Jáma lvová

Zadání 1. kola
XV. ročník

Ahoj!

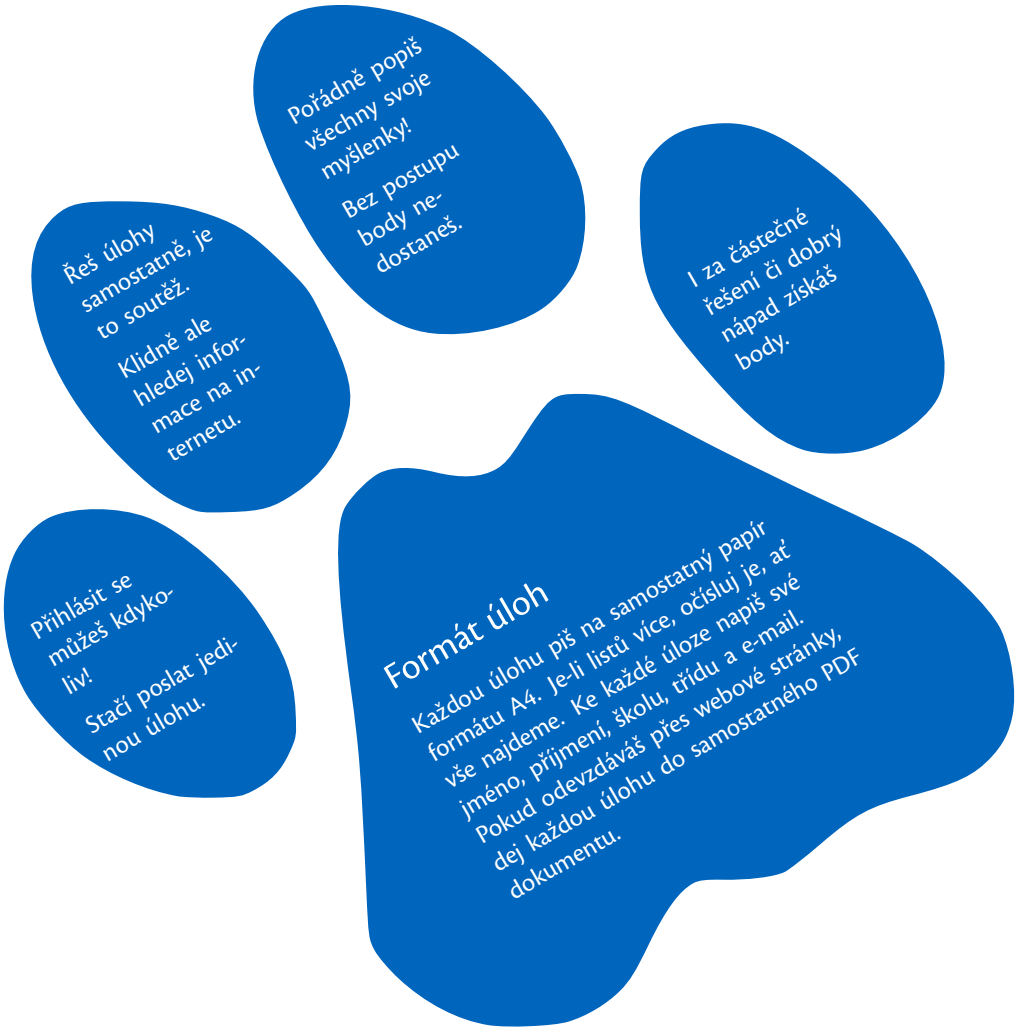
Vítej v Jámě lvové! Jsme korespondenční soutěž na pomezí matematiky a informatiky pro žáky 6. – 9. tříd ZŠ a odpovídajících ročníků gymnázií pořádaná již patnáctým rokem Českým vysokým učením technickým v Praze.

Soutěž je rozdělena na dvě kategorie, Mladší (6. a 7. třída) a Starší (8. a 9. třída). Skládá se ze čtyř kol, v každém na Tebe čekají dvě záludné úlohy a jedno rozsáhlejší *tématko*, kde Tě zasvětíme do určitého zákoutí matematiky, fyziky nebo informatiky. Na léto je pro soutěžící přichystán jedinečný letní tábor. Kapacita je 24 účastníků a přednost dostanou ti s lepším umístěním. Než se vrhneš do řešení, mrkni na pravidla.

Více informací o nás najdeš na `https://jamalvova.cz` a dále na Facebooku a Instagramu.

Novinky v 15. ročníku

V letošním ročníku se mění struktura kol a úloh. Zadání každé kategorie se nově skládá z dvou kratších úloh a jedné rozsáhlejší úlohy, které budeme říkat *tématko*. Tématko se věnuje konkrétní oblasti matematiky, fyziky či informatiky a snaží se Ti ji přiblížit pomocí několika podúloh. Doufáme, že se Ti tato změna bude líbit a rádi od Tebe uslyšíme případnou zpětnou vazbu.



Svá řešení nám pošli do **4. prosince 2023** prostřednictvím stránek soutěže, nebo na adresu:

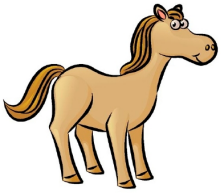
Odbor PR a marketingu – Jáma lvová
Rektorát ČVUT
Jugoslávských partyzánů 3
160 00 Praha 6

Hodně štěstí a bystrou mysl při řešení přejí

Alenka, Bětka, Honza, Honza, Káťa, Kobi, Lenička, Linda, Láďa, Lída, Martin, Matěj, Mája, Rézi, Zuzka a Zuzka

Kategorie mladší

Úloha 0A Byrokratická (2 body)

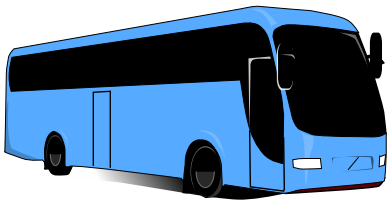


Úředního šimla Honzíka i jeho kolegy velmi unavuje neustálé třídění a přebírání úloh. Poslední dobou musí dokonce dělat přesčasy a zůstávat v kanceláři přes noc. Rozhodli se tedy, že budou vyžadovat, aby měly všechny úlohy opravdu správný formát. Pomoz Honzíkovi tak, že Tvé úlohy budou splňovat požadavky uvedené v úvodním textu. (Tedy každá bude na samostatném listu papíru A4, nadepsaná jménem, příjmením, emailem, třídou a názvem školy a číslem úlohy. Témátko, ač je děleno na podúlohy, prosím odevzdávej jako jeden celek, tedy jako by to byla jedna velká úloha.)

Chceš-li si ulehčit práci s nadepisováním hlavičky a odesíláním obálek, můžeš svá řešení po přihlášení nahrát na stránky Jámy lvové `jamalvova.cz`. Ale pozor! Pouze ve formátu PDF! Pokud bys měl jakékoli problémy, napiš nám na e-mail (`jamalvova@jamalvova.cz`).

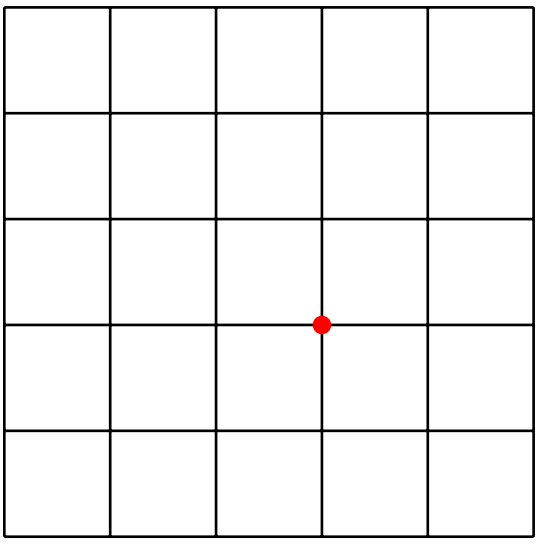
Úloha 1A Levácký autobus (5 bodů)

Zvířátkům z Pravé Vesnice se omrzela pravá strana, a tak se rozhodla přihlásit do unikátního projektu That's left! a vytvořit nejdelší trasu vyhlídkového autobusu uskutečňujícího prohlídky historického centra sídla v celém Levém kraji. Zvířátka v soutěži bojují s tvrdou konkurencí, ale mají k dispozici ty nejlepší architekty, projektanty a logistické pracovníky, kteří na plánu Levé trasy usilovně pracují.



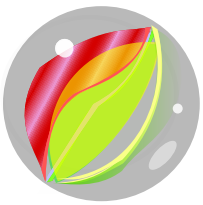
A jak by taková trasa měla podle požadavků organizátorů soutěže That's left! vypadat? Musí být zkrátka a jednoduše nejdelší. Město se skládá z 25 stejně velkých bloků s čtvercovým půdorysem o straně dlouhé 100 m. Bloky jsou uspořádané do čtverce 5 x 5. Trasa musí začínat a končit na křižovatce u radnice (viz obrázek). Vyhlídkový autobus samozřejmě neumí zatáčet doprava, takže na každé křižovatce se dá jet pouze rovně, nebo zahnout doleva. Autobus také nesmí projet tou samou ulicí více než jednou, protože by byla jízda moc nudná, na stejné křižovatce se však autobus více než jednou objevit smí.

Pomůžeš projektovému týmu odborníků naplánovat 3 možné vyhlídkové trasy s minimální délkou 3 600 metrů, které splňují všechny výše zmíněné požadavky? Je možné, aby se při takové vyhlídkové trase turisté podívaly do všech koutů (= rohů) města?



Obrázek 1: Mapa města.

Úloha 2A Kuličky (8 bodů)



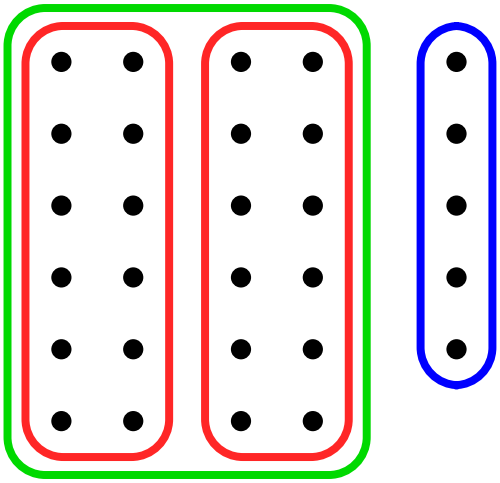
Beruška Bětuška je vášnivá sběratelka. Chtěla by začít ve velkém sbírat kuličky, a proto si vytvořila plán: první den si koupí tři a každý další den o tři více, než den předchozí. Doma si je bude skládat do čtvercové mřížky, první den do prvního řádku, druhý den do druhého řádku a každý další den do dalšího řádku.

Po n dnech už jí ale rozloha uschovávací mřížky začne překážet, takže by si chtěla kuličky přesypat do krabice, na kterou napíše, kolik jich tam je. Pomůžeš jí kuličky v krabici spočítat?

Témátko 3A Počítání se zbytky (celkem 10 bodů)

Dělení se zbytkem pravděpodobně znáš z prvního stupně. Člověk zkrátka dělí (třeba pomocí dělení pod sebe), a když výsledný podíl nevychází hezky, oddělí se stranou malý zbytek jako jakási „chyba“. V tomto textíku se Ti pokusíme nabídnout ochutnávku toho, co se začne dít, pokud se naopak zaměříme právě na zbytek po dělení a nebude nás zajímat samotný podíl.

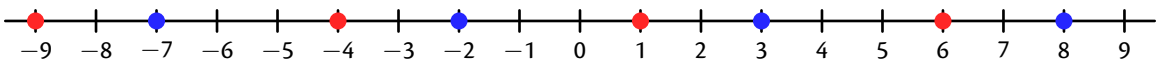
Jak to bude fungovat? Budeme mít zvoleno nějaké číslo m, které bude představovat dělitele, podle kterého zbytky bereme – říkáme mu *modulo*. Vezmeme-li např. $m = 12$, pak se díváme na zbytky po dělení dvanácti. Například číslo 29 dává po dělení zvoleným m zbytek 5 a dovedeme ho tedy zapsat jako $29 = 2 \cdot 12 + 5$ (číslo = násobek modula + zbytek). V reálném světě právě takto fungují ručičkové hodiny: neukáží nám celkovou uplynulou dobu od dané chvíle ale pouze její zbytek po dělení dvanácti hodinami. Ručičky tedy 29 hodin po půlnoci ukazují stejně jako 5 hodin po půlnoci.



$$29 = 2 \cdot 12 + 5$$
$$\text{číslo} = \text{násobek modula} + \text{zbytek}$$

Obrázek 2: Co přesně znamená $29 \equiv 5 \pmod{12}$.

Všechna celá čísla se nám tímto seskupí do rodinek, které dávají stejný zbytek. V rodince čísel dávajících zbytek 5 po dělení dvanácti tak bude třeba pětka samotná, dále 29, ale také 17 a 41, 53, 65 a tak dále – skákáním o dvanáct budeme dostávat další čísla se stejným zbytkem. Opomenout nelze ani čísla záporná: skoky od 5 o dvanáct níže získáme -7, -19, -31 a tak dále. Brát zbytek záporného celého čísla po dělení dvanácti není o nic méně smysluplné než brát zbytky kladných celých čísel – stále se o správnosti zbytku 5 po dělení dvanácti dovedeme přesvědčit vyjádřením $-31 = -3 \cdot 12 + 5$. Matematici těmto „rodinkám podle zbytků“ říkají *zbytkové třídy*. V tomto odstavci jsme tedy jen obšírně popsali, že čísla 5, 17, 29, … a stejně tak -7, -19, … leží v té samé zbytkové třídě modulo 12. Vztahu, kdy dávají dvě čísla a a b stejný zbytek modulo m, se též říká, že „a a b jsou *kongruentní* modulo m“, a pro krátký zápis se vžil symbol „trojitého rovnítka“, přičemž modulo se připíše do závorky: píšeme $a \equiv b \pmod{m}$.



Obrázek 3: Dvě různé zbytkové třídy modulo 5.

Podúloha i) (1 bod)

Kolik zbytkových tříd modulo 2023 *celkem existuje?*

Dosud by sis mohl(a) právem říkat, že tohle všechno je jen spousta názvosloví bez skutečné matematické novoty. Klíčovou vlastností počítání se zbytky je to, že když nás na výsledku příkladu se sčítáním, odečítáním a násobením zajímá jen jeho zbytek po dělení, pak i u všech jednotlivých čísel či mezivýsledků výpočtu můžeme poskočit o modulo a usnadnit si tak počítání. Uveďme na příkladu.

Opusťme nyní počítání modulo 12 a zvolme si pro ozvláštnění třeba modulo $m = 7$. Dejme tomu, že chceme spočíst $71 \cdot 7001 \pmod{7}$. Samozřejmě vždycky můžeme zatnout zuby a násobením pod sebe spočítat, že $71 \cdot 7001 = 497\,071$, a posléze se neméně úmorným dělením pod sebe se zbytkem zjistit, že 497 071 dává po dělení sedmi zbytek 1. Existuje však snadnější cesta: ještě před násobením si můžeme říct, že 71 dává zbytek 1 po dělení sedmi (protože $71 = 10 \cdot 7 + 1$), stejně jako 7001 dává zbytek 1 po dělení sedmi (protože $7001 = 1000 \cdot 7 + 1$), takže

$$71 \cdot 7001 \equiv 1 \cdot 1 \equiv 1 \pmod{7}.$$

Ostatně to, že zbytek výsledku nějakého příkladu závisí jen na zbytcích jednotlivých čísel, se kterými počítáme, je dobře známé v konkrétních případech: to, zda je součet (nebo součin) dvou čísel sudý či lichý, záleží jen na lichosti/sudosti oněch čísel. Stejně tak poslední cifra součinu/součtu závisí jen na posledních cifrách činitelů/sčítanců, protože „poslední cifra“ je jen jiné pojmenování pro „zbytek po dělení deseti“.

Podúloha ii) **(3 body)**

Představ si, že bychom na papír zapsali 120 pětek a všechny je znásobili. Jaký zbytek modulo 23 by dával výsledek? Snaž se co nejvíce si usnadnit práci modulením mezivýsledků tak, abys nemusel(a) nikdy počítat s příliš velkými čísly.

Podúloha iii) **(1 bod)**

Při počítání se zbytky se mohou dít na první pohled zvláštní věci: zatímco za obvyklých okolností víme, že součin dvou nenulových čísel je vždy nenulový, při počítání jen se zbytky už to nemusí tak docela platit. Najdi dvě celá čísla a, b taková, že ačkoliv $a \not\equiv 0 \pmod{512}$ i $b \not\equiv 0 \pmod{512}$, přesto $a \cdot b \equiv 0 \pmod{512}$.

Dosud jsme se dívali vždy jen na jedno modulo, nyní proto zkusme říci něco o tom, jak spolu souvisí či nesouvisí zbytky, které může jedno číslo dávat po dělení různými moduly m, n.

Nejjednodušší situace nastává, je-li n dělitelem m. Uvažujme třeba $m = 12$ a k tomu $n = 4$. Dvanáct je násobkem čtyř, takže pokud známe zbytek nějakého neznámého x po dělení dvanácti, snadno dopočteme zbytek po dělení čtyřmi. Uděláme to tak, že ze samotného zbytku po dělení dvanácti spočítáme zbytek po dělení čtyřmi. Pokud tedy třeba $x \equiv 7 \pmod{12}$, zaručeně to znamená, že $x \equiv 7 \equiv 3 \pmod{4}$. Toto „zeslabení modula“ funguje díky tomu, že když už víme, že $x = y \cdot 12 + 7$ pro nějaké celé číslo y (což dosvědčuje $x \equiv 7 \pmod{12}$), jednoduše tuto rovnost přepíšeme na

$$x = y \cdot 3 \cdot 4 + 4 + 3 = (3y + 1) \cdot 4 + 3$$

(což dosvědčuje $x \equiv 3 \pmod{4}$).

Pokud však n nedělí m, z jednoho zbytku nejspíš druhý nezjistíme: kupříkladu čísla 7, 19, 31, 43, 55 leží všechny v té samé zbytkové třídě modulo 12, ale modulo 5 dávají popořadě zbytky 2, 4, 1, 3, 0. Zbytek modulo 12 nám tedy evidentně nic nedovede napovědět o zbytku modulo 5.

Co kdybychom se ale zabývali opačnou úlohou – jak ze zbytků v několika menších modulech zjistit zbytek ve větším modulu? Konkrétně, dejme tomu, že známé zbytky $x \pmod{m}$ a $x \pmod{n}$, a zkusme zjistit $x \pmod{mn}$. „Zkoušku“ pak provedeme snadno, protože m i n jsou dělitelé čísla mn, takže informace o zbytku x modulo mn v sobě automaticky obsáhne informace o zbytku modulo m i o zbytku modulo n. Přesně takovýmto „složením“ informací modulo m a modulo n se zabývá *Čínská zbytková věta*, jež praví:

Nechť jsou m a n dvě nesoudělná celá čísla. Potom kdykoliv zvolíme zbytek $y \pmod{m}$ a zbytek $z \pmod{n}$, pak existuje existuje číslo x, které splňuje obě kongruence

$$x \equiv y \pmod{m},$$
$$x \equiv z \pmod{n}.$$

Navíc platí, že všechna taková x jsou navzájem kongruentní modulo mn.

Co to znamená? Zaprvé je nutné, aby modula byla nesoudělná, tedy aby jejich největší společný dělitel byl roven 1. Tomu vyhovuje třeba náš předchozí příklad $m = 12$, $n = 5$, protože děliteli 12 jsou jen 1, 2, 3, 4, 6 a 12 sama, zatímco 5 má za dělitele jen 1 a 5 samu, takže jediným společným dělitelem je 1. Čínská zbytková věta tak potvrzuje předchozí pozorování, že zbytek modulo 5 nijak nezávisí na zbytku modulo 12, protože si můžeme oba zbytky navolit libovolně a stále bude zaručeno, že nějaké celé číslo (resp. dokonce právě jedna zbytková třída modulo $12 \cdot 5 = 60$) jich dosáhne.

Řečeno neformálně, Čínská zbytková věta praví, že znát zbytek x modulo mn je zcela stejně hodnotná informace, jako znát jeho zbytek modulo m a zároveň jeho zbytek modulo n, protože dvojice zbytků modulo m a n jednoznačně určuje zbytek modulo mn, a naopak. Tomu mimochodem krásně odpovídá, že existuje m různých zbytků modulo m, k tomu n různých zbytků modulo n, takže z nich vytvoříme přesně $m \cdot n$ dvojic, což je přesně počet různých zbytků modulo mn.

Jak ale onu zbytkovou třídu modulo mn, která má odpovídat $y \pmod{m}$ a zároveň $z \pmod{n}$, nalezneme? Vždy bychom mohli prostě vyzkoušet všechny možnosti, ale lze to i přímočařeji. Uvažujme opět náš příklad $m = 12$, $n = 5$. Tvrdíme, že bude vyhovovat takové x, které lze vyjádřit jako $x = ay + bz$ pro $a = 25$ a $b = 36$. Můžeme si to vyzkoušet na konkrétním příkladě, kdy za y a z zvolíme třeba 7 a 3. Potom $x = 25 \cdot 7 + 36 \cdot 3$. Zkus si ověřit, ze nalezené x skutečně dává zbytek 7 modulo 12 a zbytek 3 modulo 5.

Proč by ale měla fungovat zrovna takováhle magie? Trik se skrývá v tom, jaké zbytky dávají sama a, b modulo m, n. Konkrétně a jsme zvolili tak, aby bylo násobkem $n = 5$, ale modulo $m = 12$ dávalo zbytek 1. To znamená, že výraz ay přispívá y do výsledného zbytku modulo m, zatímco zbytek modulo n nijak nemění, protože už samo a dává modulo n zbytek 0. Obdobně jsme b zvolili tak, aby dávalo zbytek 0 modulo m, ale zbytek 1 modulo n, takže bz nijak nemění výsledný zbytek modulo m, zatímco do zbytku modulo n přispívá přesně z.

Podúloha iv) **(3 body)**

Uvažuj situaci, kdy se naše modula m a n liší pouze o 1, tedy $n = m + 1$. Vymysli, jaká čísla použít v roli „magických čísel" a, b, která dají vždy v jednom modulu zbytek 0 a v druhém 1. Ověř svou odpověď pro $m = 2023$, $n = 2024$ tím, že nalezneš nějaké celé číslo x, které splňuje

$$x \equiv 15 \pmod{2023},$$
$$x \equiv 42 \pmod{2024}.$$

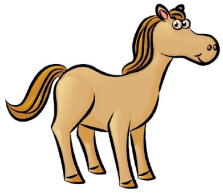
Podúloha v) **(2 body)**

V Čínské zbytkové větě jsme uvedli podmínku, že modula m a n musí být nesoudělná. Je tato podmínka skutečně nutná? Zvládneš najít dvojici zbytků modulo $m = 65$ a modulo $n = 91$, která nebude splněna žádným jedním celým číslem?

Vrtá ti stále hlavou, jak jsme nalezli ta správná a, b? To je příběh na někdy příště – jako upoutávku můžeme prozradit, že souvisí s Eukleidovým algoritmem, kterým mimo jiné počítáme největší společné dělitele.

Kategorie starší

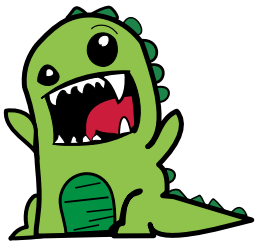
Úloha 0B Byrokratická (2 body)



Úředního šimla Honzíka i jeho kolegy velmi unavuje neustálé třídění a přebírání úloh. Poslední dobou musí dokonce dělat přesčasy a zůstávat v kanceláři přes noc. Rozhodli se tedy, že budou vyžadovat, aby měly všechny úlohy opravdu správný formát. Pomoz Honzíkovi tak, že Tvé úlohy budou splňovat požadavky uvedené v úvodním textu. (Tedy každá bude na samostatném listu papíru A4, nadepsaná jménem, příjmením, emailem, třídou a názvem školy a číslem úlohy. Témátko, ač je děleno na podúlohy, prosím odevzdávej jako jeden celek, tedy jako by to byla jedna velká úloha.)

Chceš-li si ulehčit práci s nadepisováním hlavičky a odesíláním obálek, můžeš svá řešení po přihlášení nahrát na stránky Jámy lvové `jamalvova.cz`. Ale pozor! Pouze ve formátu PDF! Pokud bys měl jakékoli problémy, napiš nám na e-mail (`jamalvova@jamalvova.cz`).

Úloha 1B Výprava do pravěku (5 bodů)



Cestovatelé časem manželé Medvědovi během své návštěvy v dávné historii udělali několik hezkých fotek. Avšak cestou do přítomnosti se jim zničil jejich fotoaparát. Jediné co se jim podařilo zachránit jsou data z jedné fotografie, která značí součet intenzity pixelů ve sloupcích a řádcích. Dále se jim podařilo zjistit jaká intenzita pixelu se rovná jaké barvě.

1	1	1	1	1	5	4	4	1	2	1	5	3	2
1	1	1	3	2	4	3	3	1	2	5	2	1	2
1	2	2	1	2	1	3	3	3	3	1	3	1	2
1	1	2	1	2				4	3	2		1	4
2	1	1	2	3				1		1		4	
4	1	1	2										
	3	1											
		1											

69	66	72	69	69	57	64	64	60	70	69	54	55	52		různých barev	předělů
														70	4	4
	6						4					4		79	4	4
			8											76	4	4
														66	5	6
													5	65	4	9
				7						7				84	2	2
9														102	4	3
													8	113	3	7
				9										117	3	7
		7									8			118	3	3

Obrázek 4: Tabulka předělů. (tmavě červená = 1, světle červená = 2, tmavě modrá = 3, světle modrá = 4, oranžová = 5, světle žlutá = 6, tmavě zelená = 7, světle zelená = 8, hnědá = 9)

Čísla nad tabulkou říkají, kolik je v daném sloupci kostiček stejné barvy nad sebou, to znamená po kolika kostičkách přijde předěl mezi barvami. Čísla napravo od tabulky značí počet různých barev v dané řadě a počet předělů pro danou řadu. Na obrázku jsou jen barvy s číselnými hodnotami od 1 do 9, které uvádí tabulka.

Pomůžeš manželům Medvědovým sestrojit jejich jedinou památku na cestu do dálné minulosti?

Úloha 2B Je těžší ten či onen? (8 bodů)

Brouček Bořek má 16 předmětů, z nichž každé dva mají rozdílnou váhu. Na rovnoramenné váze může zvážit dva předměty a zjistit tím, který je těžší.

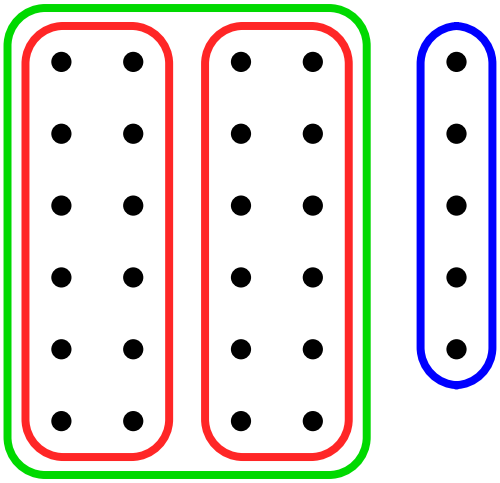
Pomůžeš Bořkovi najít postup, kterým vždy na 22 vážení nebo méně nalezne druhý nejtěžší předmět?

Pokud se Ti nepodaří nalézt řešení v rámci 22 kroků, nevadí to, popiš nám a pošli i řešení, které této podmínce nevyhovuje, i za něj dostaneš bodové ohodnocení!

Témátko 3B Počítání se zbytky (celkem 10 bodů)

Dělení se zbytkem pravděpodobně znáš z prvního stupně. Člověk zkrátka dělí (třeba pomocí dělení pod sebe), a když výsledný podíl nevychází hezky, oddělí se stranou malý zbytek jako jakási „chyba“. V tomto textíku se Ti pokusíme nabídnout ochutnávku toho, co se začne dít, pokud se naopak zaměříme právě na zbytek po dělení a nebude nás zajímat samotný podíl.

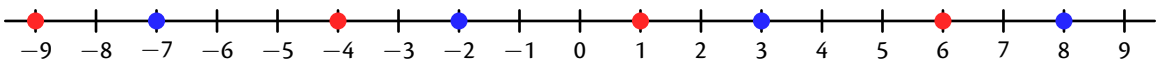
Jak to bude fungovat? Budeme mít zvoleno nějaké číslo m, které bude představovat dělitele, podle kterého zbytky bereme – říkáme mu *modulo*. Vezmeme-li např. $m = 12$, pak se díváme na zbytky po dělení dvanácti. Například číslo 29 dává po dělení zvoleným m zbytek 5 a dovedeme ho tedy zapsat jako $29 = 2 \cdot 12 + 5$ (číslo = násobek modula + zbytek). V reálném světě právě takto fungují ručičkové hodiny: neukáží nám celkovou uplynulou dobu od dané chvíle ale pouze její zbytek po dělení dvanácti hodinami. Ručičky tedy 29 hodin po půlnoci ukazují stejně jako 5 hodin po půlnoci.



$$29 = 2 \cdot 12 + 5$$
$$\text{číslo} = \text{násobek modula} + \text{zbytek}$$

Obrázek 5: Co přesně znamená $29 \equiv 5 \pmod{12}$.

Všechna celá čísla se nám tímto seskupí do rodinek, které dávají stejný zbytek. V rodince čísel dávajících zbytek 5 po dělení dvanácti tak bude třeba pětka samotná, dále 29, ale také 17 a 41, 53, 65 a tak dále – skákáním o dvanáct budeme dostávat další čísla se stejným zbytkem. Opomenout nelze ani čísla záporná: skoky od 5 o dvanáct níže získáme -7, -19, -31 a tak dále. Brát zbytek záporného celého čísla po dělení dvanácti není o nic méně smysluplné než brát zbytky kladných celých čísel – stále se o správnosti zbytku 5 po dělení dvanácti dovedeme přesvědčit vyjádřením $-31 = -3 \cdot 12 + 5$. Matematici těmto „rodinkám podle zbytků“ říkají *zbytkové třídy*. V tomto odstavci jsme tedy jen obšírně popsali, že čísla 5, 17, 29, … a stejně tak -7, -19, … leží v té samé zbytkové třídě modulo 12. Vztahu, kdy dávají dvě čísla a a b stejný zbytek modulo m, se též říká, že „a a b jsou *kongruentní* modulo m“, a pro krátký zápis se vžil symbol „trojitého rovnítka“, přičemž modulo se připíše do závorky: píšeme $a \equiv b \pmod{m}$.



Obrázek 6: Dvě různé zbytkové třídy modulo 5.

Podúloha i) (1 bod)

Kolik zbytkových tříd modulo 2023 *celkem existuje?*

Dosud by sis mohl(a) právem říkat, že tohle všechno je jen spousta názvosloví bez skutečné matematické novoty. Klíčovou vlastností počítání se zbytky je to, že když nás na výsledku příkladu se sčítáním, odečítáním a násobením zajímá jen jeho zbytek po dělení, pak i u všech jednotlivých čísel či mezivýsledků výpočtu můžeme poskočit o modulo a usnadnit si tak počítání. Uveďme na příkladu.

Opusťme nyní počítání modulo 12 a zvolme si pro ozvláštnění třeba modulo $m = 7$. Dejme tomu, že chceme spočíst $71 \cdot 7001 \pmod{7}$. Samozřejmě vždycky můžeme zatnout zuby a násobením pod sebe spočítat, že $71 \cdot 7001 = 497\,071$, a posléze se neméně úmorným dělením pod sebe se zbytkem zjistit, že 497 071 dává po dělení sedmi zbytek 1. Existuje však snadnější cesta: ještě před násobením si můžeme říct, že 71 dává zbytek 1 po dělení sedmi (protože $71 = 10 \cdot 7 + 1$), stejně jako 7001 dává zbytek 1 po dělení sedmi (protože $7001 = 1000 \cdot 7 + 1$), takže

$$71 \cdot 7001 \equiv 1 \cdot 1 \equiv 1 \pmod{7}.$$

Ostatně to, že zbytek výsledku nějakého příkladu závisí jen na zbytcích jednotlivých čísel, se kterými počítáme, je dobře známé v konkrétních případech: to, zda je součet (nebo součin) dvou čísel sudý či lichý, záleží jen na lichosti/sudosti oněch čísel. Stejně tak poslední cifra součinu/součtu závisí jen na posledních cifrách činitelů/sčítanců, protože „poslední cifra“ je jen jiné pojmenování pro „zbytek po dělení deseti“.

Podúloha ii) **(3 body)**

Představ si, že bychom na papír zapsali 120 pětek a všechny je znásobili. Jaký zbytek modulo 23 by dával výsledek? Snaž se co nejvíce si usnadnit práci modulením mezivýsledků tak, abys nemusel(a) nikdy počítat s příliš velkými čísly.

Podúloha iii) **(1 bod)**

Při počítání se zbytky se mohou dít na první pohled zvláštní věci: zatímco za obvyklých okolností víme, že součin dvou nenulových čísel je vždy nenulový, při počítání jen se zbytky už to nemusí tak docela platit. Najdi dvě celá čísla a, b taková, že ačkoliv $a \not\equiv 0 \pmod{512}$ i $b \not\equiv 0 \pmod{512}$, přesto $a \cdot b \equiv 0 \pmod{512}$.

Dosud jsme se dívali vždy jen na jedno modulo, nyní proto zkusme říci něco o tom, jak spolu souvisí či nesouvisí zbytky, které může jedno číslo dávat po dělení různými moduly m, n.

Nejjednodušší situace nastává, je-li n dělitelem m. Uvažujme třeba $m = 12$ a k tomu $n = 4$. Dvanáct je násobkem čtyř, takže pokud známe zbytek nějakého neznámého x po dělení dvanácti, snadno dopočteme zbytek po dělení čtyřmi. Uděláme to tak, že ze samotného zbytku po dělení dvanácti spočítáme zbytek po dělení čtyřmi. Pokud tedy třeba $x \equiv 7 \pmod{12}$, zaručeně to znamená, že $x \equiv 7 \equiv 3 \pmod{4}$. Toto „zeslabení modula“ funguje díky tomu, že když už víme, že $x = y \cdot 12 + 7$ pro nějaké celé číslo y (což dosvědčuje $x \equiv 7 \pmod{12}$), jednoduše tuto rovnost přepíšeme na

$$x = y \cdot 3 \cdot 4 + 4 + 3 = (3y + 1) \cdot 4 + 3$$

(což dosvědčuje $x \equiv 3 \pmod{4}$).

Pokud však n nedělí m, z jednoho zbytku nejspíš druhý nezjistíme: kupříkladu čísla 7, 19, 31, 43, 55 leží všechny v té samé zbytkové třídě modulo 12, ale modulo 5 dávají popořadě zbytky 2, 4, 1, 3, 0. Zbytek modulo 12 nám tedy evidentně nic nedovede napovědět o zbytku modulo 5.

Co kdybychom se ale zabývali opačnou úlohou – jak ze zbytků v několika menších modulech zjistit zbytek ve větším modulu? Konkrétně, dejme tomu, že známé zbytky $x \pmod{m}$ a $x \pmod{n}$, a zkusme zjistit $x \pmod{mn}$. „Zkoušku“ pak provedeme snadno, protože m i n jsou dělitelé čísla mn, takže informace o zbytku x modulo mn v sobě automaticky obsáhne informace o zbytku modulo m i o zbytku modulo n. Přesně takovýmto „složením“ informací modulo m a modulo n se zabývá *Čínská zbytková věta*, jež praví:

Nechť jsou m a n dvě nesoudělná celá čísla. Potom kdykoliv zvolíme zbytek $y \pmod{m}$ a zbytek $z \pmod{n}$, pak existuje existuje číslo x, které splňuje obě kongruence

$$x \equiv y \pmod{m},$$
$$x \equiv z \pmod{n}.$$

Navíc platí, že všechna taková x jsou navzájem kongruentní modulo mn.

Co to znamená? Zaprvé je nutné, aby modula byla nesoudělná, tedy aby jejich největší společný dělitel byl roven 1. Tomu vyhovuje třeba náš předchozí příklad $m = 12$, $n = 5$, protože děliteli 12 jsou jen 1, 2, 3, 4, 6 a 12 sama, zatímco 5 má za dělitele jen 1 a 5 samu, takže jediným společným dělitelem je 1. Čínská zbytková věta tak potvrzuje předchozí pozorování, že zbytek modulo 5 nijak nezávisí na zbytku modulo 12, protože si můžeme oba zbytky navolit libovolně a stále bude zaručeno, že nějaké celé číslo (resp. dokonce právě jedna zbytková třída modulo $12 \cdot 5 = 60$) jich dosáhne.

Řečeno neformálně, Čínská zbytková věta praví, že znát zbytek x modulo mn je zcela stejně hodnotná informace, jako znát jeho zbytek modulo m a zároveň jeho zbytek modulo n, protože dvojice zbytků modulo m a n jednoznačně určuje zbytek modulo mn, a naopak. Tomu mimochodem krásně odpovídá, že existuje m různých zbytků modulo m, k tomu n různých zbytků modulo n, takže z nich vytvoříme přesně $m \cdot n$ dvojic, což je přesně počet různých zbytků modulo mn.

Jak ale onu zbytkovou třídu modulo mn, která má odpovídat $y \pmod{m}$ a zároveň $z \pmod{n}$, nalezneme? Vždy bychom mohli prostě vyzkoušet všechny možnosti, ale lze to i přímočařeji. Uvažujme opět náš příklad $m = 12$, $n = 5$. Tvrdíme, že bude vyhovovat takové x, které lze vyjádřit jako $x = ay + bz$ pro $a = 25$ a $b = 36$. Můžeme si to vyzkoušet na konkrétním příkladě, kdy za y a z zvolíme třeba 7 a 3. Potom $x = 25 \cdot 7 + 36 \cdot 3$. Zkus si ověřit, ze nalezené x skutečně dává zbytek 7 modulo 12 a zbytek 3 modulo 5.

Proč by ale měla fungovat zrovna takováhle magie? Trik se skrývá v tom, jaké zbytky dávají sama a, b modulo m, n. Konkrétně a jsme zvolili tak, aby bylo násobkem $n = 5$, ale modulo $m = 12$ dávalo zbytek 1. To znamená, že výraz ay přispívá y do výsledného zbytku modulo m, zatímco zbytek modulo n nijak nemění, protože už samo a dává modulo n zbytek 0. Obdobně jsme b zvolili tak, aby dávalo zbytek 0 modulo m, ale zbytek 1 modulo n, takže bz nijak nemění výsledný zbytek modulo m, zatímco do zbytku modulo n přispívá přesně z.

Podúloha iv) **(3 body)**

Uvažuj situaci, kdy se naše modula m a n liší pouze o 1, tedy $n = m + 1$. Vymysli, jaká čísla použít v roli „magických čísel" a, b, která dají vždy v jednom modulu zbytek 0 a v druhém 1. Ověř svou odpověď pro $m = 2023$, $n = 2024$ tím, že nalezneš nějaké celé číslo x, které splňuje

$$x \equiv 15 \pmod{2023},$$
$$x \equiv 42 \pmod{2024}.$$

Podúloha v) **(2 body)**

V Čínské zbytkové větě jsme uvedli podmínku, že modula m a n musí být nesoudělná. Je tato podmínka skutečně nutná? Zvládneš najít dvojici zbytků modulo $m = 65$ a modulo $n = 91$, která nebude splněna žádným jedním celým číslem?

Vrtá ti stále hlavou, jak jsme nalezli ta správná a, b? To je příběh na někdy příště – jako upoutávku můžeme prozradit, že souvisí s Eukleidovým algoritmem, kterým mimo jiné počítáme největší společné dělitele.