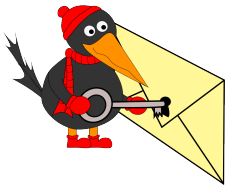
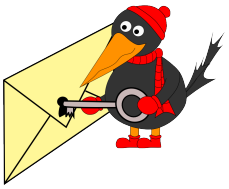


Řešení 3. série

Grupy

autor: *Vláďa a Kvágr*



Úloha 3.1. Liběnka zjistila, že má na zahradě čtyři různé druhy semínek jedné cizokrajné květiny, od každého druhu plný pytel. Druhy se jmenovaly velmi zvláštně: *antalis*, *borenas*, *ciruta* a *durum*. To ale Liběnku tolik netrápilo, spíše přemýšlela, co s nimi udělá. Nakonec ji napadlo, že by je mohla zkusit křížit a zjistit, co z nich vyroste. Pracovala velmi usilovně, až zjistila, že když zkříží druh *borenas* se sebou samým, dostane opět druh *borenas*. Tento druh dostala i po zkřížení druhu *antalis* s druhem *ciruta*. Na chvíli se zamyslela, podívala se znovu do pomocného textu a všimla si, že druhy jejích květin s operací křížení tvoří komutativní grupu! Určete, jak mohly dopadnout výsledky křížení ostatních druhů květin a ukažte, že se opravdu jedná o grupu.

Řešení. Označme naši grupu jako $(G, \otimes)$ a jednotlivé druhy písmeny a, b, c, d. Neutrální prvek označme e. Ze zadání víme, že platí $b \otimes b = b = b \otimes e$, takže podle pravého zákona o krácení dostáváme $b = e$. Dále (díky komutativitě) víme, že platí $a \otimes c = c \otimes a = b$, takže a a c jsou vůči sobě vzájemně inverzní. Neutrální prvek b je inverzní sám k sobě, a protože je inverze v grupě určena jednoznačně, musí být i d inverzní sám k sobě. Napišme si dosavadní Caleyho tabulku:

$\otimes$	a	b	c	d
a		a	b	
b	a	b	c	d
c	b	c		
d		d		b

Nyní si uvědomme, že ze zákonů o krácení plyne, že v každém řádku i sloupce se každý prvek musí vyskytnout právě jednou (pokud se totiž v řádku příslušném x vyskytne stejný prvek ve sloupcích příslušných y a z, pak $x \otimes y = x \otimes z$, tedy $y = z$), jedná se vlastně o latinský čtverec. Díky tomu můžeme snadno dopočítat $d \otimes a = c$, $a \otimes a = c$, $d \otimes c = a$, $c \otimes c = d$, zbytek plyne z komutativity (ta vlastně odpovídá souměrnosti Cayleho tabulky podle hlavní diagonály). Nyní zbývá ukázat, že naše tabulka skutečně odpovídá grupě (stačí vlastně jen ověřit asociativitu, zbytek už je jasný). Pokud se chceme vyhnout přímému výpočtu, můžeme si všimnout, že tabulka komutativní grupy $(\mathbb{Z}_4, +)$ má zcela totožnou strukturu, a protože na pojmenování prvků nijak nezáleží, musí i naše tabulka odpovídat grupě (říkáme, že tyto grupy jsou *izomorfní*).

$\otimes$	a	b	c	d
a	d	a	b	c
b	a	b	c	d
c	b	c	d	a
d	c	d	a	b

$+$	$[1]_4$	$[0]_4$	$[3]_4$	$[2]_4$
$[1]_4$	$[2]_4$	$[1]_4$	$[0]_4$	$[3]_4$
$[0]_4$	$[1]_4$	$[0]_4$	$[3]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$
$[2]_4$	$[3]_4$	$[2]_4$	$[1]_4$	$[0]_4$

Úloha 3.2. Henry se vychloubal dětem, že má skvělou novou grupovou krabičku, do které umí vložit číslo napravo, číslo nalevo a dole mu vypadne číslo, které je výsledkem grupové operace s nimi. Po chvilce však se smutkem přiznal, že každý prvek této grupy je řádu nejvýše dva. „To nevadí," utěšovala ho Bubla. „Alespoň máš jistotu, že je ta grupa komutativní!" Ukažte, že Bubla měla pravdu.

Řešení. Označme naši grupu $(G, \odot)$ a její neutrální prvek e. Pak vlastnost, že každý prvek z G má řád nejvýše 2, můžeme ekvivalentně přeformulovat jako $a \odot a = e$ pro všechna $a \in G$. Proto také $a^{-1} = a$ pro všechna $a \in G$. Pak pro libovolná $b, c \in G$ platí (s využitím asociativity)

$$(b \odot c) \odot (c \odot b) = b \odot (c \odot c) \odot b = b \odot e \odot b = b \odot b = e$$

a podobně

$$(c \odot b) \odot (b \odot c) = c \odot (b \odot b) \odot c = c \odot e \odot c = c \odot c = e.$$

Protože je v grupě inverzní prvek určen jednoznačně, dostáváme $b \odot c = (c \odot b)^{-1} = c \odot b$. Protože jsme b, c volili libovolně, je grupa $(G, \odot)$ komutativní.

Úloha 3.3. Matěj se ocitl v grupovém teleportovém bludišti skládajícím se z několika místností, každá byla označená jiným symbolem. V každé místnosti byl stejný ovládací panel obsahující symboly všech místností. Po zadání symbolu α a symbolu β by se Matěj teleportoval do místnosti se symbolem $\alpha \otimes \beta$, kde operace $\otimes$ společně s množinou symbolů místností tvoří grupu. Matěj začal v místnosti ε, která byla shodou náhod označena symbolem, jenž byl neutrálním prvkem oné grupy. Aby se v bludišti neztratil, vybral si vždy v neutrální místnosti nějaký symbol, a pak vždy zmáčkl vybraný symbol a symbol místnosti, ve které se nacházel. To opakoval tak dlouho, dokud se neteleportoval zpět do místnosti ε. Po chvilce veselého teleportování zjistil, že počet místností, které projde, než se vrátí zpět do místnosti ε (včetně té, ve které začal), nabývá pro různé symboly všech hodnot $1, 2, \ldots, 2013$. Uveďte příklad struktury, jakou mohlo bludiště mít.

Řešení. Zadání vlastně požaduje příklad grupy, ve které pro každé $k \in \{1, 2, \ldots, 2013\}$ existuje prvek řádu k. Příkladem takové grupy je aditivní grupa zbytkových tříd $(\mathbb{Z}_{2013!}, +)$, neboť pro daná k má prvek $\left[\frac{2013!}{k}\right]_{2013!}$ řád k. Stačí si totiž uvědomit, že platí

$$\underbrace{\left[\frac{2013!}{k}\right]_{2013!} + \cdots + \left[\frac{2013!}{k}\right]_{2013!}}_{k} = k \cdot \left[\frac{2013!}{k}\right]_{2013!} = [2013!]_{2013!} = [0]_{2013!},$$

což je neutrální prvek naší grupy, a že pro $n \in \mathbb{N}$, $n < k$ platí

$$\underbrace{\left[\frac{2013!}{k}\right]_{2013!} + \cdots + \left[\frac{2013!}{k}\right]_{2013!}}_{n} = n \cdot \left[\frac{2013!}{k}\right]_{2013!} = \left[n \cdot \frac{2013!}{k}\right]_{2013!} \neq [0]_{2013!},$$

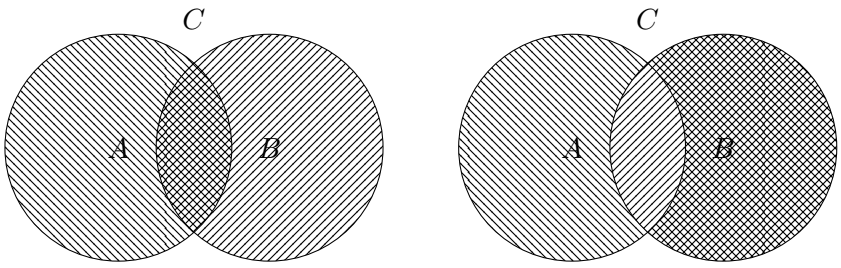
neboť $0 < n \cdot \frac{2013!}{k} < 2013!$.

Úloha 3.4. Ňouma si připravil pro Koumu zapeklitý příklad. „Koumo, myslím si konečnou n-prvkovou množinu X. Dokaž, že $(P(X), \div)$ je grupa a urči počet všech jejích podgrup!" „Hmm, ale co znamenají ty symboly?" „To je jednoduché, $P(X)$ je množina všech podmnožin množiny X a $\div$ je symetrický rozdíl (pro libovolné množiny A, B je definován vztahem $A \div B = (A \cup B) \setminus (A \cap B)$)." Koumu to ale příliš neuspokojilo. „Vždyť je to hrozně těžké!" „Možná by se ti k tomu mohla hodit tzv. Bellova čísla," slitoval se nad ním Ňouma. Pomozte Koumovi splnit jeho úkol.

Řešení. Nejprve ukažme, že jde o grupu. Operace je zřejmě uzavřená, protože sjednocováním a průnikem podmnožim X může vzniknout opět jedině podmnožina X. Dále asociativita je zřejmá, neboť $(A \div B) \div C$ je množina všech prvků ležících buď pouze v jedné z množin nebo ve všech třech a tato vlastnost zřejmě nezávisí na pořádí operace (z toho je zároveň zřejmá i komutativita). Neutrálním prvkem je zřejmě prázdná množina a inverzním prvkem ke každému prvku je prvek sám ($A \div A = \varnothing$).
Nyní dokažme důležitou vlastnost symetrického rozdílu.

Lemma. Nechť $A, B, C \subseteq X$ a $A \div B = C$. Pak $B \div C = A$.

Důkaz. Nejlépe je to vidět z následujících obrázků:



Zde vždy levý z operandů je šrafován opačně než pravý a výsledek operace je vše, co je vyšrafováno jen jedním způsobem. □

Nyní tedy spočítejme všechny podgrupy. Díky výše uvedenému lemmatu platí, že pokud do nějaké množiny $P \subset P(X)$ uzavřené na operaci $\div$ vložíme prvek $A \in P(X) \setminus P$ a přidáme $A \div K$ pro každé $K \in P$, bude nově vzniklá množina opět uzavřená na $\div$. (Toto neplatí obecně. Například při sčítání na celých číslech můžeme do množiny obsahující pouze 0 – což je podgrupa – přidat číslo 1 (a $1 = 1 + 0$), ale určitě se pak nebude jednat o grupu.) Zároveň je zřejmé, že každou podgrupu lze získat postupným přidáváním prvků (počínaje přidáním do prázdné množiny) tímto způsobem. Množinu podmnožin X, které jsme „postupně přidávali“, než nám vznikla požadovaná podgrupa, nazveme elementárním výběrem. Je zřejmé, že podgrupa je určena některým svým elementárním výběrem a počet prvků podgrupy a počet prvku elementárního výběru závisí pouze jedno na druhém. Pak tedy platí následující rovnost

$$S = 1 + \sum_{i=1}^{n} \frac{\alpha_i}{\beta_i},$$

kde S je počet všech podgrup, n počet prvků X, α_i je počet všech možných elementárníh výběrů o i prvcích a β_i je počet všech elementárních výběrů, které přísluší stejné podgrupě. (Elementární výběr nemůže mít více prvků než n, protože počet prvků podgrupy závisí pouze na počtu prvků el. výběru a pokud budeme vybírat postupně všechny jednoprvkové podmnožiny X, získáme nakonec elementární výběr o n prvcích udávající podgrupu, jež je přímo rovna celé grupě.)
Nyní dokažme, že

$$\alpha_i = (2^n - 2^0)(2^n - 2^1)(2^n - 2^2)\dots(2^n - 2^{i-1})$$
$$\beta_i = (2^i - 2^0)(2^i - 2^1)(2^i - 2^2)\dots(2^i - 2^{i-1})$$

Platnost druhého vztahu plyne bezprostředně z prvního, pro $n = i$ jde o stejné číslo. První vztah dokažme matematickou indukcí:

Pro $i = 1$ lze vybrat libovolnou neprázdnou podmnožinu X a je to také jediný prvek, který vybíráme. Neprázdných podmnožin je právě $2^n - 1$.
Nyní předpokládejme, že vztah platí pro $i = k$ a ukažme, že platí pro $i = k + 1$. Využijme našeho „přidávání“. Přidáme do elementárního výběru jeden prvek A a tudíž se počet prvků podgrupy zdvojnásobí (pro každé $K \in P$ přidáme $K \div A$). Pro $i = 1$ je počet prvků podgrupy 2 (prázdná množina a daný prvek), a tedy opět dle matematické indukce je počet prvků grupy s elementárním výběrem o k prvcích roven 2^k. Tedy pro přidávání vybíráme z $2^n - 2^k$ podmnožin X, které ještě v podgrupě neleží. Výsledný počet podgrup s elementárním výběrem o $k+1$ prvcích je tedy $(2^n - 2^k)$-krát větší, což jsme přesně chtěli dokázat.
Na závěr drobná omluva za poznámku o Bellových číslech. Naše původní řešení využívalo tuto znalost, ale nakonec se ukázalo býti chybným.

Úloha 3.5. V Lenošíně se s tradiční podzimní výrobou čísel příliš nenadřou. Proto mají v Hloupětíně poté tolik práce, aby čísla upravili a udělali z nich čísla celá. Nedávno přišel do Hloupětína zlomek $\frac{(\sqrt[3]{2}+\sqrt[3]{4})^n}{\sqrt[3]{2}+\sqrt[3]{4}+1}$. Najděte alespoň jedno přirozené číslo n, které mohou Hloupětínští použít, aby ze zlomku udělali celé číslo.

Řešení. Pro $n = 3$ dostáváme

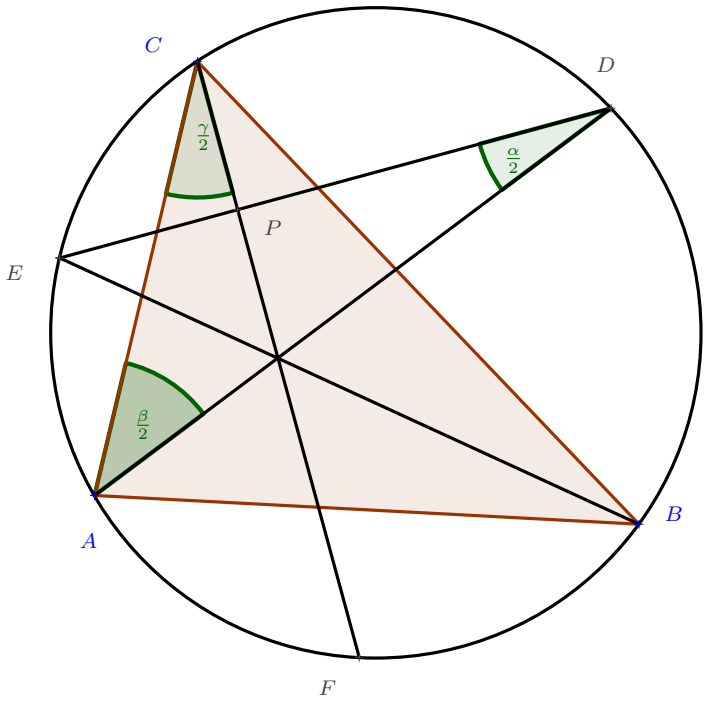
$$\frac{(\sqrt[3]{2}+\sqrt[3]{4})^3}{\sqrt[3]{2}+\sqrt[3]{4}+1} = \frac{2+4+3\cdot\sqrt[3]{2}\cdot\sqrt[3]{4}\cdot(\sqrt[3]{2}+\sqrt[3]{4})}{\sqrt[3]{2}+\sqrt[3]{4}+1} = \frac{6+6(\sqrt[3]{2}+\sqrt[3]{4})}{\sqrt[3]{2}+\sqrt[3]{4}+1} = 6.$$

Úloha 3.6. Liběnka si zatím trénovala rýsování. Začala tím, že si nakreslila trojúhelník ABC a opsala mu kružnici k. Nové průsečíky kružnice k s osami úhlů BAC, ABC, ACB označila po řadě D,E,F. Matějovi se povedlo dokázat, že přímky DE a CF svírají pravý úhel. Svedete to taky?

Řešení. Označme standardně α, β, γ velikosti vnitřních úhlů $\triangle ABC$. Z bodů D a B se díváme na tětivu AE pod stejným úhlem, tj.

$$|\sphericalangle ADE| = |\sphericalangle ABE| = \frac{\alpha}{2}$$

Nyní budeme uvážíme tři rotace ϕ, χ, ψ v kladném směru (tj. proti směru hodinových ručiček). Rotace ϕ bude rotace o $\frac{\alpha}{2}$ kolem bodu D. Druhá rotace χ bude rotace o $\frac{\beta}{2}$ kolem bodu A. A konečně ψ bude rotace o $\frac{\gamma}{2}$ kolem bodu C. Snadno nahlédneme, že přímka ED se v ϕ zobrazí na přímku AD, která se v χ zobrazí na přímku AC, která se v ψ zobrazí na přímku FC.



Tedy přímka FC je obrazem přímky ED v zobrazení $\psi \circ (\chi \circ \phi)$ (neboli v ϕ ji otočíme na AD, potom v χ ji otočíme na AC a nakonec v ψ ji otočíme na CF.)
Proto svírají přímky ED a CF úhel $\frac{\alpha}{2} + \frac{\beta}{2} + \frac{\gamma}{2} = \frac{\pi}{2}$, což jsme chtěli dokázat. Není krásné, že se takové přímky protnou zrovna v P?

□

Úloha 3.7. Henry zrovna přemýšlel o prapůvodním významu slova množina, když ho napadlo, jak by asi vypadala taková množina přirozených čísel, ze které by nešlo vybrat několik prvků, které by mu v součtu dávaly nějakou pořádnou mocninu. Zajímalo ho, jestli taková množina může být nekonečná a jestli by mu vůbec k něčemu užitečnému mohla být. Pomožte Henrymu! Rozhodněte, zda existuje nekonečná množina přirozených čísel, pro kterou platí, že součet prvků její libovolné neprázdné konečné podmnožiny není tvaru n^k, kde n, k jsou přirozená čísla větší než 1. Můžete se vyjádřit i k užitečnosti takové množiny.

Řešení. Ano, taková množina skutečně existuje, uvažme například množinu

$$M = \{2^n 3^{n+1} \mid n \in \mathbb{N}\},$$

zřejmě je nekonečná. Nyní zvolme libovolná pod dvou různá $a_1, a_2, \ldots, a_r \in M$ a označme $a_i = 2^{l_i} 3^{l_i+1}$ pro $l_i \in \mathbb{N}$ a $i \in \{1, 2, \ldots, r\}$. BÚNO předpokládejme $0 < l_1 < l_2 < \cdots < l_k$. Počítejme součet S vybraných prvků:

$$S = a_1 + a_2 + \cdots + a_k = 2^{l_1} 3^{l_1+1} + 2^{l_2} 3^{l_2+1} + \cdots + 2^{l_k} 3^{l_k+1} = 2^{l_1} 3^{l_1+1} (1 + 6^{l_2-l_1} + \cdots + 6^{l_k-l_1}).$$

V poslední pravé závorce jsou všechny členy kromě 1 přirozené mocniny čísla 6, proto je tato závorka nedělitelná šesti, což znamená, že mocnina 2 v prvočíselném rozkladu S je o jedna menší než mocnina 3. Přitom $6 \mid S$, takže pokud $S = n^k$ pro nějaká $n, k \in \mathbb{N}$, $n > 1$, $k > 1$, pak také $6 \mid S$, takže $n = 2^p 3^q t$, kde $p, q, t \in \mathbb{N}$ a $\gcd(t, 6) = 1$. Pak ale

$S = n^k = 2^{kp}3^{kq}t^k$, tedy $kp + 1 = kq$, což je spor, protože $k > 1$. Proto součet prvků libovolné neprázdné konečné podmnožiny M nemůže být tvaru n^k. Co se týče užitečnosti, tato množina je zcela nezpochybnitelně bezva.