Řešení 5. série

Úloha A5. *Pro všechna přirozená čísla $n \geq 2$ dokažte rovnost*

$$\lfloor \sqrt[2]{n} \rfloor + \lfloor \sqrt[3]{n} \rfloor + \cdots + \lfloor \sqrt[n]{n} \rfloor = \lfloor \log_2(n) \rfloor + \lfloor \log_3(n) \rfloor + \cdots + \lfloor \log_n(n) \rfloor .$$

Řešení. Mějmě tabulku $n \times n$ políček, kde do políčka v a-tém sloupci a b-tém řádku napíšeme číslo a^b. Vybarvíme všechna čísla, která jsou menší nebo rovna n. Na obrázku je jako příklad vyobrazena tabulka pro $n = 100$.

1	2	3	4	5	6	7	8	9	10	11	...	100	100
1	4	9	16	25	36	49	64	81	100	121	...	100^2	10
1	8	27	64	125	216	343	512	729	10^3	11^3	...	100^3	4
1	16	81	256	5^4	6^4	7^4	8^4	9^4	10^4	11^4	...	100^4	3
1	32	243	4^5	5^5	6^5	7^5	8^5	9^5	10^5	11^5	...	100^5	2
1	64	729	4^6	5^6	6^6	7^6	8^6	9^6	10^6	11^6	...	100^6	2
1	128	3^7	4^7	5^7	6^7	7^7	8^7	9^7	10^7	11^7	...	100^7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱	⋮	⋮
1	2^{100}	3^{100}	4^{100}	5^{100}	6^{100}	7^{100}	8^{100}	9^{100}	10^{100}	11^{100}	...	100^{100}	1
100	6	4	3	2	2	2	2	2	2	1	...	1	

Dvěma způsoby spočítáme počet vybarvených čtverečků, z čehož dostaneme kýženou rovnost. Zřejmě je vybarvený celý první řádek i první sloupec.

Podívejme na čísla v a-tém sloupci ($a > 1$). Poslední vybarvené políčko označme jako x-té. Potom $a^x \leq n$, ale $a^{x+1} > n$. To ale přesně znamená, že $x = \lfloor \log_a n \rfloor$. Navíc všechna čísla v předchozích řádcích jsou také vybarvena, takže v a-tém (kromě prvního, který je vybarven celý) řádku je tedy vybarveno $\lfloor \log_a n \rfloor$ čísel.

Nyní se podívejme na čísla v b-tém řádku. Opět poslední vybarvené políčko označme jako x-té, nyní platí $x^b \leq n$, ale $x^{b+1} > n$, tedy $x = \lfloor \sqrt[b]{n} \rfloor$. Stejně jako předtím, i všechna čísla v předchozích řádcích musí být vybarvena, tedy v b-tém řádku je vybarveno přesně $\lfloor \sqrt[b]{n} \rfloor$ čísel.

Celkový počet vybarvených čísel musí být stejný, ať je počítáme po řádcích nebo po sloupcích. Z toho dostáváme:

$$n + \lfloor \log_2 n \rfloor + \lfloor \log_3 n \rfloor + \cdots + \lfloor \log_n n \rfloor = n + \lfloor \sqrt[2]{n} \rfloor + \lfloor \sqrt[3]{n} \rfloor + \cdots + \lfloor \sqrt[n]{n} \rfloor$$

Po odečtení n od obou stran zbude dokazovaná rovnost.

Poznámky opravujícího. Úloha to byla spíše lehčí, což se také projevilo na počtu došlých (správných) řešení. Většina řešitelů postupovala indukcí, k čemuž úloha na první pohled docela vybízí a každý z vás se po chvíli dobral k cíli. Vzorové řešení, které poslal i Eduard Batmendijn, pěkně využívá techniku počítání dvěma způsoby a je z něj lépe vidět, co ona rovnost ze zadání vůbec znamená a proč platí. Na závěr jenom malá poznámka: pokuste se vyhnout posílání naskenovaného řešení a pokud vás k tomuto zoufalému činu něco dovede, zkontrolujte aspoň, jestli je to čitelné.

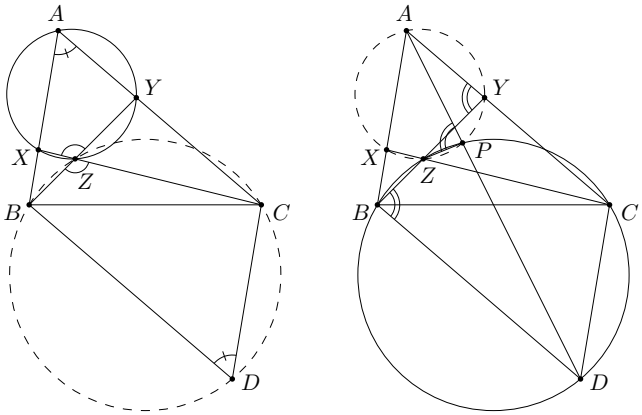
Úloha G5. *Je dán ostroúhlý trojúhelník ABC. O kružnici k řekneme, že je šikovná, pokud prochází bodem A, protíná strany AB a AC (průsečíky označíme postupně X_k, Y_k) a navíc průsečík úseček BY_k a CX_k leží na k. Dokažte, že všechny šikovné kružnice prochází pevným bodem různým od A.*

První řešení. (podle Patrika Baka)

Uvažme šikovnou kružnici k protínající strany AB, AC v bodech X, Y a označme $Z = BY \cap CX$. Ať D je takový bod, že $ABDC$ je rovnoběžník. Ze šikovnosti plyne

$$|\sphericalangle BZC| + |\sphericalangle CDB| = |\sphericalangle YZX| + |\sphericalangle BAC| = 180^\circ,$$

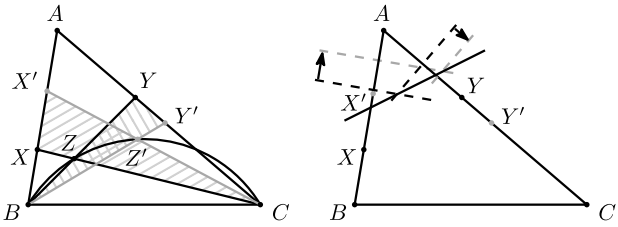
takže čtyřúhelník $BDCZ$ je tětivový (bod Z zřejmě leží uvnitř $\triangle ABC$). Označme P druhý průsečík AD a kružnice opsané čtyřúhelníku $BDCZ$. Tvrdíme, že P leží na kružnici s body A, Y a Z, a tedy je to hledaný pevný bod.



Je-li $P = Z$, není co dokazovat. Leží-li P na kratším oblouku ZC, máme $|\sphericalangle APZ| = |\sphericalangle DBZ| = |\sphericalangle AYZ|$, takže $AYPZ$ je tětivový. Leží-li P na kratším oblouku BZ, postupujeme obdobně (zkus si).

Druhé řešení. (podle Filipa Bialase)

Jako v prvním řešení si všimneme, že pro průsečík $Z = BY \cap CX$ platí $|\sphericalangle BZC| = 180^\circ - \alpha$. Uvažme na tomto oblouku kromě pevného bodu Z ještě pohyblivý bod Z' a jemu odpovídající body X', Y'. Snadno vyúhlíme $\triangle CXX' \sim \triangle BYY'$. A teď ... je zbytek zřejmý.



Když totiž hýbeme bodem Z' po kružnici tak, aby se X' vzdaloval od X konstantní rychlostí, bude se díky podobnosti konstantní rychlostí vzdalovat i bod Y' od Y. Osy stran AX,

AY se při tom budou konstantními (polovičními) rychlostmi posouvat na osy stran AX', AY' a jejich průsečík (čili střed kružnice opsané trojúhelníku $AX'Y'$) se tak bude konstantní rychlostí posouvat po přímce. Všechny šikovné kružnice pak budou kromě A procházet i obrazem A podle této přímky.

Poznámky opravujícího. Co řešení, to unikát. Není se co divit, neboť onen pevný bod má ohromnou spoustu neuvěřitelných vlastností :). Pokud tě toho o něm zajímá více, nahlédni do sborníku prvního soustředění iKS (`http://iksko.org/files/sbornik1.pdf`) na stránku 21. Jde o bod H_a.

Úloha C5. *Na kružnici leží dva bílé žetony (a žádné černé). Je povoleno provádět následující operace.*

- *Vložíme na kružnici další bílý žeton a sousední dva žetony přebarvíme (z bílé na černou a obráceně).*
- *Zbývají-li na kružnici alespoň 3 žetony, jeden bílý žeton odebereme a přebarvíme dva žetony, se kterými tento odebraný sousedil.*

Je možné dosáhnout stavu, kdy zbudou na kružnici pouze dva černé žetony a žádné bílé?

Řešení.

Učiníme krok stranou a podíváme se na trochu jinou úlohu – nazvěme ji *žlutomodrou*:

Na kružnici leží dva žetony a celá kružnice je obarvena na žluto. Je povoleno provádět následující operace.

- Vložíme na kružnici další žeton a oblouk mezi sousedními dvěma žetony přebarvíme (z žluté na modrou a obráceně).
- Zbývají-li na kružnici alespoň 3 žetony, odebereme jeden žeton sousedící se stejně barevnými oblouky, a následně přebarvíme „sloučený“ oblouk mezi žetony, se kterými tento odebraný sousedil.

Je možné dosáhnout stavu, kdy zbudou na kružnici pouze dva žetony, jeden oblouk bude obarvený na žluto a druhý na modro?

Ukážeme, že odpověď na tuto úlohu zní „ne“ a proto i na původní úlohu zní „ne“.

Souvislost původní a žlutomodré úlohy

Žetony ve žlutomodré úloze, které sousedí se stejně barevnými oblouky, budeme nazývat *bílé* a žetony, které sousedí z různě barevnými oblouky budeme nazývat *černé*. Snadno si rozmyslíme, že povolené kroky ve žlutomodré úloze za takto definovaných barev žetonů přesně odpovídají povoleným krokům v původní úloze a že počáteční stav ve žlutomodré úloze odpovídá počátečnímu stavu v původní úloze.

Pokud by tedy bylo možné v původní úloze nějakou posloupností kroků dostat stav, kde jsou dva černé žetony, mohli bychom tutéž posloupnost kroků použít ve žlutomodré úloze a dostali stav, kde je jeden oblouk žlutý a jeden modrý. K tomu, abychom ukázali, že v původní úloze taková posloupnost kroků neexistuje, stačí ukázat, že neexistuje ve žlutomodré úloze.

Řešení žlutomodré úlohy

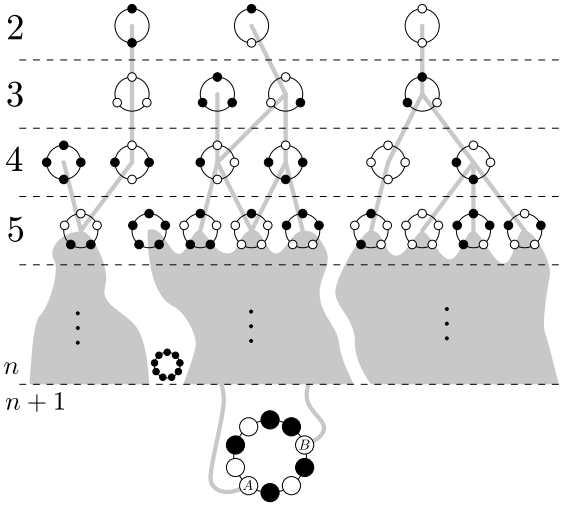
V každém kroku se při přidávání / odebírání žetonu změní (vzroste, je-li kladné) počet oblouků jedné barvy o ± 2 a opačné barvy o ∓ 1. Nicméně platí

$$\pm 2 \equiv \mp 1 \pmod 3,$$

takže můžeme říci, že modulo třemi se oba počty změní o stejné číslo. Na začátku máme 2 žluté oblouky a žádný modrý, tedy tyto počty dávají různý zbytek po dělení třemi. Díky předchozímu poznatku budou tyto počty stále nekongruentní (modulo třemi), takže není možné se dostat do stavu, kdy jsou oba počty stejné, což jsme chtěli dokázat.

Alternativní řešení

Všimneme si, že odebrání bílého žetonu je jen inverzní operace k přidání toho samého žetonu. Nakreslíme jako na obrázku po patrech všechna možná rozložení žetonů na kružnici (až na spojité posuvy) a spojíme ta rozložení, která na sebe lze jedním tahem převést.



Na prvních patrech shledáváme, že se obrázek (graf) dělí na tři oddělené větve (komponenty souvislosti). K dokončení řešení zbývá zdůvodnit, proč se tyto větve ani později nesrostou. Indukcí – předpokládejme že se větve nesrostly až do patra n, dokážeme, že se nesrostou ani po přidání patra $n+1$. V patře n zbývá ještě jedno dosud nezařazené rozložení – samé černé, nicméně to spojit větve nemůže, protože bude spojeno až na symetrii s jediným dalším rozložením. Nyní uvažme libovolné rozložení z patra $n+1$, ze kterého vedou alespoň dvě spojnice do patra n (tedy obsahuje alespoň dva bílé). Stačí ukázat, že odebráním jednoho bílého žetonu A se dostaneme do stejné větve jako odebráním jiného bílého žetonu B.

(i) Pokud A a B nesousedí, dostaneme odebráním B stejné rozložení jako když nejprve odebereme A a (dále se pohybujeme z indukce uvnitř větve) pak odebereme B a zpět přidáme A.

(ii) Pokud A a B sousedí, ale existuje bílý C, která nesousedí s A ani s B, použijeme dvakrát předchozí bod – odebráním A jsme ve stejné větvi jako odebráním C a tím jsme ve stejné větvi jako odebráním B.

(iii) Pokud A a B sousedí a žádný nesousední bílý žeton tam není, jsou to buď dva nebo tři bílé vedle sebe. První možnost vede jen do jednoho (až na symetrii) rozložení s n žetony, druhá krom toho už jen do samých černých.

Ve všech případech se napojíme jen na jednu původní větev a důkaz je hotov.

Poznámky opravujícího. První vzorové řešení je jen efektní způsob, jak popsat neměnku[1] „střídavě sčítej a odčítej počty bílých mezi jednotlivými černými a celé to počítej modulo třemi“. To

[1] *Neměnka* (cizím slovem invariant) je veličina, kterou spočítáme z kombinatorické situace a která zůstává zachována při povolených úpravách.

bylo nejčastěji vyskytující se řešení – ve skutečnosti na tuto neměnku navádí všelijaké poznatky, například:

- Počet černých žetonů je stále sudý (za tento poznatek jsem uděloval jeden bod).
- Pokud je černý žeton na bílém úseku, tak přidáním žetonu z jedné strany a odebráním žetonu z druhé strany posuneme černý žeton o tři políčka.
- Experimentálně jsme zjistili, že samé bílé je možné dostat jen když jejich počet není dělitelný třemi. Přitom z libovolného stavu umíme samé bílé dostat tak, že vždy mezi dvojičkou černých vložíme žeton do každé mezery.

Zmíněná neměnka naráží na drobnou potíž, jak se chová při celé bílé kružnici. Tímto případem se nikdo neobtěžoval zabývat, jediný řešitel, který se tomu elegantně vyhnul, byl Eduard Batmendijn, který svou neměnku opohádkoval pomocí lampáře z Malého prince.

Druhé vyobrazené řešení je inspirováno řešením Bui Truc Lama. Tento řešitel postupoval zcela originálně, bohužel však nenápadně vydával důkaz kruhem za důkaz indukcí. Tím pádem jsem nemalou dobu strávil přemítáním, zda jeho postup vede k cíli. Jak se ale můžete přesvědčit ze vzorového řešení, skutečně vede.

Úloha N5. *David zkoumal monický*[2] *polynom p s celočíselnými koeficienty. Snažil se dokázat, že tento polynom nemá celočíselný kořen tak, že chtěl najít přirozené číslo n takové, aby pro všechna $k \in \{0, \ldots, n-1\}$ platilo*

$$p(k) \not\equiv 0 \pmod{n}.$$

Zjistil ale, že takové n není možné najít. Musí už v takovém případě polynom p mít celočíselný kořen?

Řešení. Dokážeme, že správná odpověď je ne, tedy existuje monický polynom s celočíselnými koeficienty, který má celočíselný kořen modulo každé přirozené číslo, ale nemá celočíselný kořen. Konkrétně z těchto vlastností usvědčíme polynom $P(x) = (x^2+1)(x^2+7)(x^2-7)$. Tento polynom je zjevně monický a nemá celočíselné kořeny. Nyní ukážeme, že $P(x)$ má kořen modulo jakákoliv mocnina prvočísla a nakonec pomocí Čínské zbytkové věty najdeme kořen modulo libovolné přirozené číslo. Nebudeme uvažovat modulo 1, jelikož každé celé číslo je kořenem $P(x)$ modulo 1.

Důkaz existence kořenu modulo něco (volně podle Anh Dung „Tondy“ Le):

Nechť p je libovolné liché prvočíslo. Pro $p = 7$ je jistě kořenem $x = 0$. Pro všechna ostatní prvočísla použijeme Legendreova symbolu k nalezení kořenu jedné ze závorek. Jak známo platí $(\frac{-1}{p})(\frac{-7}{p}) = (\frac{7}{p})$, kde $(\frac{a}{p}) = a^{\frac{p-1}{2}}$ je právě Legendreův symbol. Pokud první dvě závorky nemají kořen modulo p, tedy -1, ani -7 nejsou kvadratické zbytky modulo p, tedy $(\frac{-1}{p}) = (\frac{-7}{p}) = -1$, máme $(\frac{7}{p}) = (-1)(-1) = 1$, čili 7 je kvadratický zbytek modulo p, takže třetí závorka má modulo p kořen. Přejděme teď k mocninám.

Dokážeme matematickou indukcí, že $P(x)$ má kořen modulo p^k, kde k je přirozené číslo a p libovolné liché prvočíslo. Pro $k = 1$ a libovolné liché prvočíslo p jsme již pro jednu ze závorek kořen našli. Nechť $n^2 + a \equiv 0 \pmod{p^k} \Leftrightarrow p^k \mid n^2 + a$, kde $a \in \{1, 7, -7\}$. Uvažme p čísel $(n + ip^k)^2 + a$, kde $i \in \{0, 1, 2, \ldots, p-1\}$. Platí

$$(n + ip^k)^2 + a \equiv n^2 + a + 2nip^k + i^2p^{2k} \equiv n^2 + a \equiv 0 \pmod{p^k}.$$

Všechna tato čísla tedy dávají po dělení p^{k+1} jeden z těchto p zbytků: $0, p^k, 2p^k, ..., (p-1)p^k$. Kdyby $(n+ip^k)^2+a \equiv (n+jp^k)^2+a \pmod{p^{k+1}}$ pro nějaká dvě různá $i, j \in \{0, 1, 2, \ldots, p-1\}$,

[2] Monický polynom je takový, který má koeficient u členu nejvyššího stupně roven jedné, tedy například polynom $x^3 + 2x^2 + 3$ je monický, zatímco polynom $2x^2 + 1$ není.

potom by $p^{k+1} \mid 2(i-j)p^k \Rightarrow p \mid 2(i-j)$, což je spor. Existuje tedy takové $i \in \{0, 1, 2, \ldots, p-1\}$, pro které $(n+ip^k)^2+a \equiv 0 \pmod{p^{k+1}}$, čili $n+ip^k$ je kořenem jedné ze závorek (podle hodnoty a) modulo p^{k+1}. Tím je důkaz indukcí ukončen.

Pro $p = 2$ budeme postupovat podobně. Z důvodů, které budou jasné později, začneme s indukcí od $k = 3$. Platí $1^2 + 7 \equiv 0 \pmod{2^3}$. Dále předpokládejme, že $2^k \mid n^2 + 7$. Potom uvažme čísla $n^2 + 7$ a $(n + 2^{k-1})^2 + 7$. Obě tato čísla jsou dělitelná 2^k - první z indukčního předpokladu, druhé z úpravy $(n + 2^{k-1})^2 + 7 \equiv n^2 + 7 + n2^k + 2^{2k-2}$. Pokud by obě tato čísla dávala stejný zbytek po dělení 2^{k+1}, muselo by $2^{k+1} \mid n2^k + 2^{2k-2}$ a tedy $2 \mid n$ (totiž $k \geq 3$, takže $2k - 2 \geq k + 1$), což je spor, protože n je z předpokladu $2^k \mid n^2 + 7$ liché.

Nyní již víme, že $P(x)$ má kořen modulo libovolná mocnina prvočísla. Nyní si uvědomíme, že ze známého tvrzení $a \equiv b \Rightarrow P(a) \equiv P(b)$ pro $P(x)$ polynom s celočíselnými koeficienty plyne, že pokud je n kořenem modulo nějaké přirozené m, tak i každé celé $q \equiv n \pmod{m}$ je kořen. Mějme tedy libovolné přirozené n. Uvažme jeho rozklad na mocniny prvočísel. Modulo každá mocnina z tohoto rozkladu již nějaký kořen $P(x)$ umíme najít. Z Čínské zbytkové věty plyne existence celého čísla r takového, že $r \equiv h_{p^k} \pmod{p^k}$, kde p^k je libovolná mocnina prvočísla p z rozkladu čísla n a h_{p^k} je odpovídající kořen $P(x)$ modulo p^k. Z toho a výše uvedného tvrzení již plyne, že $P(r) \equiv 0 \pmod{m}$. Tím je tvrzení dokázáno.

Poznámky opravujícího. Kromě zmíněného řešení dorazila ještě dvě. Rado Švarc se pasáži s indukcí vyhnul tak, že pomocí primitivního prvku[3] dokázal, že vlastnost „kvadratický nezbytek krát kv. nezbytek je kv. zbytek“ pro zbytky nesoudělné s prvočíslem p platí i modulo p^k. Liu Zhen Ning „David“ použil pro hledání kořenů modulo mocnina prvočísla *Hensel´s lifting lemma*[4]. Všechna tři řešení byla relativně krátká a s výjimkou zmíněného lemmatu nepoužívala žádnou pokročilou teorii. Proto soudím, že hlavním kamenem úrazu byl způsob nalezení vyhovujícího polynomu. Jak ho tedy najít? Chceme mít polynom co nejjednodušší, se kterým se bude dobře manipulovat a hledat jeho kořeny modulo různá čísla. Jeví se tedy výhodné hledat polynom jakožto součin závorek s malým stupněm. Zároveň nesmíme vyrobit „skutečný“ kořen, takže stupeň dva vypadá docela dobře. Pak zbývá vzpomenout si na kvadratické zbytky, nebo jinou popsanou techniku.

[3] Modulo p^k existuje zbytek takový, že jeho umocňováním dostaneme všechny zbytky nesoudělné s p, viz `http://iksko.org/files/sbornik1.pdf`

[4] `http://en.wikipedia.org/wiki/Hensel's_lemma`