8 bodov ♢

1A. Akým trojčíslím sa končí číslo 2024^{2024}?

Riešenie: Všetkých možných trojčísiel je iba 1000. Sú to čísla 000 až 999. Je preto jasné, že ak budeme počítať mocniny ľubovoľného čísla, teda aj 2024^1, 2024^2, 2024^3 ..., tak koncové trojčíslia sa po niekoľkých krokoch musia začať opakovať. Skúmajme preto akými trojčíslami sa končia mocniny 2024^n. K tomu nepotrebujeme ani kalkulačku, ani počítač a dokonca nemusíme ani počítať celú hodnotu týchto mocnín. Vieme, že mocnina je opakované násobenie čísla samého sebou, a preto $2024^{n+1} = 2024^n \cdot 2024$. Z algoritmu násobenia čísel, ktorý sme sa učili na základnej škole, potom vieme z koncového trojčíslia mocniny 2024^n rýchlo vypočítať koncové trojčíslie mocniny 2024^{n+1}. Dostaneme

2024^1	...**024**
2024^2	...576
2024^3	...824
2024^4	...776
2024^5	...624
2024^6	...976
2024^7	...424
2024^8	...176
2024^9	...224
2024^{10}	...376
2024^{11}	...**024**

Z uvedenej tabuľky vidíme, že mocniny 2024^n sa končia len 10 možnými trojčíslami, ktoré sa cyklicky opakujú. Stačí sa preto pozrieť na exponent, zistíme, že $(2024 \bmod 10) = 4$ a z toho je zrejmé, že mocniny 2024^4 a 2024^{2024} sa budú končiť rovnakým trojčíslím. Číslo 2024^{2024} sa končí trojčíslím 776.

Poznámka: Zápis $(n \bmod k)$, kde $n, k \in \mathbb{N}$ označuje zvyšok, ktorý dáva číslo n po delení (celočíselné delenie) číslom k.

8 bodov ♢

1B. Akým trojčíslím sa končí číslo $2024^{2024^{\cdot^{\cdot^{\cdot^{2024}}}}\Big\}2025}$?

Riešenie: Využijeme to, čo sme o mocninách 2024^n zistili v úlohe **1A**. Vieme, že 2024^{2024} sa končí trojčíslím 776. Platí $(\ldots 776 \bmod 10) = 6$. Preto $2024^{2024^{2024}}$ sa bude končiť trojčíslím 976. Opäť $(\ldots 976 \bmod 10) = 6$ a takto môžeme pokračovať ďalej. Vidíme, že v prípade čísla 2024 môžeme naskladať ľubovoľný počet (väčší než 2) poschodí mocnín a výsledné číslo sa vždy bude končiť trojčíslím 976.

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

9 bodov ♡

2A. Nájdite všetky prirodzené čísla p, pre ktoré je každé z čísel

$$p, \quad p+17, \quad p+37$$

prvočíslo.

Riešenie: Pre začiatok si všimnime nasledovné

$$0 \bmod 3 = 0\,, \quad 37 \bmod 3 = 1\,, \quad 17 \bmod 3 = 2\,. \tag{1}$$

Zápis $(n \bmod k)$, kde $n, k \in \mathbb{N}$ označuje zvyšok, ktorý dáva číslo n po delení (celočíselné delenie) číslom k. Rovnosti (1) znamenajú, že pre $p > 3$ bude aspoň jedno z čísel p, $p+17$, $p+37$ deliteľné číslom 3.

Preto ak by existovali čísla p vyhovujúce zadaniu úlohy, mohli by to byť len $p = 0$, $p = 1$, $p = 2$, alebo $p = 3$. Pre $p = 0$ dostávame trojicu $(0, 17, 37)$, pre $p = 1$ dostávame trojicu $(1, 18, 38)$, pre $p = 2$ dostávame trojicu $(2, 19, 39)$ a pre $p = 3$ dostávame trojicu $(3, 20, 40)$. Ani jedna z týchto trojíc nevyhovuje zadaniu úlohy (0 nie je prvočíslo). Preto neexistuje žiadne prvočíslo p, pre ktoré je každé z čísel p, $p+17$, $p+37$ prvočíslo.

---

9 bodov ♡

2B. Nájdite všetky prirodzené čísla p, pre ktoré je každé z čísel

$$p, \quad p+6, \quad p+12, \quad p+24, \quad p+48$$

prvočíslo.

Riešenie: Pre začiatok si všimnime nasledovné

$$0 \bmod 5 = 0\,, \quad 6 \bmod 5 = 1\,, \quad 12 \bmod 5 = 2\,, \quad 48 \bmod 5 = 3\,, \quad 24 \bmod 5 = 4\,. \tag{2}$$

Rovnosti (2) znamenajú, že pre $p > 5$ bude aspoň jedno z čísel p, $p+6$, $p+12$, $p+24$, $p+48$ deliteľné číslom 5.

Preto ak by existovali čísla p vyhovujúce zadaniu úlohy, mohli by to byť len $p = 0$, $p = 1$, $p = 2$, $p = 3$, $p = 4$, alebo $p = 5$. Párne čísla môžeme hneď vyhodiť, pretože 6, 12, 24 aj 48 sú párne. Zostávajú nám preto iba 3 možnosti, ktoré musíme vyskúšať. Rýchlo zistíme, že jediné riešenie je $p = 5$, pre ktoré dostaneme päticu čísel $(5, 11, 17, 29, 53)$.

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

7 bodov ♣

3A. V priestore je daných 9 bodov s celočíselnými súradnicami. Dokážte, že stred niektorej úsečky určenej týmito bodmi má tiež celočíselné súradnice.

Riešenie: Ak máme v priestore dva body, ktorých súradnice sú $[x_1, y_1, z_1]$ a $[x_2, y_2, z_2]$, tak stred úsečky určenej týmito bodmi je bod so súradnicami $\left[\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}, \frac{z_1+z_2}{2}\right]$. Preto ak koncové body úsečky budú mať celočíselné súradnice, tak stred tejto úsečky bude mať celočíselné súradnice práve vtedy, ak súčty x_1+x_2, y_1+y_2, z_1+z_2 budú P+P, alebo N+N, kde P označuje párne a N označuje nepárne číslo. Každé celé číslo je buď párne, alebo nepárne. Preto pre celočíselné súradnice bodu v priestore máme len 8 možností (P,P,P), (P,P,N), (P,N,P), (P,N,N), (N,P,P), (N,P,N), (N,N,P), (N,N,N). Ak máme v priestore 9 bodov s celočíselnými súradnicami, tak to podľa Dirichletovho princípu znamená, že medzi nimi musia byť aspoň 2 body, ktorých súradnice majú rovnakú paritu. To potom znamená, že stred úsečky určenej takýmito dvoma bodmi bude mať celočíselné súradnice.

---

7 bodov ♣

3B. V rovine je daných 17 bodov, ktoré tvoria vrcholy pravidelného 17-uholníka. Ľubovoľné dva rôzne body sú spojené buď modrou, alebo červenou, alebo zelenou úsečkou. Dokážte, že existuje trojuholník s vrcholmi v daných bodoch, ktorého všetky strany sú úsečky rovnakej farby.

Riešenie: Z každého, z daných 17 bodov, vychádza 16 úsečiek do ďalších bodov. Vyberme si jeden z daných bodov. Podľa Dirichletovho princípu musí mať aspoň 6 z neho vychádzajúcich úsečiek rovnakú farbu. Označne si túto farbu M. Pozrime sa teraz na tých 6 bodov, do ktorých ide úsečka farby M z nami vybraného bodu. Ak by niektoré dva z týchto 6 bodov boli spojené úsečkou farby M, tak máme trojuholník, ktorého všetky strany majú rovnakú farbu (M).

Predpokladajme teda, že žiadne dva zo skúmaných 6 bodov nie sú spojené úsečkou farby M. Sú teda medzi nimi iba úsečky farby Č, alebo Z. Vyberme si jeden z týchto 6 bodov. Vychádza z neho 5 úsečiek do ostatných 5 bodov. Podľa Dirichletovho princípu musia mať aspoň 3 z týchto úsečiek rovnakú farbu, označme ju Č. Skúmajme teraz tie 3 body, do ktorých z vybratého bodu idú úsečky farby Č. Ak by niektoré dva z nich boli spojené úsečkou farby Č, tak opäť máme trojuholník, ktorého všetky strany majú rovnakú farbu (Č).

V opačnom prípade musia byť skúmané 3 body spojené iba úsečkami farby Z, čím dostávame trojuholník, ktorého všetky strany majú rovnakú farbu (Z).

10 bodov

4A. Nájdite všetky riešenia rovnice $179x + 182y = 202505$ na množine prirodzených čísel (nulu tiež považujeme za prirodzené číslo).

Riešenie: Takýto typ rovnice sa nazýva (lineárna) *Diofantická rovnica* (podľa gréckeho matematika Diofanta) a spôsob jej riešenia je známy už od staroveku. Jeden zo spôsobov riešenia lineárnych diofantických rovníc je založený na použití Euklidovho algoritmu. Je to ten istý algortmus, ktorý slúži na nájdenie najväčšieho spoločného deliteľa dvoch celých čísel.

Ak máme rovnicu $Ax + By = C$, tak táto bude mať celočíselné riešenie práve vtedy, keď čísla $NSD(A, B)$ delí číslo C, pričom $NSD(A, B)$ označuje najväčší spoločný deliteľ čísel A a B. V našom prípade sú čísla 179 a 182 nesúdeliteľné, t. j. majú najväčší spoločný deliteľ 1 a 1 delí 202505, takže podmienka existencie riešenia je splnená. Postupným aplikovaním Euklidovho algoritmu dostaneme $NSD(182, 179)$ a zároveň aj jedno (partikulárne) riešenie danej rovnice.

$$\begin{aligned} 182 &= 1 \cdot \underline{179} + 3 \\ 179 &= 59 \cdot \underline{3} + 2 \\ 3 &= 1 \cdot \underline{2} + 1 \\ 2 &= 2 \cdot \underline{1} + 0 \end{aligned}$$

Z posledného riadku vidíme, že $NSD(182, 179) = 1$ a ďalej

$$182 = 1 \cdot \underline{179} + 3 \quad \Rightarrow \quad 3 = 182 - 1 \cdot 179 \tag{3}$$
$$179 = 59 \cdot \underline{3} + 2 \quad \Rightarrow \quad 2 = 179 - 59 \cdot 3 \tag{4}$$
$$3 = 1 \cdot \underline{2} + 1 \quad \Rightarrow \quad 1 = 3 - 2 \tag{5}$$

Dosadením (3) a (4) do (5) dostaneme

$$1 = 182 - 1 \cdot 179 - (179 - 59 \cdot 3) = 182 - 1 \cdot 179 - \big(179 - 59 \cdot (182 - 1 \cdot 179)\big) = -61 \cdot 179 + 60 \cdot 182$$

Potom $202505 = -12352805 \cdot 179 + 12150300 \cdot 182$. Toto riešenie je jedno (partikulárne) riešenie danej rovnice, nie je však jediné a ani nespĺňa podmienku, že x a y musia byť prirodzené čísla. Vieme však, že

$$Ax + By = C \;\Leftrightarrow\; A(x + tB) + B(y - tB) = C\,, \quad \text{pre } \forall t \in \mathbb{Z}\,.$$

Delením ľahko vypočítame, že najmenšie také $t \in \mathbb{Z}$, pre ktoré $-12352805 + t \cdot 182 \geq 0$, je $t = 67873$, čím dostávame prvé vyhovujúce riešenie, kde x a y sú prirodzené čísla. Spolu existuje 6 vyhovujúcich riešení danej úlohy. Sú to

$$\begin{aligned} (x, y) = (81, 1033) &\quad\to\quad 81 \cdot 179 + 1033 \cdot 182 = 202505 \\ (x, y) = (263, 854) &\quad\to\quad 263 \cdot 179 + 854 \cdot 182 = 202505 \\ (x, y) = (445, 675) &\quad\to\quad 445 \cdot 179 + 675 \cdot 182 = 202505 \\ (x, y) = (627, 496) &\quad\to\quad 627 \cdot 179 + 496 \cdot 182 = 202505 \\ (x, y) = (809, 317) &\quad\to\quad 809 \cdot 179 + 317 \cdot 182 = 202505 \\ (x, y) = (991, 138) &\quad\to\quad 991 \cdot 179 + 138 \cdot 182 = 202505 \end{aligned}$$

V prípade, ak by x a y mohli byť celé čísla, by daná rovnica mala nekonečne veľa riešení v tvare $(x, y) = (81 + t \cdot 182, 1033 - t \cdot 179)$ pre $\forall t \in \mathbb{Z}$.

10 bodov

4B. Nájdite všetky riešenia rovnice $\frac{1}{u}+\frac{1}{v}+\frac{1}{z}=1$ na množine prirodzených čísel.

Riešenie: Hľadáme riešenie rovnice $\frac{1}{u}+\frac{1}{v}+\frac{1}{z}=1$ na prirodzených číslach. Bez ujmy na všeobecnosti môžeme predpokladať, že $u \leq v \leq z$. Potom platí

$$\frac{1}{u} \geq \frac{1}{v} \geq \frac{1}{z} \quad \Rightarrow \quad \frac{1}{u}+\frac{1}{v}+\frac{1}{z}=1 \leq \frac{3}{u} \quad \Rightarrow \quad u \leq 3\,.$$

Z toho vyplýva, že najmenšie z čísel u, v, z musí byť menšie alebo rovné 3. Máme teda len 3 možnosti:

- ▷ $\mathbf{u=1}$: Potom musíme riešiť rovnicu $\frac{1}{v}+\frac{1}{z}=0$. Táto rovnica však nemá riešenie pre prirodzené čísla v a z.
- ▷ $\mathbf{u=2}$: Potom musíme riešiť rovnicu $\frac{1}{v}+\frac{1}{z}=\frac{1}{2}$. Rovnako, ako sme to robili vyššie, dostávame

  $$\frac{1}{v} \geq \frac{1}{z} \quad \Rightarrow \quad \frac{1}{v}+\frac{1}{z}=\frac{1}{2} \leq \frac{2}{v} \quad \Rightarrow \quad v \leq 4\,.$$

  Máme teda len 3 možnosti $v \in \{2,3,4\}$ (nezabúdajme, že $u \leq v \leq z$). Ľahko nahliadneme, že pre $v=1$ a $v=2$ rovnica nemá riešenie, pre $v=3$ dostaneme $z=\frac{1}{6}$ a pre $v=4$ dostaneme $z=4$.
- ▷ $\mathbf{u=3}$: Potom musíme riešiť rovnicu $\frac{1}{v}+\frac{1}{z}=\frac{2}{3}$. Rovnako, ako sme to robili vyššie, dostávame

  $$\frac{1}{v} \geq \frac{1}{z} \quad \Rightarrow \quad \frac{1}{v}+\frac{1}{z}=\frac{2}{3} \leq \frac{2}{v} \quad \Rightarrow \quad v \leq 3\,.$$

  Máme teda len 1 možnosť $v=3$ (opäť nezabúdajme, že $u \leq v \leq z$). Ľahko vypočítame, že potom aj $z=3$.

Spolu má teda rovnica $\frac{1}{u}+\frac{1}{v}+\frac{1}{z}=1$ tri riešenia na prirodzených číslach. Sú to trojice

$$(u,v,z)=(2,3,6)\,, \qquad (u,v,z)=(2,4,4)\,, \qquad (u,v,z)=(3,3,3)\,.$$

9 bodov ♡

5A. Pre nasledujúcu úlohu budeme potrebovať programovací jazyk používajúci „korytnačkovú grafiku“ (*turtle graphics*). Odporúčame použiť buď voľne dostupné *Berkeley Logo*, prípadne môžete použiť aj modul „korytnačka“ (*turtle*) pre jazyk Python. Cieľom je minimalizovať množstvo kódu mimo funkcie, ktorá sa volá rekurzívne. Dôležité je Vaše pochopenie logiky a jej vysvetlenie, takže všetko komentujte a podrobne vysvetlite, najmä pri použití rekurzie.

Napíšte program, ktorý pomocou Loga, alebo modulu *„turtle“*, nakreslí jednoduchý rekurzívny strom. Podmienky kreslenia stromu sú nasledovné:

- Kreslenie stromu sa začína s dĺžkou vetvy 100 jednotiek.
- Kreslenie stromu sa zastaví, ak dĺžka vetvy klesne pod 8 jednotiek.
- Kreslený strom bude asymetrický.
- Každá vetva sa rozvetvuje náhodne na dva až tri konáre s uhlami $-30°$, $0°$ a $+30°$ (rôzne vetvy, rôzne uhly).
- Dĺžka každej ďalšej vetvy sa bude náhodne skracovať v rozmedzí od 60 % do 90 % dĺžky predošlej vetvy.

Úlohy:

1. Koľkokrát sa rekurzívna funkcia zavolá, ak začíname so stromom dĺžky 100?
2. Napíšte verziu programu, v ktorej sa farba vetiev bude meniť podľa ich dĺžky.

Riešenie: Ukážka kódu (v jazyku Python s použitím modulu „korytnačka“) je na nasledujúcej strane. Tento kód využíva *rekurziu*, t. j. funkcia volá samu seba, a je v ňom implementované aj menenie farby vetvy podľa jej dĺžky.

V prvej otázke sme chceli vedieť, koľkokrát sa funkcia rekurzívne (samu seba) zavolá, ak začneme s dĺžkou 100. Keďže dĺžka vetiev je náhodná v rozsahu 60 % až 90 % z dĺžky predchádzajúcej vetvy, presný počet volaní sa nedá určiť, ale vieme odhadnúť jeho hranice (minimum a maximum).

Odhad sa robí nasledovne. Počet volaní bude najmenší vtedy, ak by sa v každom kroku dĺžka vetvy skracovala na 60 % predošlej dĺžky. Ľahko vypočítame, že $100 \cdot 0,6^4 \doteq 12,9$ a $100 \cdot 0,6^5 \doteq 7,7$. Takže po 5 krokoch by dĺžka vetvy klesla pod 8. Naopak, počet volaní bude najväčší vtedy, ak by sa v každom kroku dĺžka vetvy skracovala na 90 % predošlej dĺžky. Ľahko vypočítame, že $100 \cdot 0,9^{23} \doteq 8,8$ a $100 \cdot 0,9^{24} \doteq 7,9$. Takže až po 24 krokoch by dĺžka vetvy klesla pod 8.
Preto odpoveď bude: rekurzívnych volaní funkcie bude od 5 do 24.

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

```
import turtle
import random

# Rekurzívna funkcia
def kresli_strom(dlzka):
    if dlzka < 8:
        return

    ratio = (dlzka - 8) / (100 - 8)
       # tento blok kódu prefarbuje čiary pre každú dĺžku, toto riešenie
       # je univerzálne a relatívne komplikované, akékolvek riešenie
       # zfarbenia bude akceptované
    r = int(139 - ratio * (139 - 34))
    g = int(69 + ratio * (139 - 69))
    b = int(19 + ratio * (34 - 19))
    turtle.pencolor(r/255, g/255, b/255)
    turtle.pensize(max(1, dlzka/20))

    turtle.forward(dlzka)

    pocet_vetiev = random.randint(2, 3) #vyberie, či počet vetiev bude 2 alebo 3

    i = 0
    while pocet_vetiev > i:
        i = i + 1
        list_uhlov = [-30, 0, 30] #zoznam uhlov
        r = random.randint(0, 2) #vyberie uhol
        turtle.left(list_uhlov[r]) #otočí o uhol
        nova_dlzka = dlzka * random.uniform(0.6, 0.8) #vyberie novú dlžku
        kresli_strom(nova_dlzka) #rekurzívne volanie
        turtle.right(list_uhlov[r]) #otočí naspäť

    turtle.backward(dlzka)                        # návrat na začiatok vetvy

turtle.speed(0)
turtle.left(90)
turtle.up()
turtle.goto(0, -250)
turtle.down()

kresli_strom(100)
turtle.done()
```

9 bodov ♡

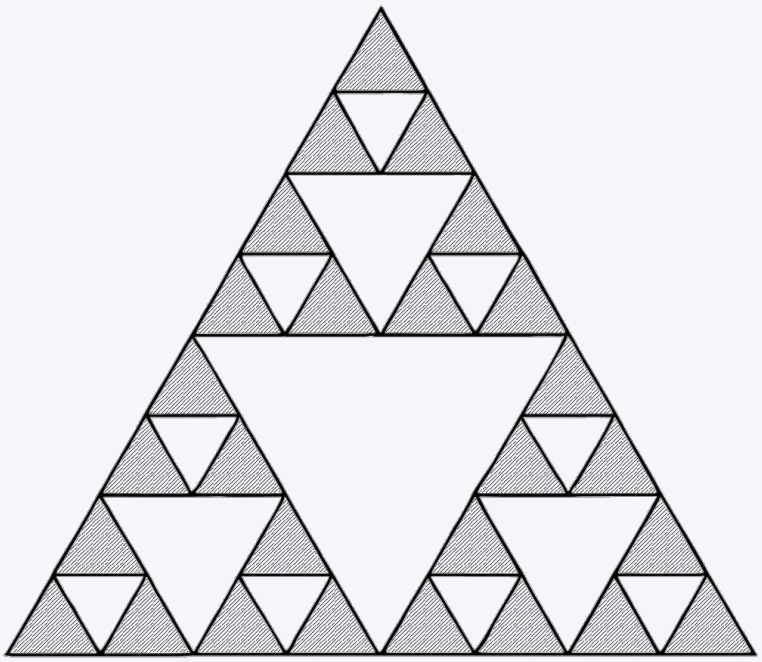
5B. Pre nasledujúcu úlohu budeme potrebovať programovací jazyk používajúci „korytnačkovú grafiku“ (*turtle graphics*). Odporúčame použiť buď voľne dostupné *Berkeley Logo*, prípadne môžete použiť aj modul „korytnačka“ (*turtle*) pre jazyk Python. Cieľom je minimalizovať množstvo kódu mimo funkcie, ktorá sa volá rekurzívne. Dôležité je Vaše pochopenie logiky a jej vysvetlenie, takže všetko komentujte a podrobne vysvetlite, najmä pri použití rekurzie.

Napíšte program, ktorý pomocou Loga, alebo modulu *„turtle“*, nakreslí nasledovný útvar:

- Najskôr sa nakreslí veľký rovnostranný trojuholník so stranou dlhou 200 jednotiek.
- Stredy strán nakresleného trojuholníka sa spoja úsečkami, čím sa pôvodný trojuholník rozdelí na 4 rovnaké rovnostranné trojuholníky. Prostredný trojuholník (na ilustračnom obrázku biely=nevyšráfovaný) sa vyhodí. Z pôvodného trojuholníka zostanú len 3 vyšráfované trojuholníky pri jeho vrcholoch.
- V každej ďalšej iterácii (kroku) sa všetky vyšráfované trojuholníky z predošlého kroku rozdelia na štyri rovnako veľké rovnostranné trojuholníky tak, že sa stredy ich strán spoja úsečkami a prostredné trojuholníky sa vyhodia. Viď ilustračný obrázok.
- Popísaný proces sa bude opakovať rekurzívne dovtedy, kým veľkosť strany trojuholníka neklesne pod 10 jednotiek.

Váš program musí byť riadne okomentovaný a súčasťou riešenia musí byť aj vysvetlenie postupu. Šráfovanie zostávajúcich trojuholníkov nerobte! To je na ilustračnom obrázku len pre lepšie pochopenie postupu.

Príklad trojuholníkov po 3 iteráciach:



Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

Riešenie: Nižšie je uvedená ukážka kódu (v jazyku Python s použitím modulu „korytnačka“). Tento kód využíva *rekurziu*, t. j. funkcia volá samu seba.

```
import turtle  # Importujeme modul na kreslenie pomocou "korytnačky"

# Rekurzívna funkcia na kreslenie trojuholníka a menších trojuholníkov na jeho stranách
def draw_triangle(size):
    if size < 10:
        # Ak je trojuholník príliš malý, ukončíme rekurziu
        return

    for _ in range(3):
        turtle.forward(size)    # Nakreslíme jednu stranu trojuholníka
        turtle.right(120)       # Otočíme sa doprava o 120 stupňov

        # Posunieme sa do stredu práve nakreslenej strany
        turtle.penup()
        turtle.forward(size / 2)
        turtle.pendown()

        # Rekurzívne nakreslíme menší trojuholník v strede tejto strany
        draw_triangle(size / 2)

        # Vrátime sa naspäť na pôvodné miesto pred kreslením menšieho trojuholníka
        turtle.penup()
        turtle.backward(size / 2)
        turtle.pendown()

# --- Nastavenie korytnačky a spustenie kreslenia ---
turtle.left(60)
turtle.speed(0)         # Nastavíme najrýchlejšie kreslenie
turtle.penup()
turtle.goto(-150, -100) # Posunieme sa na vhodné miesto, aby bol výstup na obrazovke vycentrovaný
turtle.pendown()

draw_triangle(200)      # Spustíme kreslenie hlavného trojuholníka veľkosti 200

turtle.done()           # Ukončíme kreslenie (necháme okno otvorené)
```

10 bodov

6A. Dešifrujte nasledujúci text a zistite akou transpozičnou šifrou je zašifrovaný (zistite názov šifry a šifrovací kľúč / heslo).

NTTEEOXTETZJIAFSAONVIYFSURKODAIRLNAACRHIIEELXUXX

Riešenie: Ak si pozrieme začiatok zašifrovaného textu, tak nám udrie do očí postupnosť písmen NTTEEOXTET..., ktorá je anagramom slov TENTOTEXT. S najväčšou pravdepodobnosťou sa preto jedná o transpozičnú šifru a musíme zistiť podľa akého kľúča a akým spôsobom sú poprehadzované písmena otvoreného textu.

Skúsme vytvoriť vhodnú permutáciu písmen a overiť svoju hypotézu. Pokúsime sa na začiatku textu vytvoriť slovo TENTO. Zo zašifrovaného textu skúsime zobrať 2. písmeno (T) (mohlo by to byť aj 3., to zatiaľ nevieme), potom 4. písmeno (E), potom 1. písmeno (N), potom 3. písmeno (T) a nakoniec 6. písmeno (O). Slovo TENTO sme vytvorili vybraním znakov zašifrovaného textu v poradí $(2, 4, 1, 3, 6)$. Usporiadanej pätici $(2, 4, 1, 3, 6)$ sa hovorí *permutácia* a tejto konkrétnej permutácii sa hovorí *kryptografický sled*, ktorý určuje v akom poradí musíme vyberať písmená otvoreného textu, aby sme dostali zašifrovaný text. Tento kryptografický sled určite nie je správny, alebo nie je kompletný, pretože kryptografický sled dĺžky n musí obsahovať všetky čísla od 1 po n. Mohli by sme ho buď skúsiť predĺžiť, alebo skrátiť. Vidíme však, že prvé 4 cifry sú $(2, 4, 1, 3)$, čo by mohol byť kompletný kryptografický sled. Kryptografickému sledu $(2, 4, 1, 3)$ zodpovedá permutácia $(3, 1, 4, 2)$, ktorá sa nazýva *anagramový sled*. Anagramový sled určuje v akom poradí musíme zo zašifrovaného textu vyberať písmená, aby sme dostali otvorený text.
Vysvetlenie: pri transpozičných šifrách sa šifruje pomocou kryptografického sledu a dešifruje sa pomocou anagramového sledu.

Skúsme teraz nájdenú permutáciu (anagramový sled) aplikovať na písmená zašifrovaného textu a zistiť, čo dostaneme

3	1	4	2	3	1	4	2	3	1	4	2
N	T	T	E	E	O	X	T	E	T	Z	J

→ TENT OTEX TJEZ...

Vidíme, že aj pokračovanie textu dáva zmysel, tak skúsime aplikovať nájdený anagramový sled na celý zašifrovaný text a dostaneme

TENT OTEX TJEZ ASIF OVAN YSIF ROUK ARDI NALA RICH ELIE UXXX

Dostali sme v podstate zmysluplný text. Text hovorí, že otvorený text bol zašifrovaný šifrou kardinála Richelieu. Pri tejto šifre sa musí otvorený text rozdeliť na skupiny písmen, ktoré majú rovnakú dĺžku ako kryptografický sled. Ak nám na konci textu nejaké písmená chýbajú do počtu, tak sa doplnia náhodne (to sú tie XXX na konci). Ak vyhodíme doplnené XXX a dáme do textu prirodzené medzery dostaneme

TENTO TEXT JE ZASIFOVANY SIFROU KARDINALA RICHELIEU

Ako môžeme vidieť, v slove ZASIFROVANY chýba písmeno R. Pri ručných šifrách sa doporučovalo robiť v otvorenom texte úmyselné chyby a preklepy, ktorých cieľom bolo zmiasť nepriateľa a sťažiť mu lúštenie. V tomto prípade sa priznávam, že preklep vznikol ako neúmyselná chyba autora úlohy.

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

10 bodov

6B. Substitučná šifra, ktorou je zašifrovaný nasledujúci text, bola navrhnutá v roku 1854. Britská armáda ju používala v Búrskej vojne a potom aj počas I. svetovej vojny a II. svetovej vojny ako poľnú šifru.
Keď túto šifru lord Playfair predvádzal britskému ministrovi zahraničia, tak ten ju neodporučil, pretože sa mu zdala príliš zložitá. Potom lord Playfair predviedol túto šifru v miestnej škole, kde sa ju žiaci veľmi rýchlo naučili bezchybne používať. Keď o tom spolu s autorom šifry hovorili ministrovi zahraničia, tak ten im údajne odpovedal: *„Áno džentlmeni, to je síce možné, ale naši diplomati sa to nikdy nenaučia.“*
Dešifrujte nasledujúci text.

```
KMNUG TVZAL HJUDT FVQUZ GCILA CETAM NKBSE JOJUS HJKMN UGTVZ
JNLAO EASUS LNLEO TPBTJ XVVOI TAOSF ASAMA LCHTO OGDLF UNESE
ROXOF SVHYO EZJAJ ABOVQ UTALB SBEHJ ESDMR VLGEL CPAMN JHJMX
UIALB JROAV HMIOB GHULO RNGMP JVAHU GLJGA MEVLI AGJGR OVQUX
OTALC HNGBG EHMEV LILGO GXDVR VROJN IOHJA LBJRO AVHML ALMJT GL
```

Riešenie: Už z krátkeho úvodného textu sme vydedukovali, že v tejto úlohe budeme riešiť šifru, ktorú lord Playfair predstavoval ministrovi zahraničia. Po vyhľadaní tejto šifry (knihy, internet) zistíme, že táto šifra sa na počesť lorda Playfaira, ktorý bol jej propagátorom, volá *Playfairova šifra*, hoci jej autorom bol Charles Wheatstone.

Riešenie úlohy začneme krátkym objasnením algoritmu Playfairovej šifry, lebo pre ďalší postup bude dôležité rozumieť postupu šifrovania a dešifrovania Playfairovou šifrou.

Playfairova šifra patrí medzi bigramové substitúcie. To znamená, že bigram (dvojicu po sebe idúcich písmen) otvoreného textu nahrádzame bigramom zašifrovaného textu. Text teda šifruje po dvojiciach po sebe idúcich písmen. Pracuje so šifrovacou abecedou usporiadanou do mriežky 5x5 (niekedy aj 6x6 – písmená + číslice, prípadne písmená s diakritikou), ktorú nazývame Playfairov štvorec. Do takejto mriežky je možné vložiť 25 (alebo 36) znakov. Keďže anglická abeceda má 26 znakov, najmenej frekventované písmeno anglického jazyka J sa spája s písmenom I. To znamená, že J v anglofónnom Playfairovom štvorci obvykle nenájdeme. V slovenčine sa z rovnakého dôvodu spája písmeno W s písmenom V, prípadne sa vynecháva písmeno Q. Playfairov štorec pre slovenský jazyk potom môže vyzerať nasledovne

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	x	y	z

Pozor! Písmená vo štvorci obvykle nie sú usporiadané podľa abecedy, ale môžu byť usporiadané ľubovoľne. Je to dokonca vítané, keďže práve znalosť štvorca rozhoduje o schopnosti úspešne dešifrovať zašifrovaný text. Najčastejšie sa písmená vo štvorci zamiešajú pomocou dohodnutého hesla. Tak aj druhá strana šifrovanej komunikácie dokáže štvorec ľahko zrekonštruovať a prečítať správu. Generovanie štvorca podľa hesla prebieha takým spôsobom, že do prázdnej mriežky

zapíšeme najskôr heslo, pričom opakujúce sa písmená vynecháme (berie sa vždy len prvý výskyt písmena) a potom zapíšeme zvyšné písmená abecedy usporiadané podľa abecedy. Ak je heslo KRYPTOGRAFIA, tak dostaneme nasledovný Playfairov štvorec

k	r	y	p	t
o	g	a	f	i
b	c	d	e	h
j	l	m	n	q
s	u	v	x	z

Šifrovanie / dešifrovanie pomocou Playfairovho štvorca sa riadi nasledujúcimi pravidlami. Písmená bigramu, ktorý šifrujeme / dešifrujeme, môžu ležať v Playfairovom štvorci buď v rovnakom riadku, alebo v rovnakom stĺpci, alebo ležia v rôznych riadkoch a stĺpcoch. Rozlišujeme preto nasledujúce tri možnosti:

1. **Rovnaký riadok:** Ak obe písmená bigramu ležia v tom istom riadku, tak bigram zašifrovaného textu dostaneme tak, že každé písmeno sa cyklicky posunie o jeden stĺpec doprava.

2. **Rovnaký stĺpec:** Ak sú obe písmená bigramu v tom istom stĺpci, tak bigram zašifrovaného textu dostaneme tak, že každé písmeno sa cyklicky posunie o jeden riadok nadol.

3. **Rôzny riadok aj stĺpec:** Ak obe písmená bigramu ležia v rôznych riadkoch a rôznych stĺpcoch Playfairovej tabuľky, tak v nej tvoria dva vrcholy obdĺžnika. Bigram zašifrovaného textu dostaneme tak, že každé písmeno sa nahradí písmenom ležiacim v rovnakom riadku a tvoriacim vrchol spomenúteho obdĺžnika (ležiacim v tom istom stĺpci ako druhé písmeno šifrovaného bigramu).

Z týchto pravidiel vyplýva, že dešifrovanie prebieha analogicky. V uvedených pravidlách stačí obrátiť v prvých dvoch pravidlách slová doprava / doľava, nadol / nahor.
Vo všeobecnosti existujú tri možné prístupy využívané na prelamovanie Playfairovej šifry.

1. Frekvenčná analýza V prípade dostatočne dlhého textu je možné porovnať frekvenciu bigramov v zašifrovanom texte s frekvenciou bigramov slovenského jazyka. Je to však veľmi komplikovaný postup a Playfairova šifra patrí medzi šifry, pri ktorých je frekvenčná analýza veľmi komplikovaná. Naviac náš text obsahuje iba 86 rôznych bigramov, z ktorých až 81 má absolútnu početnosť 1. To znamená, že pri riešení nášho textu nám frekvenčná analýza nepomôže.

2. Prístup hrubou silou Keďže abeceda má konečný počet písmen, existuje konečný počet možností ako písmená v Playfairovom štvorci usporiadať. Takých možností je však príliš veľa na ručné lúštenie a aj pre bežný počítač by to bolo na hrane, alebo už za hranou realizovateľnosti.

3. Kombinovaný prístup Ide o kombináciu rôznych metód. Môžu to byť prvé dve spomenuté metódy, prípadne hádanie predpokladaných slov. Hádať predpokladané slová môžeme, ak je známy účel komunikácie. V našom prípade sa v texte úlohy hovorí o Playfairovej šifre, v texte sa opakujú reťazce `KMNUGTVZ`, môžeme preto predpokladať, že

```
KM NU GT VZ = PL AY FA IR
```

.

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

Do úvahy prichádza ešte aj reťazec `AL BJ RO AV HM`, ktorý sa v texte tiež vyskytuje dvakrát. Budeme preto pracovať s týmito dvoma alternatívami a ukáže sa, že hneď tá prvá je správna.

Ako sme spomenuli vyššie, Playfairova šifra využíva tri pravidlá na šifrovanie dvojice písmen. To znamená, že každý zo štyroch bigramov slova `PL AY FA IR` mohol vzniknúť troma spôsobmi. Skúmať všetky tri možností by bolo zdĺhavé, aj keď niekedy sa tomu vyhnúť nedá. Je však výrazne pravdepodobnejšie, že písmená bigramu ležia vo vrcholoch obdĺžnika, než to, že ležia v tom istom riadku, alebo v tom istom stĺpci. Pre začiatok preto budeme predpokladať, že slovo `PLAYFAIR` bolo zašifrované len podľa 3. pravidla a až keď týmto spôsobom nedostaneme žiadne riešenie, skúsime prvé dve pravidlá.

Teraz sa sústreďme na rekonštrukciu samotného Playfairovho štvorca. Zvolíme `KM NU GT VZ` ako kandidáta na slovo `PL AY FA IR`. Zo stanovenej hypotézy potom vyplýva nasledovné:

1. písmená `P, K` sú spolu v jednom riadku a písmená `L, M` sú spolu v inom riadku,
2. písmená `A, N` sú spolu v jednom riadku a písmená `Y, U` sú spolu v inom riadku,
3. písmená `F, G` sú spolu v jednom riadku a písmená `A, T` sú spolu v inom riadku,
4. písmená `I, V` sú spolu v jednom riadku a písmená `R, Z` sú spolu v inom riadku.

Okrem toho, vzhľadom na zostavovanie Playfairovho štvorca pomocou hesla, môžeme predpokladať, že pízmeno `Z` s vysokou pravdepodobnosťou leží v pravom dolnom rohu štvorca. Aplikovaním týchto faktov a predpokladov môžeme zostaviť napríklad nasledovný Playfairov štvorec

v		l	m	i
t	a		n	
f	g	k	p	
r	u		y	z

Samozrejme možností ako uvedené znaky umiestniť je viac a treba ich skúšať, pokiaľ nám pomocou ich usporiadania nezačne pri dešifrovaní vychádzať zmysluplný text. Hľadanie správneho usporiadania uvedených písmen nám uľahčí (výrazne zredukuje počet možností) to, že v zašifrovanom texte budeme hľadať bigramy tvorené rôznymi kombináciami znakov `K M N U G T V Z`, čo nám napovie, v akom vzťahu sú v Playfairovom štvorci štyri obdĺžniky tvorené znakmi `PKLM ANYU FGAT IVRZ`. Okrem toho, ak predpokladáme, že Playfairov štvorec bol zostavený pomocou hesla, tak v prvom riadku štvorca musí byť ešte aj písmeno `E`. Štvorec potom bude

v	e	l	m	i
t	a		n	
f	g	k	p	
r	u		y	z

Pokračovať v lúštení môžeme napríklad tak, že budeme analyzovať početnosť jednotlivých bigramov v zašifrovanom texte. Viac ako dvakrát sa v texte vyskytujú nasledovné bigramy

bigram	AL	HJ	RO	AM	VQ
početnosť	6	5	5	4	3

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})

Asociujme tieto bigramy s najfrekventovanejšími bigramami slovenského jazyka ako napríklad `JE, SI, NA, NE, ...` Najpočetnejšie `AL` sa vyskytuje v prvom riadku hneď za hypotetickým slovom `PLAYFAIR`. Mohlo by ísť o začiatok vety `PLAYFAIR JE ...`? Ako text to zatiaľ dáva zmysel.

Jediný spôsob, ako v našom (predpokladanom) Playfairovom štvorci môžeme `JE` šifrovať na `AL`, je uplatniť tretie (najpravdepodobnejšie) pravidlo o šifrovaní pomocou obdĺžnika. Potom by sa písmeno `J` vo štvorci nachádzalo v druhom riadku a v treťom stĺpci. Výsledkom je štvorec

v	e	l	m	i
t	a	j	n	
f	g	k	p	
r	u		y	z

Zo zatiaľ nekompletného štvorca je možné nájsť asociácie pre 30 ďalších bigramov. Po dešifrovaní textu pomocou nekompletného Playfairovho štvorca dostávame text

PLAYFAIRJEHJUDTFVQUZGC**ME**AC**VANEJP**BS**LA**OJUSHJ**PLAYFAIR**
JN**EJ**OEASUS**MJEV**OTPBTJXVVOITAOSFAS**NEJE**CHTOOGDL**GRAM**SEROXOF
SVHYO**IUATAT**BOVQUT**JE**BSBEHJESDM**FREKVE**CP**NEJA**HJMX**ZEJE**BJRO
TEHMIOBGHULO**YTPEKNER**HU**KEAKNEVIEM**AG**AK**ROVQUXOT**JE**CH
APBGEH**LVIEME**GOGXDV**FR**RO**AJ**IOHJ**JE**BJRO**TE**HM**EJEL**JT**KE**

V uvedenom texte už je možné vidieť náznaky slov ako napríklad *menovanej*, alebo *pomenovanej* v 1. riadku, *frekvencnej* v 3. riadku, *je lahke* na konci textu. Pomocou týchto slov vieme v Playfairovom štvorci doplniť ďalšie znaky, opäť dešifrujeme text, nájdeme v ňom ďalšie slová, doplníme ďalšie znaky atď. Nakoniec dostaneme kompletný Playfairov štvorec

v	e	l	m	i
t	a	j	n	h
s	l	b	c	d
f	g	k	p	q
r	u	x	y	z

Rozlúštený text znie

```
PLAYFAIR JE NAZOV SIFRY POMENOVANEJ PODLA BARONA PLAYFAIRA JEJ
AUTOROM JE VSAK CHARLES WHEATSTONE JEDNA SA O BIGRAMOVU
SUBSTITUCIU A TATO SIFRA JE ODOLNA VOCI FREKVENCNEJ ANALYZE JEJ
LUSTENIE DOKAZE BYT PEKNE TAZKE AK NEVIEME O AKU SIFRU SA
JEDNA POKIAL VIEME O AKU SIFRU SA JEDNA JEJ LUSTENIE JE LAHKE
```

Veľmi dobrým nástrojom uľahčujúcim prácu s bigramami je Bigrams Frequency Analysis. Na rovnakej stránke `https://www.dcode.fr` nájdete aj *PlayFair Decoder*, ktorý nám uľahčí overovanie Playfairových štvorcov, ale iba v prípade ak už máme kompletný Playfairov štvorec.

Termín odovzdania: 31. 5. 2025 (riešenia musia byť odovzdané do 24^{00})