iff n(1-k) \geq 1 \mp 1 + k \geq k > 0.$$

My ovšem víme, že platí $1-k < 0$, tedy jsme došli ke sporu, z kterého můžeme usoudit, že $n \pm 1 - k = 0$ neboli $k = n \pm 1$.

Pro $k = n+1$ dostáváme $p+n = n(n+1)+1+n = (n+1)^2$ a následně pro $k = n-1$ máme $p-n = n(n-1)+1-n = (n-1)^2$, tímto je důkaz hotov.

Poznámky:
Většina došlých řešení byla správná a postupovala obdobně jako ve vzorovém řešení. Některá řešení zapomněla dostatečně zdůvodnit, proč $k = n \pm 1$. Když p dělí $n^2 \pm n + 1$ nemusí hned platit, že $p = n^2 \pm n + 1$. *(Denisa Hanušková)*

Úloha 8.

Buď p prvočíslo. Dokažte, že součin[1]

$$\prod_{k=1}^{p-1} k^{2k-p-1}$$

je přirozené číslo. *(Zdeněk Pezlar)*

[1]Symbolem $\prod$ značíme součin, například $\prod_{k=1}^{5} (2k+1) = 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11$.

Trikové řešení:
Označme součin ze zadání jako S_p. Dále si jej napíšeme jako

$$\frac{1^2 \cdot 2^4 \cdot 3^6 \cdots (p-1)^{2(p-1)}}{(1 \cdot 2 \cdots (p-1))^{p+1}} = \frac{\left(1 \cdot 2^2 \cdot 3^3 \cdots (p-1)^{(p-1)}\right)^2}{((p-1)!)^{p+1}}.$$

Čitatel tohoto zlomku je druhá mocnina výrazu, který můžeme přirozeně zapsat následovně:

$$\begin{aligned}\Big(1 \cdots (p-1)\Big) \cdot \Big(2 \cdots (p-1)\Big) \cdot \Big(3 \cdots (p-1)\Big) \cdots (p-1) \cdot 1 = \\ = (p-1)! \cdot \frac{(p-1)!}{1!} \cdot \frac{(p-1)!}{2!} \cdots \frac{(p-1)!}{(p-2)!} \cdot \frac{(p-1)!}{(p-1)!}.\end{aligned}$$

Součin S_p jsme tedy přepsali na výraz, ve kterém se vyskytuje spousta faktoriálů. Upravujme S_p dále:

$$S_p = \frac{\left((p-1)! \cdot \frac{(p-1)!}{1!} \cdot \frac{(p-1)!}{2!} \cdots \frac{(p-1)!}{(p-2)!} \cdot \frac{(p-1)!}{(p-1)!}\right)^2}{(p-1)!^{p+1}} = \frac{\left(\frac{((p-1)!)^p}{1! \cdot 2! \cdots (p-1)!}\right)^2}{(p-1)!^{p+1}} = \frac{((p-1)!)^{p-1}}{(1! \cdot 2! \cdots (p-1)!)^2}.$$

Co nám podíl s mnoha faktoriály připomíná? Kombinační čísla! Spárujeme tedy faktoriály ve jmenovateli následovně:

$$S_p = \frac{(p-1)!}{1! \cdot (p-1)!} \cdot \frac{(p-1)!}{2! \cdot (p-2)!} \cdots \frac{(p-1)!}{(p-1)! \cdot 1!}.$$

To je skoro to, co chceme. Ke spokojenosti nám ale chybí faktor p, proto si ho do každého součinu doplníme:

$$S_p = \frac{1}{p} \cdot \frac{p!}{1! \cdot (p-1)!} \cdot \frac{1}{p} \cdot \frac{p!}{2! \cdot (p-2)!} \cdots \frac{1}{p} \cdot \frac{p!}{(p-1)! \cdot 1!} = \prod_{k=1}^{p-1} \frac{\binom{p}{k}}{p}.$$

Každý z činitelů v právě získaném součinu je přirozené číslo, protože pro každé prvočíslo platí $p \mid \binom{p}{k}$. Tudíž i samotný součin S_p je přirozené číslo.

Počítací řešení, volně podle Jakuba Štěpa:
Pokud nepřijdeme na (velmi trikové) řešení výše, nejsme ještě v koncích! Můžeme se totiž obrátit na zdánlivě jednoduchou myšlenku – abychom dokázali, že S_p je přirozené číslo, stačí ukázat, že se každé prvočíslo q vyskytující se v rozkladu[2] S_p ukáže v nezáporné mocnině. Zapíšeme si S_p jako

$$S_p = \frac{\prod_{k=1}^{p-1} k^{2k}}{((p-1)!)^{p+1}}.$$

Abychom se mohli poprat s S_p, připravme si nejprve nějakou „munici“. Jako *q-valuaci* racionálního čísla $v_q(a/b)$ označme rozdíl exponentů příslušících prvočíslu q v rozkladech čísel a a b. Například $v_5(100) = 2$ a $v_3(1/9) = -2$. Připomeňme známý vzorec pro určení q-valuace faktoriálů, tzv. *Legendreův vzorec*, platný pro libovolné $N \in \mathbb{N}$:

$$v_q(N!) = \sum_{i=1}^{\infty} \left\lfloor \frac{N}{q^i} \right\rfloor.$$

Zafixujme nyní nějaké prvočíslo $q < p$. Potom q-valuace jmenovatele S_p je rovna

$$(p+1)v_q((p-1)!) = (p+1) \sum_{i=1}^{\infty} \left\lfloor \frac{p-1}{q^i} \right\rfloor.$$

[2]Prvočísla dělící jmenovatel uvažujeme v záporné mocnině.

Nyní se zamysleme nad q-valuací čitatele S_p. Zjevně ji můžeme zapsat jako $2\sum_{k=1}^{p-1} kv_q(k)$. To lze interpretovat tak, že pro každé $i \geq 1$ přispějí do součtu jednou všechna čísla pod p, jejichž q-valuace je alespoň i, takových čísel je $\left\lfloor \frac{p-1}{q^i} \right\rfloor$. Potom každé číslo k bude započítané přesně $v_q(k)$-krát. Můžeme tak psát:

$$2\sum_{k=1}^{p-1} kv_q(k) = 2\sum_{i=1}^{\infty} \sum_{t=1}^{\left\lfloor \frac{p-1}{q^i} \right\rfloor} tq^i = 2\sum_{i=1}^{\infty} q^i \frac{\left\lfloor \frac{p-1}{q^i} \right\rfloor \left(\left\lfloor \frac{p-1}{q^i} \right\rfloor + 1 \right)}{2} = \sum_{i=1}^{\infty} q^i \left\lfloor \frac{p-1}{q^i} \right\rfloor \left(\left\lfloor \frac{p-1}{q^i} \right\rfloor + 1 \right).$$

Naším cílem je ukázat, že q-valuace čitatele je alespoň tolik, co q-valuace jmenovatele. S tím cílem na mysli si uvedeme lemma ohledně necelé části[3] zlomku $\frac{p-1}{q^i}$, které nám pomůže odhadnout výše napsané číslo.

Lemma. *Pro prvočíslo p a přirozené číslo $k \nmid p$ platí*

$$\left\{ \frac{p-1}{k} \right\} \leq 1 - \frac{2}{k}.$$

Důkaz. Necelou část zlomku $\frac{p-1}{k}$ můžeme opět napsat jako zlomek se jmenovatelem k a čitatelem $c < k$. Nemůže se stát $c = k-1$, jelikož $k \nmid p$, takže $c \leq k-2$. □

Díky tomuto tvrzení odhadněme dolní celou část z $\frac{p-1}{q^i}$ následovně:

$$\left\lfloor \frac{p-1}{q^i} \right\rfloor = \frac{p-1}{q^i} - \left\{ \frac{p-1}{q^i} \right\} \geq \frac{p+1}{q^i} - 1.$$

Platí tedy nerovnost

$$\sum_{i=1}^{\infty} q^i \left\lfloor \frac{p-1}{q^i} \right\rfloor \left(\left\lfloor \frac{p-1}{q^i} \right\rfloor + 1 \right) \geq \sum_{i=1}^{\infty} q^i \left\lfloor \frac{p-1}{q^i} \right\rfloor \frac{p+1}{q^i} = (p+1) \sum_{i=1}^{\infty} \left\lfloor \frac{p-1}{q^i} \right\rfloor,$$

což je přesně q-valuace jmenovatele S_p. Exponent q v S_p je tedy nezáporný pro každé prvočíslo $q < p$. Jelikož S_p je dělitelné pouze prvočísly menšími než p, už vyplývá závěr, že S_p je vskutku přirozené. Jsme doma.

Poznámka. Z prvního uvedeného řešení plyne, že pro libovolné $n \in \mathbb{N}$ je součin

$$\prod_{k=1}^{n} k^{2k-n-1} = \prod_{k=1}^{n-1} \binom{n}{k}$$

přirozené číslo.

Poznámky:
Většina úspěšných řešení se ubírala směrem druhého vzorového řešení, vyzdvihnu zde proto řešení *Michala Janíka*, *Dominika Rigasze* a *Ivana Žemličky*, kteří se vydali trikovou cestou kombinačních čísel. Neúspěšná řešení z většiny argumentovala tím, že se každé číslo se záporným exponentem pokrátí s činiteli s exponentem kladným. Nikdo mě tímto argumentem bez užití valuací nepřesvědčil.
(Zdeněk Pezlar)

[3] *Necelá část* čísla x je číslo $\{x\} \in [0,1)$ splňující $x = \{x\} + \lfloor x \rfloor$.