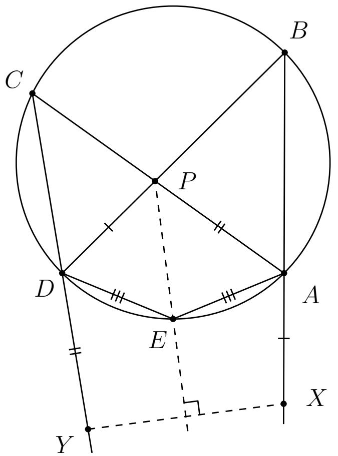
Riešenia 2. série

Úloha G2. *V tetivovom päťuholníku $ABCDE$ platí $|AE| = |ED|$. Označme P priesečník priamok AC a BD. Nech body X a Y ležia postupne na polpriamkach opačných k polpriamkam AB a DC tak, že $|AP| = |DY|$ a $|DP| = |AX|$. Ukážte, že $PE \perp XY$.*

Riešenie. Zadanie nám ponúka veľa dvojíc úsečiek s rovnakou dĺžkou. Navyše máme päť bodov na kružnici, a tak vieme poľahky prenášať uhly. To silno nabáda na to, aby sme sa pokúsili nájsť nejaké dvojice zhodných trojuholníkov.



Zhodnosť 1. $\triangle PAX \cong \triangle YDP$
Dôkaz. Zo zadania máme $|PA| = |YD|$ a $|AX| = |DP|$. Navyše vieme vďaka kružnici opísanej štvoruholníku ABCD vyuhliť $|\sphericalangle PAX| = 180° - |\sphericalangle BAC| = 180° - |\sphericalangle BDC| = |\sphericalangle YDP|$. Takže trojuholníky PAX a YDP sú zhodné podľa vety *sus*. □

Zhodnosti 2 a 3. $\triangle PAE \cong \triangle YDE$ a $\triangle PDE \cong \triangle XAE$
Dôkaz. Dokážeme len prvú z týchto zhodností - dôkaz druhej je analogický. Zo zadania vieme $|PA| = |YD|$ a $|AE| = |DE|$. Z tetivovosti štvoruholníka $ACDE$ máme navyše $|\sphericalangle PAE| = |\sphericalangle CAE| = 180° - |\sphericalangle CDE| = |\sphericalangle YDE|$. Trojuholníky PAE a YDE sú tak zhodné podľa vety *sus*. □

Tieto zhodnosti nám dávajú viacero ďalších skupín úsečiek rovnakej dĺžky. Z prvej zhodnosti máme $|PX| = |PY|$ a zo zvyšných dvoch $|PE| = |YE|$ a $|PE| = |XE|$, teda $|XE| = |YE|$. Z $|PX| = |PY|$ máme, že P leží na osi úsečky XY a z $|XE| = |YE|$ to, že E tiež leží na osi úsečky XY. To znamená, že priamka PE je osou úsečky XY, a tak je kolmá na túto úsečku, čo sme chceli ukázať.

Diskusia: Hoci sme už ukázali, čo od nás úloha vyžadovala, je potrebné sa zamyslieť, či náš dôkaz funguje v každom prípade, ktorý môže nastať. V tomto dôkaze by sa mohli pokaziť tri veci. Prvou z nich je, že body P a E by splynuli, a tak by neurčovali priamku. To sa ale nestane, keďže E je bod na kružnici opísanej päťuholníku $ABCDE$ a P vždy leží v tejto kružnici. Druhou vecou, ktorá by sa mohla pokaziť, je, že body X a Y by mohli splynúť. Ak by splynuli, tak by bol $PAXD$ (resp. $PAYD$) rovnobežník, čo by znamenalo, že priamky CA a CD by boli navzájom rovnobežné (a taktiež aj priamky BA a BD), čo nastať nemôže. Poslednou vecou, ktorá by mohla nefungovať, je, že by zlyhalo uhlenie. Našťastie ani v tomto sa dôkaz nepokazí, keďže zadanie jednoznačne popisuje poradie bodov na kružnici a na priamkach. Takže vyššie popísaný dôkaz sa nemôže „pokaziť“, a tak funguje pre všetky konfigurácie.

Poznámky opravovateľa. Konfigurácie. V geometrii sa dá najľahšie prísť o body práve vtedy, keď dôkaz nefunguje vo všetkých možných prípadoch, ktoré môžu nastať. Síce kvalitná diskusia všetkých konfigurácií môže niekedy byť dlhšia ako samotný dôkaz, je dobré spraviť ju. Často totiž býva ľahšie nestratiť tieto body v diskusii, ako získať body v iných úlohách.

(Marián Poturnay)

Úloha C2. *Dané sú prirodzené číslo n a množina A, ktorá obsahuje n rôznych zvyškov po delení n^2. Ukážte, že existuje množina B obsahujúca n rôznych zvyškov po delení n^2 taká, že aspoň polovica zvyškov po delení n^2 sa dá vyjadriť ako súčet prvku A a prvku B (brané modulo n^2).*

Riešenie. Začnime s prázdnou množinou B a budeme do nej postupne pridávať zvyšky. Zvyšky po delení n^2, ktoré sa dajú vyjadriť ako $a + b,\ a \in A, b \in B$ budeme nazývať pokryté. Keď pridáme do množiny B jeden zvyšok, niektoré zvyšky po delení n^2, ktoré doteraz neboli pokryté sa stanú pokrytými. Tieto budeme nazývať novopokryté.

Keď v množine B máme k zvyškov, tak počet pokrytých zvyškov bude najviac kn, lebo počet všetkých možných dvojíc $a + b$ je $n \cdot k$, ale niektoré výsledky sa môžu opakovať.

Lemma. *Keď máme pokrytých nanajvýš kn zvyškov, tak vieme pridať do množiny B jeden zvyšok tak, aby sme dostali aspoň $n - k$ novopokrytých zvyškov.*

Dôkaz. Zoberme si všetky možné dvojice (a, x), kde $a \in A$, x je ľubovoľný zvyšok modulo n^2. Týchto dvojíc máme n^3. Pozrime sa, koľkokrát dostaneme zo súčtu $a + x$ zvyšok, ktorý je už pokrytý. Spočítame to tak, že pre každý pokrytý zvyšok z sa pozrieme, koľkokrát sme ho mohli dostať ako $a + x \equiv z \pmod{n^2}$. Pre dané a-čko máme jednoznačne určené x. Čiže keď chceme dostať v súčte z, máme n možností pre voľbu a-čka z množiny A, následne máme určené presne jedno x, takže každý pokrytý zvyšok vytvoríme presne v n dvojiciach. Máme najviac kn pokrytých zvyškov, takže najviac kn^2 súčtov $a + x$ je rovných pokrytému zvyšku. □

Tým pádom aspoň $n^3 - kn^2 = (n-k)n^2$ súčtov $a+x$ dá nepokrytý zvyšok. Možných zvyškov x je n^2, takže z Dirichletovho princípu niektoré x sa nachádza aspoň v $n - k$ súčtoch, ktoré dajú nepokrytý zvyšok. Pre dané x-ko sú zjavne všetky súčty $a + x$ rôzne modulo n^2. Preto keď teraz pridáme zvyšok x do množiny B, tak vznikne aspoň $n - k$ novopokrytých zvyškov.

Keď budeme takto pridávať prvky do množiny B, postupne dostaneme aspoň

$$n,\ n-1,\ n-2,\ \dots,\ 1$$

novopokrytých zvyškov, takže spolu pokryjeme aspoň $\frac{n(n+1)}{2} \geq \frac{n^2}{2}$ zvyškov. Vidno, že aspoň polovicu všetkých zvyškov vieme vyjadriť ako súčet $a + b$, $a \in A$, $b \in B$.

Iné riešenie. Zvoľme množinu B náhodne a pozrime sa, koľko priemerne zvyškov bude pokrytých, teda sa bude dať zapísať ako súčet $a + b$, $a \in A$, $b \in B$. Ukážeme, že očakávaná hodnota počtu pokrytých zvyškov je $P \geq \frac{n^2}{2}$, takže pri niektorej voľbe B-čka sme museli dostať aspoň polovicu všetkých zvyškov.

Hodnotu P spočítame ako súčet očakávaných hodnôt pre jednotlivé zvyšky. Očakávaná hodnota, že jeden konkrétny zvyšok bude pokrytý je v skutočnosti pravdepodobnosť, že tento zvyšok bude pokrytý. Ukážeme, že všetky zvyšky majú rovnakú pravdepodobnosť E byť pokryté, pričom $E \geq \frac{1}{2}$, takže $P = En^2 \geq \frac{n^2}{2}$.

Každý zvyšok z vieme pokryť tak, že zoberieme ľubovoľný zvyšok $a \in A$ a k nemu máme jednoznačne určený zvyšok x_a, aby $a + x_a \equiv z$. Spočítajme pravdepodobnosť, že z nebude pokrytý. To znamená, že žiadny zo zvyškov x_a sme nevybrali do množiny B. Ku každému a-čku máme jeden zvyšok x_a, ktorý nemôžeme vybrať, lebo by sme dostali v súčte z, nazvyme ho zakázaný. Všetky zakázané zvyšky sú rôzne, ich počet je teda n. Množina B sa dá vybrať $\binom{n^2-n}{n}$ spôsobmi aby neobsahovala žiadny zakázaný zvyšok. Všetkých možných množín B je $\binom{n^2}{n}$, takže pravdepodobnosť, že zvyšok z sa nebude dať vyjadriť ako $a + b$ je

$$\frac{\binom{n^2-n}{n}}{\binom{n^2}{n}}.$$

Teraz stačí dokázať

$$\frac{\binom{n^2-n}{n}}{\binom{n^2}{n}} \leq \frac{1}{2}.$$

Rozpísaním na faktoriály a ďalšou úpravou dostaneme

$$\frac{n^2}{n^2-n} \cdot \frac{n^2-1}{n^2-n-1} \cdots \frac{n^2-n+1}{n^2-2n+1} \geq 2.$$

Urobme odhad

$$\frac{n^2-i}{n^2-n-i} = 1 + \frac{n}{n^2-n-i} \geq 1 + \frac{1}{n}.$$

Teraz máme

$$\prod_{i=0}^{n-1} \frac{n^2-i}{n^2-n-i} \geq \left(1 + \frac{1}{n}\right)^n \geq 2.$$

Posledná nerovnosť platí, lebo je známe, že funkcia $\left(1 + \frac{1}{n}\right)^n$ je rastúca a už pre $n = 1$ nerovnosť platí. Iná možnosť je priamočiaro použiť Bernoulliho nerovnosť. Dostali sme, presne čo sme chceli, takže sme hotoví.

(Tomáš Sásik a Mišo Staník)

Úloha A2. *Rozhodnite, či existujú funkcie $g, h : \mathbb{R} \to \mathbb{R}$ také, že jediná funkcia $f : \mathbb{R} \to \mathbb{R}$, ktorá pre každé $x \in \mathbb{R}$ spĺňa*

$$f(g(x)) = g(f(x)) \quad a \quad f(h(x)) = h(f(x))$$

je $f(x) = x$.

Riešenie. Ano, takové funkce existují. Zkonstruujeme si dokonce dvě vyhovující dvojice:

Řešení prvé (podle Tomáše Hully). Zvolme $g(x) = x+1$ a $h(x) = x^2$. Funkce f tedy podle zadání musí splňovat:

$$f(x+1) = f(x) + 1, \tag{1}$$

$$f(x^2) = f(x)^2. \tag{2}$$

Z (1) dostáváme indukcí pro libovolné $x \in \mathbb{R}$ a $k \in \mathbb{Z}$ vztah

$$f(x+k) = f(x) + k. \tag{3}$$

Obdobná indukce z (2) nám pro $n \in \mathbb{N}$ dá (dosazením x^{2^n})

$$f(x^{2^n}) = f(x)^{2^n}. \tag{4}$$

Dále ukážeme, že f musí být lichá. Z (2) dostáváme $f(-x)^2 = f((-x)^2) = f(x^2) = f(x)^2$, takže díky (1) máme:

$$\begin{aligned}(1 + f(-x))^2 = f(1-x)^2 = f(x-1)^2 = (f(x)-1)^2,\\ 1 + 2f(-x) + f(-x)^2 = f(x)^2 - 2f(x) + 1,\\ f(-x) = -f(x).\end{aligned}$$

Nyní si všimněme, že pro $x \geq 0$ je $f(x) = f((\sqrt{x})^2) = f(\sqrt{x})^2 \geq 0$. Podobně pro $x \leq 1$, neboli $1 - x \geq 0$, platí $1 - f(x) = 1 + f(-x) = f(1-x) \geq 0$. Je-li tedy $x \in \langle 0; 1\rangle$, pak i $f(x) \in \langle 0; 1\rangle$. Pomocí (3) můžeme vztah zobecnit: jestliže $x \in \langle k; k+1\rangle$ pro nějaké $k \in \mathbb{Z}$, pak i $f(x) \in \langle k; k+1\rangle$. Nutně tak platí $|x - f(x)| \leq 1$.

Podle (4) má platit dokonce $\left|x^{2^n} - f(x)^{2^n}\right| \leq 1$, čímž už jsme téměř hotovi, protože pro $x \geq 1$ (a tedy $f(x) \geq 1$) by v případě $x \neq f(x)$ jistě stačilo tato dvě čísla umocnit na dost velkou mocninu dvojky, aby se od sebe „vzdálila“ o více než 1. Přesněji řečeno:

$$1 \geq \left|x^{2^n} - f(x)^{2^n}\right| = |x - f(x)| \cdot \left(\sum_{i=0}^{2^n-1} x^i f(x)^{2^n-1-i}\right) \geq |x - f(x)| \cdot x^{2^n-1},$$

$$|x - f(x)| \leq x^{1-2^n}.$$

Tato nerovnost platí pro libovolně velká n, neboli pro libovolně malá x^{1-2^n}, což už vynucuje $x = f(x)$ pro všechna $x \geq 1$. Získanou rovnost pomocí (3) snadno rozšíříme na všechna reálná čísla, takže f musí být identita a naše volba funkcí g, h vyhovuje.

Řešení druhé (binárka). Je známo, že existuje bijekce mezi množinou reálných čísel $\mathbb{R}$ a množinou nekonečných posloupností nul a jedniček $\{0,1\}^{\mathbb{N}}$ (mají stejnou mohutnost). Stačí nám proto najít vhodné funkce $g', h' : \{0,1\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ splňující obdobnou podmínku pro funkce $f' : \{0,1\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$, neboli uvažovat nad čísly jako nad jím přiřazenými posloupnostmi.

Zvolíme g', h' takové, že pro libovolnou posloupnost nul a jedniček $(a_1, a_2, \dots)$ platí

$$g'((a_1, a_2, a_3, \dots)) = (0, a_1, a_2, \dots) \qquad \text{a} \qquad h'((a_1, a_2, \dots)) = (1, a_1, a_2, \dots).$$

Ukážeme, že jediná funkce f' komutující s oběma těmito funkcemi je identita.

Nechť $A \in \{0,1\}^{\mathbb{N}}$ je posloupnost začínající nulou. Pak ji můžeme vyjádřit jako $g'(B)$, kde $B \in \{0,1\}^{\mathbb{N}}$ je "A po odebrání nuly na začátku". Máme tak $f'(A) = f'(g'(B)) = g'(f'(B))$, tedy začíná-li A nulou, $f'(A)$ také začíná nulou. Zcela analogicky postupujeme pro posloupnosti začínající jedničkou, takže víme, že první čísla posloupností A a $f(A)$ se musí shodovat.

Teď můžeme indukcí ukázat, že se musí prvních n cifer A a $f'(A)$ shodovat pro libovolnou posloupnost A; už jsme to dokázali pro $n = 1$. Buď B posloupnost A, kde jsme akorát vynechali první číslo. Zároveň ale můžeme psát buď $A = g'(B)$, nebo $A = h'(B)$ (podle toho, jaká byla vynechaná cifra). V prvním případě $A = (0, B)$ a platí

$$f'(A) = f'(g'(B)) = g'(f'(B)) = (0, f'(B)).$$

Z indukčního předpokladu se prvních $n - 1$ cifer B a $f'(B)$ shoduje, takže vidíme, že se prvních n cifer A a $f'(A)$ rovněž shoduje. Pro posloupnosti začínající jedničkou akorát stačí nahradit g' za h', takže je tímto indukční krok ukončen.

Poznámky opravovateľa. Dorazilo bohužel jediné úspěšné řešení. Ostatní řešitelé volili lineární funkce, nicméně se dá poněkud komplikovaně ukázat, že žádná dvojice lineárních funkcí úlohu neřeší.

(Danil Koževnikov a Dominik Stejskal)

Úloha N2. *Nech $\mathbb{Z}_n$ značí množinu všetkých zvyškov po delení n. Pre ktoré prirodzené čísla n existuje funkcia $g : \mathbb{Z}_n \to \mathbb{Z}_n$, pre ktorú sú všetky funkcie $g(x)$, $g(x)+x$, $g(x)+2x$, $\ldots$, $g(x)+2019x$ bijekcie?* [1]

Riešenie. Ukážeme, že vyhovují právě ta n, která jsou nesoudělná s 2020!.

Pokud n je nesoudělné s 2020!, pak volby $g(x) = x$ funguje, protože funkce x, $2x$, $\ldots$, $2020x$ jsou díky nesoudělnosti bijekce $\mathbb{Z}_n$ na $\mathbb{Z}_n$.

Nyní nechť n není nesoudělné s 2020. Pro spor předpokládejme, že takové g existuje a značme $g_k(x) = g(x) + kx$.

Idea za řešením bude následovná: protože $g(x)$ i $g(x)+x$ jsou bijekce, dostáváme

$$\sum_{x\in\mathbb{Z}_n} x \equiv \sum_{x\in\mathbb{Z}_n} g(x) \equiv \sum_{x\in\mathbb{Z}_n} (g(x)+x) \pmod{n},$$

čili $0 \equiv \sum_x x = \frac{1}{2}n(n+1) \pmod{n}$, což nám dává lichost n. Podobně z bijektnosti $g(x)$, $g(x)+x$ a $g(x)+2x$ je

$$\begin{aligned} 0 &\equiv \sum_x \left[(g(x)+2x)^2 - 2\,(g(x)+x)^2 + g(x)^2\right] \pmod{n} \\ &= \sum_x 2x^2 = 2\cdot\frac{n(n+1)(2n+1)}{6}, \end{aligned}$$

čili $3 \nmid n$. Řešení bude vlastně jen dostatečně opatrným zobecněním tohoto postupu.

Lemma 1. *Pro každé nezáporné celé k a každé celé x je*

$$k!x^k = \binom{k}{0} g_k(x)^k - \binom{k}{1} g_{k-1}(x)^k + \binom{k}{2} g_{k-2}(x)^k - \cdots + (-1)^k \binom{k}{k} g_0(x)^k,$$

kde $g(x)$ považujeme za libovolné celé číslo.[2]

Dôkaz. Pro $k = 0$ je rovnost zjevná. Dále nechť $k > 0$.

Pro $x = 0$ jsou obě strany nulové, neboť díky $g_i(x) = g(x) + ix = g(x)$ platí

$$\begin{aligned} k!x^k = 0 = (1-1)^k &= \left(\binom{k}{0} - \binom{k}{1} + \cdots + (-1)^k\binom{k}{k}\right) = \\ &= \left(\binom{k}{0} - \binom{k}{1} + \cdots + (-1)^k\binom{k}{k}\right) g(x) = \\ &= \binom{k}{0} g_k(x)^k - \binom{k}{1} g_{k-1}(x)^k + \binom{k}{2} g_{k-2}(x)^k - \cdots + (-1)^k \binom{k}{k} g_0(x)^k, \end{aligned}$$

takže nadále uvažujme $x \neq 0$.

Langrangeova interpolace říká, že pokud P je polynom stupně nanejvýš m, a y_0, y_1, $\ldots$, y_m jsou různá reálné čísla, pak

$$P(y) = \sum_{i=0}^{m} P(y_i) \prod_{i\neq j} \frac{y - y_j}{y_i - y_j}.$$

[1] Pričítanie berieme ako zvyšky modulo n, napr. pre $n = 6$ je $4 + 3 = 1$.

[2] Tedy $g_i(x)$ ponecháme definováno jako $g(x) + ix$, ale $g(x)$ bereme jako novou proměnnou zcela nezávislou na x. Důvodem tohoto zavedení je fakt, že dokazujeme rovnost v $\mathbb{Z}$, ale g je bijekce na $\mathbb{Z}_n$.

(To platí proto, že na obou stranách jsou polynomy stupně nanejvýš n a, jak je jednoduchým dosazením vidět, shodují se v $m+1$ různých číslech $y_0, \ldots, y_m$. Protože dva různé polynomy stupně m se mohou shodovat nanejvýš v m bodech, musí být stejné.)

Nechť $P(y) = y^k$ a $y_i = g(x) + ix$ pro i od 0 do k. Protože $x \neq 0$, je toto $k+1$ různých čísel, takže

$$y^k = \sum_{i=0}^{k} (ix + g(x))^k \prod_{i \neq j} \frac{y - jx - g(x)}{(i-j)x}.$$

Tyto polynomy (v proměnné y) mají speciálně stejný koeficient u členu stupně k, tedy

$$1 = \sum_{i=0}^{k} \frac{(ix + g(x))^k}{x^k} \prod_{i \neq j} \frac{1}{i-j}.$$

Vynásobením obou stran $k!x^k$ získáme

$$\begin{aligned} k!x^k &= \sum_{i=0}^{k} (ix + g(x))^k k! \prod_{i \neq j} \frac{1}{i-j} \\ &= \sum_{i=0}^{k} g_i(x)^k k! \cdot \frac{1}{i!} \cdot \frac{(-1)^{k-i}}{(k-i)!} \\ &= \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{k-i} g_i(x)^k, \end{aligned}$$

což je to, co jsme chtěli. □

Nyní využijeme předpoklad sporu:

Lemma 2. *Pro každé $k \in \{0, 1, \ldots, 2019\}$ platí*

$$k! \sum_{x \in \mathbb{Z}_n} x^k \equiv 0 \pmod{n}.$$

Dôkaz. Pro $k = 0$ je tvrzení jasné. Dále nechť $k > 0$.

Označme si $S_k = \sum_{x \in \mathbb{Z}_n} x^k$. Všimněme si, že ze zadání je g_ℓ bijekce pro každé $0 \leq \ell \leq k$, tedy $\sum_{x \in \mathbb{Z}_n} g_\ell(x)^k = \sum_{x \in \mathbb{Z}_n} x^k = S_k$. Rovnost z lemmatu 1 platí určitě i v $\mathbb{Z}_n$ (kde už $g(x)$ můžeme přiřknout původní význam), sečtem přes $x \in \mathbb{Z}_n$ tedy máme

$$\begin{aligned} k! \sum_{x \in \mathbb{Z}_n} x^k = \binom{k}{0} \sum_{x \in \mathbb{Z}_n} g_k(x)^k - \binom{k}{1} \sum_{x \in \mathbb{Z}_n} g_{k-1}(x)^k + \\ + \binom{k}{2} \sum_{x \in \mathbb{Z}_n} g_{k-2}(x)^k - \cdots + (-1)^k \binom{k}{k} \sum_{x \in \mathbb{Z}_n} g_0(x)^k \\ &\equiv \binom{k}{0} S_k - \binom{k}{1} S_k + \binom{k}{2} S_k - \cdots + (-1)^k \binom{k}{k} S_k \pmod{n} \\ &\equiv S_k \left(\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k \binom{k}{k} \right) \pmod{n} \\ &\equiv S_k (1-1)^k \pmod{n} \\ &\equiv 0 \pmod{n}. \end{aligned}$$

□

Lemma 3. *Nechť p je prvočíslo a M, n čísla taková, že $p \mid n$ a*

$$M \mid 1^k + 2^k + \cdots + n^k$$

pro všechna $k \in \{0, 1, \ldots, p-1\}$. Pak[3] $\nu_p(M) < \nu_p(n)$.

Dôkaz. Z předpokladu nám plyne, že pokud f je polynom s celočíselnými koeficienty stupně nanejvýš $p-1$, pak

$$\sum_{x \in \mathbb{Z}_n} f(x) \equiv 0 \pmod{M}.$$

Speciálně tedy

$$\begin{aligned} 0 &\equiv \sum_{x=1}^{n} (x-1)(x-2)\cdots(x-(p-1)) \\ &= (p-1)! \sum_{x=1}^{n} \binom{x-1}{p-1} = (p-1)! \binom{n}{p} \pmod{M}. \end{aligned}$$

Ale pak $\nu_p(M) \leq \nu_p\left(\binom{n}{p}\right) = \nu_p(n) - 1$, kde poslední rovnost plyne díky $p \mid n$ z

$$\binom{n}{p} = \frac{n \cdot (n-1) \cdots (n-+1)}{1 \cdot 2 \cdots p}.$$ □

Nyní už zvládáme úlohu dořešit. Buď $p \leq 2020$ nejmenší prvočíslo dělící n. Z lemmatu 2 je $n \mid k! \sum_{x \in \mathbb{Z}_n} x^k$ pro všechna nezáporná celá $k \leq 2020$. Speciálně pak (díky tomu, že p je nejmenší prvočíslo soudělné s n) je $n \mid \sum_{x \in \mathbb{Z}_n} x^k$ pro všechna nezáporná celá $k \leq p-1$ (z volby p totiž pro tato k musí být $k!$ nesoudělné s n). Ale pak v lemmatu 3 můžeme položit $M = n$ a dostaneme, že $\nu_p(n) < \nu_p(n)$, což je spor.

Poznámky opravovateľa. Několik řešení přišlo se správným tipem na výsledek a konstrukcí. Důkaz, že pro jiná n to nelze, bohužel žádný nepřišel. *(Rado van Švarc)*

[3] Funkce $\nu_p(x)$ je takzvaná p-valuace, a nenulovému celému číslu x přiřazuje největší nezáporné celé a takové, že $p^a \mid x$.