Milý řešiteli,

vítáme Tě u 4. série úloh 4. ročníku korespondenčního semináře MoRoUS. Doufáme, že se ti budou další úlohy líbit a také se něco nového naučíš.

4. série 2017/2018

Termín odeslání 4. série: **9. 4. 2018**

Kam posílat řešení?

Až budeš mít řešení hotové, pošli nám prosím celá svá řešení, včetně všech nákresů, prográmků, prostě vše, co by nám usnadnilo opravování Tvé úlohy. Stačí, když pošleš řešení jen některých úloh nebo jejich částí.

Řešení posílej nejlépe e-mailem na adresu `seminar@morous.fel.cvut.cz`, nebo poštou (řešení každé úlohy v tomto případě napiš na samostatný papír A4) na adresu

Korespondenční seminář Morous,
Katedra kybernetiky FEL ČVUT,
Karlovo náměstí 13,
121 35 Praha

Aleš, Honza, Kája, Klárka, Martin, Mirek, Ondra a Terka

Úloha č. 1: Čapek (20 bodů)

Pirátství a obchod s kradeným olejem přímo kvete. To se samozřejmě nelíbí Intergalaktickému obchodnímu cechu a ani mezihvězdné policii. Nedávno kvůli tomu dokonce vznikla i četa automatů potírající enormní kriminalitu (zkráceně Čapek). Tato veskrze elitní jednotka má učinit přítrž všemu pirátství. Jak to ale u velkých korporací bývá, peněz na robotiku a rozvoj jako takový není nikdy dost a roboti tedy obsahují hlavně součástky z druhé ruky nebo výprodeje.

Roboti jednotky Čapek (hovorově se jim někdy přezdívá „Karel“) nejsou možná nejnovější a jejich technologie je zastaralá, ale rozhodně se nejedná o žádné „tupouny“.

Členové jednotky mezi sebou potřebují bezpečně komunikovat. Protože znají své slabé stránky a vědí, že spolehlivě dokáží pracovat jen s celými nezápornými čísly a že i maximální číslo, které se jim do paměti vejde, je přísně omezeno, začali používat modulární aritmetiku.

Pokud vezmeme klasickou množinu celých čísel $\mathbb{Z}$ a rozdělíme ji na n částí (například podle zbytku po dělení číslem n) a ze všech čísel, která spadají do stejné části, vybereme jednoho reprezentanta dané části (třeba právě hodnotu zbytku po dělení číslem N). Dostaneme tak konečnou množinu $\mathbb{Z}_n$, které se také říká množina zbytkových tříd po dělení číslem n.

Příklad: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Pokud nyní upravíme operace pro počítání s čísly (sčítání, odčítání, ale třeba také násobení nebo mocnění) tak, že po každé operaci zjistíme zbytek po dělení n a číslo nahradíme reprezentantem odpovídající zbytkové třídy, začneme vlastně provádět tzv. modulární aritmetiku.

Otázka 1.1

Abychom se trochu vžili do běžného provozu členů jednotky, pojďme si vyzkoušet nějaké příklady. Budeme používat $\mathbb{Z}_5$, všechny operace se tedy počítají modulo 5 a tedy například čísla 1 a 6 jsou z tohoto pohledu ekvivalentní a také libovolný násobek 5 je roven 0.

$$1 + 2 = 3 \equiv 3 \pmod 5 \qquad 2 + 4 = 6 = 1 \cdot 5 + 1 \equiv 1 \pmod 5$$
$$3 - 1 = 2 \equiv 2 \pmod 5 \qquad 2 - 4 = -2 = -1 \cdot 5 + 3 \equiv 3 \pmod 5$$
$$4 \cdot 2 = 8 = 1 \cdot 5 + 3 \equiv 3 \pmod 5 \qquad 3^4 = 81 = 16 \cdot 5 + 1 \equiv 1 \pmod 5$$

Jak si možná všimneš, je úplně jedno, zda budeme postupovat zcela přímočaře a operaci modulo použijeme na výsledek, nebo zda tak budeme ošetřovat i mezivýsledky. V každém případě se dostaneme ke stejnému číslu. Postupné počítání a modulování výsledků má však výhodu v tom,

že nebudeme pracovat s příliš velkými čísly. Například poslední příklad si můžeme rozložit na iterované násobení:

$$\begin{aligned} 3^4 = 3 \cdot 3 \cdot 3^2 = 9 \cdot 3^2 = (1 \cdot 5 + 4) \cdot 3^2 \equiv 4 \cdot 3^2 \pmod 5 = \\ = 4 \cdot 3 \cdot 3 = 12 \cdot 3 = (2 \cdot 5 + 2) \cdot 3 \equiv 2 \cdot 3 \pmod 5 = \\ = 6 = 1 \cdot 5 + 1 \equiv 1 \pmod 5 \end{aligned}$$

Modulární umocňování je možné dělat i jinou, rychlejší, metodou. Můžeš zkusit metodu opakování čtverců (nebo též metodu binárního umocňování zprava doleva).

Teď je řada na Tobě. Zkus si, nejlépe bez kalkulačky, spočítat následující příklady v $\mathbb{Z}_{24}$:

$$23 + 12 \cdot 12 - 1 = \quad (1)$$

$$3 \cdot 2 \cdot 5 \cdot 4 = \quad (2)$$

$$4^7 = \quad (3)$$

$$(2 \cdot 13)^3 = \quad (4)$$

Otázka 1.2

Jednotka Čapek ale umí i jiné modulární kousky – umí i dělení (byť ne zcela vždy). Podíváme se na chvíli na klasickou matematiku. Mějme $a : b = c$, pak platí $c \cdot b = a$. Přeneseme tuto znalost do modulární aritmetiky. Abychom spočetli $a : b = c \pmod n$, potřebujeme vlastně vědět, jakým číslem z $\mathbb{Z}_n$ musíme vynásobit b, abychom získali a. Například $7 : 2 = x \pmod{11}$ lze převést na problém $x \cdot 2 = 7 \pmod{11}$. Chvilku budeme zkoušet čísla a brzo zjistíme, že $9 \cdot 2 = 18 \equiv 7 \pmod{11}$ a že tedy $x = 9$.

Pozor na to, že modulární dělení může být někdy zrádné – občas řešení neexistuje, občas jich je víc. Zkus spočítat následující příklady v $\mathbb{Z}_{14}$:

$$2 : 3 = \quad (5)$$

$$12 : 10 = \quad (6)$$

$$7 : 5 = \quad (7)$$

$$4 : 7 = \quad (8)$$

Otázka 1.3

Teď už pro Tebe jistě bude hračka zjistit, jakým způsobem mohou roboti v $\mathbb{Z}_n$ počítat a^{-1} (nebo též inverzní prvek k a). Dokážeš popsat, za jakých podmínek tento prvek existuje?

Otázka 1.4

Kapitán Aphael a vedoucí jednotky Belarius se spolu potřebují dohodnout na tajném šifrovacím klíči. Jejich vysílání ale může zachytit zlý robot Erasmus, proto vymyslí jednoduchý trik. Nejprve si spolu oba „Karlové“ vymění čísla $g = 3$ a $p = 29$. Vůbec je netrápí, že je Erasmus bude znát také. Pak si každý z nich vymyslí jedno tajné číslo menší než p. (Nyní budeme předpokládat, že Aphael si vymyslí číslo $a = 5$ a Belarius zvolí číslo $b = 13$.) Každý z „Karlů“ nyní vezme číslo g a umocní jej na své tajné číslo a tím získá číslo A. Tuto operaci bude provádět pomocí modulární aritmetiky v $\mathbb{Z}_p$, tj. $\mathbb{Z}_{29}$.

Aphael tedy ve své výpočetní jednotce postupuje například takto:

$$\begin{aligned} A &= g^a \pmod{p} \\ A &= 3^5 \pmod{29} \\ A &= 11. \end{aligned}$$

Belarius bude postupovat obdobně a získá číslo

$$\begin{aligned} B &= g^b \pmod{p} \\ B &= 3^{13} \pmod{29} \\ B &= 19. \end{aligned}$$

Tato čísla si opět vymění. Erasmus se zaraduje, neboť nyní už zná čísla g, p, A i B.

Aphael i Belarius nyní provedou poslední operaci. Každý z nich vezme číslo toho druhého a umocní jej na své tajné číslo (opět modulo 29, neboli v $\mathbb{Z}_{29}$. Aphael tedy bude počítat:

$$\begin{aligned} x &= B^a \pmod{p} \\ x &= 19^5 \pmod{29} \\ x &= 21. \end{aligned}$$

Belarius bude počítat úplně stejným postupem a získá

$$\begin{aligned} x &= A^b \pmod{p} \\ x &= 11^{13} \pmod{29} \\ x &= 21. \end{aligned}$$

Oba tedy mají stejný tajný klíč x.

Erasmus si ovšem ve svém doupěti marně láme hlavu. Vžijme se teď na chvíli do jeho role... Představme si, že jsme úspěšně odchytili z éteru čísla $g = 7$, $p = 13$, $A = 9$ a $B = 4$. Jaké je společné tajné číslo x? Jak jej Erasmus spočítá? Bude to pro něj složité?

Otázka 1.5

Jak se změní situace, když se pro jednotku Čapek nakoupí větší paměťové čipy a oni si jako číslo p zvolí něco většího, třeba $p = 2\,903$? Nebo dokonce $p = 9\,366\,253\,586\,693\,488\,019$? Bude Erasmus stále schopen dostat se k tajným klíčům?

Úloha č. 2: Černá díra (20 bodů)

Výroba robotů s sebou nese i mnohé vedlejší nepříjemnosti. Jednou takovou komplikací je produkce nejrůznějších chemických odpadů, kterých je potřeba se ve vesmíru zbavovat. Pro tyto účely vznikla takzvaná vesmírná žumpa, do které je možné chemikálie vypustit. Cílem je, aby tyto chemikálie skončily pohlcené černou dírou. To se ale ne vždy podaří. Proto byl vytvořen sbor vesmírných popelářů, který monitoruje pravidelně rozložení a množství chemikálií a případně se stará o jejich průběžnou likvidaci směrem k černé díře. Druhou možností je vyprodukované chemikálie zpracovat ve speciálně upravených zařízeních a zpracovaný chemický odpad následně přeprodávat k další spotřebě.

Prof. Morous tedy váhá mezi možností A (vypustit odpad do žumpy) a možností B (zpracovat chemický odpad a prodat).

Vypouštění do vesmírné žumpy je zdarma, navíc dostane profesor odměnu R_k od továren produkující robotické součástky za každý kilogram chemického odpadu, kterého se mohou takto bez starostí zbavit. Na druhou stranu, likvidace není okamžitá a vesmírní popeláři si účtují každý týden t poplatek C_t za každý kilogram chemického odpadu.

Pokud by se profesor rozhodl odpad dále zpracovávat, musí za každý kilogram odpadu zaplatit poplatek K_k za zpracování. Na druhou stranu, poté každý týden získá odměnu P_t z prodeje zpracovaného chemického odpadu. Po x týdnech nezbude žádný druhotný odpad k prodeji a po y týdnech je všechen odpad zlikvidován pomocí vesmírné žumpy, tudíž je možné přestat platit vesmírným popelářům.

Otázka 2.1

Momentálně je odměna $R_k = 50$ vesmírných žufníčků, poplatek vesmírným popelářům $C_t = 1$ vesmírný žufníček týdně, poplatek za zpracování chemického odpadu $K_k = 100$ vesmírných žufníčků a zisk z každého zpracovaného kilogramu odpadu $P_t = 2$ vesmírné žufníčky týdně. Jak velké by muselo být x (počet týdnů, kdy lze prodávat druhotný chemický odpad) a y (počet týdnů než je všechen odpad zlikvidován pomocí vesmírné žumpy a je možné za něj tudíž přestat platit), aby obě varianty byly stejně výhodné? Existuje více možností?

Otázka 2.2

Představte si, že poplatek vesmírným popelářům za kilogram odpadu se bude každý týden t zvyšovat podle následujícího vzorce: $C_t = 1 + \frac{t}{10}$. Zároveň se ale díky inflaci budou zvyšovat i zisky z každého prodaného kilogramu chemického materiálu: $P_t = 2 + \frac{t}{20}$. Vesmírní popeláři vyhlásili nové nařízení, že nezávisle na skutečné době likvidace odpadu, je potřeba platit poplatek C_t po

dobu 50 týdnů. Kolik minimálně týdnů (x) by muselo být možné přeprodávat druhotný chemický odpad, aby pro profesora bylo výhodnější dát chemický odpad dále zpracovat?

Otázka 2.3

Továrny na zpracování chemického materiálu ale nestíhají a tak cena za zpracování jednoho kilogramu chemického odpadu bude růst podle počtu zpracovaných kilogramů. Cena za zpracování k-tého kilogramu materiálu bude tedy: $K_k = 100 + (k-1) \cdot 10$ (za první kilogram profesor zaplatí 100 žufníčků, za druhý 110 žufníčků a tak dále). Naopak vypouštění do žumpy je pro továrny jednodušší čím více kilogramů odpadu mohou vypustit, a tak odměna pro profesora za k-tý vypuštěný kilogram bude: $R_k = 50 + (k-1) \cdot 2$ (za první kilogram tak dostane 50 žufníčků, za druhý kilogram 52 žufníčků, a tak dále). I nadále platí, že $C_t = 1 + \frac{t}{10}$ a $P_t = 2 + \frac{t}{20}$. Pomůžete profesorovi zjistit, kolik maximálně může nechat zpracovat kilogramů, aby pro něj bylo stále ještě výhodnější nechat zpracovat vyprodukované chemikálie než je vyhodit do vesmírné žumpy? Najdete řešení nezávisle na x a y?

Otázka 2.4

Uvažujte navíc, že vesmírná žumpa sežere každý týden $Z_t = 5$ kilogramů odpadu (tudíž počet kilogramů, za které musí prof. Morous platit vesmírným popelářům, se bude každý týden měnit). Pro kolik kilogramů odpadu se stále ještě vyplatí profesorovi dát odpad zpracovávat?

Otázka 2.5

Jak by se řešení změnilo, kdyby vesmírná žumpa nepožírala odpad rovnoměrně, ale místo toho každý týden v žumpě zmizela $\frac{1}{10}$ odpadu? (Tedy při vyhození 100 kg by první týden sežrala 10 kilogramů. Druhý týden opět $\frac{1}{10}$, ale tentokrát již jen z 90 kilogramů, tedy by zmizelo 9 kilogramů odpadu, atd.)

Tématko č. 1: Energie (20 bodů)

Roboti potřebovali odjakživa nějaký zdroj energie. Zamysli se nad tím, jak by mohlo být zajištění energie pro roboty vyřešeno. Můžeš kombinovat aktuálně využívané zdroje energie, stejně jako navrhnout doposud nevyužívaný přístup. Jak se může změnit způsob získávání energie už bylo ukázáno například na rozdílu pohonu auta ve filmech Návrat do budoucnosti a Návrat do budoucnosti II. Přemýšlej nad tím, jak velké by bylo samotné zařízení pro výrobu elektrické energie (a jakou by muselo mít hmotnost), nebo jestli je schopný vybraný zdroj energie fungovat bez přestání (např. i v noci, bez pohybu apod.) a pokud ne, jak zajistit, aby robot mohl fungovat nepřetržitě? Zamysli se nad možnými pozitivy i negativy jednotlivých přístupů nebo nad jejich vhodnou kombinací.