6 bodov ♣

1A. Dané je dvojciferné číslo, ktorého ciferný súčet je 8. Keď prehodíme poradie cifier daného čísla, tak dostaneme číslo o 36 menšie. Aké je dané číslo?

Riešenie: Dané číslo si môžeme zapísať ako xy, kde $x, y \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ sú jeho cifry a $x \neq 0$. Jeho ciferný súčet je 8, a preto platí $x + y = 8$. Hodnotu čísla xy vieme vyjadriť ako $10x+y$. Ďalej vieme, že ak prehodíme poradie cifier daného čísla, tak dostaneme číslo o 36 menšie. To znamená, že platí $10x + y - (10y + x) = 36$, čo po úprave znamená $x - y = 4$. Pre cifry x a y teda platí

$$\begin{array}{ccccc} x & + & y & = & 8 \\ x & - & y & = & 4 \end{array}$$

Toto je jednoduchá sústava dvoch lineárnych rovníc o dvoch neznámych, ktorej riešením je $x = 6$ a $y = 2$. Dané číslo je 62.

---

6 bodov ♣

1B. Dané je trojciferné číslo, ktorého ciferný súčet je 14. Ak jeho cifry zapíšeme v opačnom poradí, tak dostaneme číslo, ktoré je o 99 väčšie než pôvodné číslo. A ak prehodíme poradie jeho prvých dvoch (zľava) cifier, tak dostaneme číslo, ktoré je o 360 väčšie než pôvodné číslo. Aké je dané číslo?

Riešenie: Dané číslo si môžeme zapísať ako xyz, kde $x, y, z \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ sú jeho cifry, $x \neq 0$ a kvôli tretej podmienke zo zadania aj $y \neq 0$. Jeho ciferný súčet je 14, a preto platí $x + y + z = 14$. Hodnotu čísla xyz vieme vyjadriť ako $100x + 10y + z$. Druhá podmienka hovorí, že ak cifry daného čísla zapíšeme v opačnom poradí, tak sa jeho hodnota zväčší o 99. Čiže musí platiť $100z + 10y + x - (100x + 10y + z) = 99$ z čoho po úprave dostaneme $z - x = 1$. Tretia podmienka hovorí, že ak vymeníme poradie prvých dvoch cifier, tak dostaneme číslo o 360 väčšie. To znamená $100y + 10x + z - (100x + 10y + z) = 360$ z čoho po úprave dostaneme $y - x = 4$. Pre cifry x, y a z teda platia rovnice

$$\begin{array}{ccccccc} x & + & y & + & z & = & 14 \\ -x & & & + & z & = & 1 \\ -x & + & y & & & = & 4 \end{array}$$

Toto je jednoduchá sústava troch lineárnych rovníc o troch neznámych, ktorej riešením je $x = 3$, $y = 7$ a $z = 4$. Dané číslo je 374.

7 bodov

2A. Dokážte, že číslo $2^{180}+36$ je deliteľné číslom 37.

Riešenie: Číslo 2^{180} môžeme zapísať nasledovným spôsobom

$$2^{180}=\left(2^5\right)^{36}=(37-5)^{36}=37^{36}-\binom{36}{1}37^{35}\cdot 5^1+\binom{36}{2}37^{34}\cdot 5^2+\cdots-\binom{36}{35}37^1\cdot 5^{35}+5^{36}$$

Pri roznásobovaní zátvorky $(37-5)^{36}$ sme použili binomickú vetu. V takmer všetkých členoch posledného výrazu, okrem posledného členu 5^{36}, sa vyskytuje číslo 37 v nejakej mocnice väčšej než 1, a preto sú všetky tieto členy deliteľné číslom 37. Ďalej budeme skúmať už len číslo 5^{36}. To sa dá rozpísať ako

$$5^{36}=\left(5^3\right)^{12}=(125)^{12}=(3\cdot 37+14)^{12}=$$

$$=(3\cdot 37)^{12}+\binom{12}{1}(3\cdot 37)^{11}\cdot 14^1+\binom{12}{2}(3\cdot 37)^{10}\cdot 14^2+\cdots+\binom{12}{11}(3\cdot 37)^1\cdot 14^{11}+14^{12}$$

Opäť, v takmer všetkých členoch posledného výrazu, okrem posledného čísla 14^{12}, sa vyskytujú mocniny čísla 37 väčšie než 1, a preto sú všetky tieto členy deliteľné číslom 37. Zostáva nám preto preskúmať číslo 14^{12}.

$$14^{12}=\left(14^3\right)^4=(2744)^4=(74\cdot 37+6)^4=$$

$$=(74\cdot 37)^4+\binom{4}{1}(74\cdot 37)^3\cdot 6^1+\binom{4}{2}(74\cdot 37)^2\cdot 6^2+\binom{4}{3}(74\cdot 37)^1\cdot 6^3+6^4$$

V takmer všetkých členoch posledného výrazu, okrem posledného čísla 6^4, sa vyskytujú mocniny čísla 37 väčšie než 1, a preto sú všetky tieto členy deliteľné číslom 37. Zostáva nám preto preskúmať už len číslo 6^4.

$$6^4=\left(6^2\right)^2=(37-1)^2=37^2-2\cdot 37+1$$

Prvé dva členy posledného výrazu sú deliteľné číslom 37 a zostalo nám iba číslo 1. Z uvedeného vidno, že $2^{180} \bmod 37=1$, inak povedané, číslo 2^{180} má po delení číslom 37 zvyšok 1. A preto je číslo $2^{180}+36$ deliteľné číslom 37.

7 bodov

2B. Dokážte, že číslo $3^{96}+14$ je deliteľné číslom 79.

Riešenie: Číslo 3^{96} môžeme zapísať nasledovným spôsobom

$$3^{96} = \left(3^4\right)^{24} = (79+2)^{24} = 79^{24} + \binom{24}{1}79^{23}\cdot 2^1 + \binom{24}{2}79^{22}\cdot 2^2 + \cdots + \binom{24}{23}79^1\cdot 2^{23} + 2^{24}$$

Pri roznásobovaní zátvorky $(79+2)^{24}$ sme použili binomickú vetu. V takmer všetkých členoch posledného výrazu, okrem posledného členu 2^{24}, sa vyskytuje číslo 79 v nejakej mocnice väčšej než 1, a preto sú všetky tieto členy deliteľné číslom 79. Ďalej budeme skúmať už len číslo 2^{24}. To sa dá rozpísať ako

$$2^{24} = \left(2^6\right)^4 = (79-15)^4 = 79^4 + \binom{4}{1}79^3\cdot 15^1 + \binom{4}{2}79^2\cdot 15^2 + \binom{4}{3}79^1\cdot 15^3 + 15^4$$

Opäť, v takmer všetkých členoch posledného výrazu, okrem posledného čísla 15^4, sa vyskytujú mocniny čísla 79 väčšie než 1, a preto sú všetky tieto členy deliteľné číslom 79. Zostáva nám preto preskúmať už len číslo 15^4.

$$15^4 = \left(15^2\right)^2 = 225^2 = (2\cdot 79+67)^2 = 4\cdot 79^2 + 4\cdot 79\cdot 67 + 67^2$$

Prvé dva členy posledného výrazu sú deliteľné číslom 79 a zostalo nám iba číslo

$$67^2 = 4489 = 56\cdot 79 + 65$$

Z uvedeného vidno, že $3^{96} \bmod 79 = 65$, inak povedané, číslo 3^{96} má po delení číslom 79 zvyšok 65. A preto je číslo $3^{96}+14$ deliteľné číslom 79.

8 bodov

♡

3A. Daná je rovnica $2x + 8y + 14z = 2027$, kde x, y, z môžu byť len celé čísla. Zistite, či existuje celočíselné riešenie tejto rovnice a ak áno, nájdite ho.

Riešenie: Celočíselné riešenie danej rovnice neexistuje. Čísla $2x$, $8y$ a $14z$ sú pre ľubovoľné $x, y, z \in \mathbb{Z}$ párne a súčet párnych čísel je párne číslo. Na ľavej strane rovnice $2x + 8y + 14z = 2027$ máme párne číslo a na pravej strane máme nepárne číslo. Preto daná rovnica nemôže mať celočíselné riešenie.

---

8 bodov

♡

3B. Dané sú dve prirodzené čísla a, b. Označme si $\operatorname{nsd}(a, b)$ **najväčší spoločný deliteľ** čísel a, b a $\operatorname{nsn}(a, b)$ **najmenší spoločný násobok** čísel a, b. Dokážte, že platí

$$a \cdot b = \operatorname{nsd}(a, b) \cdot \operatorname{nsn}(a, b) .$$

Riešenie: V tejto úlohe je kľúčové využitie *Základnej vety aritmetiky* (klikateľná linka), ktorá hovorí, že každé prirodzené (celé) číslo sa dá jednoznačne (jediným spôsobom) zapísať ako súčin mocnín prvočísel. Inak povedané

$$\forall a \in \mathbb{N}, a \neq 0, a \neq 1 : \quad a = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

pričom všetky p_i sú prvočísla, všetky m_i sú prirodzené čísla také, že $m_i \neq 0$ a tento zápis / rozklad je jediný možný.

Pozrime sa teraz na to ako je definovaný $\operatorname{nsd}(a, b)$. Je to najväčie prirodzené číslo, ktorým sú súčasne deliteľné obe čísla a a b. Preto prvočíselný rozklad čísla $\operatorname{nsd}(a, b)$ pozostáva zo všetkých prvočísel, ktoré sa nachádzajú v rozklade oboch čísel a a b zároveň.
Analogicky $\operatorname{nsn}(a, b)$ je najmenšie prirodzené číslo, ktoré je deliteľné oboma číslami a aj b. Preto prvočíselný rozklad $\operatorname{nsn}(a, b)$ musí obsahovať všetky prvočísla, ktoré sú v rozkladoch čísel a a b, pričom prvočísla, ktoré sa nachádzajú v rozkladoch a aj b súčasne, sa v rozklade $\operatorname{nsn}(a, b)$ budú vyskytovať len raz.

Teraz číslo a zapíšeme ako $a = \alpha \cdot \beta$, kde α je súčin všetkých tých prvočísel z prvočíselného rozkladu čísla a, ktoré sa nachádzajú aj v prvočíselnom rozklade číšla b a β je súčin zvyšných prvočísel z prvočíselného rozkladu čísla a. Podobne číslo b rozložíme na $b = \alpha \cdot \gamma$. Potom platí

$$\begin{aligned} a \cdot b &= (\alpha \cdot \beta) \cdot (\alpha \cdot \gamma) = \alpha^2 \cdot \beta \cdot \gamma \\ \operatorname{nsd}(a, b) \cdot \operatorname{nsn}(a, b) &= \alpha \cdot (\alpha \cdot \beta \cdot \gamma) = \alpha^2 \cdot \beta \cdot \gamma \end{aligned}$$

Z uvedeného vidno, že $a \cdot b = \operatorname{nsd}(a, b) \cdot \operatorname{nsn}(a, b)$, čo bolo treba dokázať.

14 bodov

4A. Dokážte, že pre ľubovoľné prirodzené číslo n platí $7 \mid (n^7 - n)$. Zápis $a \mid b$ pre celé čísla a, b znamená *„číslo a delí číslo b bez zvyšku"*, alebo inak zapísané $b = k \cdot a$, kde $k \in \mathbb{Z}$.

Riešenie: Polynóm (mnohočlen) $(n^7 - n)$ sa dá rozložiť na $n\,(n^6 - 1)$ a to sa dá ďalej rozložiť

$$n^7 - n = n\left(n^3 - 1\right)\left(n^3 + 1\right)$$

Koreňom polynómu $(n^3 - 1)$ je 1, t. j. tento polynóm je deliteľný koreňovým činiteľom $(n - 1)$ a podobne koreňom polynómu $(n^3 + 1)$ je -1, t. j. tento polynóm je deliteľný koreňovým činiteľom $(n + 1)$. Delením polynómov (môžeme to spraviť aj pomocou Hornerovej schémy) dostaneme rozklad

$$n^7 - n = (n-1)n(n+1)\left(n^2 + n + 1\right)\left(n^2 - n + 1\right) \tag{1}$$

Na pravej strane máme súčin piatich činiteľov. Čísla $(n - 1)$, n a $(n + 1)$ sú tri **po sebe idúce** prirodzené čísla. Znamená to, že ak $7 \mid n$, alebo má n po delení číslom 7 zvyšok 1 alebo 6, tak súčin na pravej strane (1) bude deliteľný číslom 7, čo sme potrebovali ukázať. Ako je to ale v prípade, ak má n po delení číslom 7 zvyšok 2, 3, 4 alebo 5? Zvyšky jednotlivých činiteľov výrazu (1) si uvedieme v nasledovnej tabuľke.

$n \bmod 7$	$(n-1)n(n+1)$	n^2+n+1	n^2-n+1
0	0 ✓	1	1
1	0 ✓	3	1
2	6	3	0 ✓
3	3	0 ✓	6
4	4	6	0 ✓
5	1	0 ✓	3
6	0 ✓	1	3

Zvyšok 0 v tabuľke znamená, že daný výraz má po delení číslom 7 zvyšok 0, t. j. je deliteľný číslom 7 bez zvyšku. Ako vidíme, v každom riadku tabuľky máme zvyšok 0. To znamená, že pre ľubovoľné prirodzené číslo n bude súčin na pravej strane (1) deliteľný číslom 7 a to znamená, že pre ľubovoľné prirodzené číslo n platí $7 \mid (n^7 - n)$.

14 bodov

4B. Nech p je ľubovoľné prvočíslo väčšie než 2 a $n \in \mathbb{N}$ je ľubovoľné prirodzené číslo. Dokážte, že potom platí $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Uvedený zápis znamená, že číslo $n^{\frac{p-1}{2}}$ má po delení číslom p zvyšok 1, alebo -1, alebo inak zapísané $n^{\frac{p-1}{2}} = k \cdot p \pm 1$ pre nejaké $k \in \mathbb{Z}$.

Riešenie: Rovnosť, ktorú máme dokázať sa využíva napríklad v modernej kryptológii. Táto rovnosť je dôsledkom *malej Fermatovej vety*, ktorá hovorí

> *Nech p je ľubovoľné prvočíslo a $n \in \mathbb{N}$. Potom prvočíslo p delí výraz $(n^p - n)$.*

Ako vidíme, malá Fermatova veta platí pre ľubovoľné prvočíslo p. Obmedzenie p je väčšie než 2, ktoré je v zadaní úlohy, je tam preto, aby zlomok $\frac{p-1}{2}$ bol vždy celé číslo. Malá Fermatova veta sa niekedy zvykne zapisovať aj v tvare

> *Nech p je ľubovoľné prvočíslo a $n \in \mathbb{N}$. Potom platí $n^p \equiv n \pmod{p}$,*

ktorý je ekvivalentný s verziou uvedenou vyššie, alebo takmer ekvivalentný s nasledujúcou verziou s obmedzením, že p musí byť väčšie než 2

> *Nech p je ľubovoľné prvočíslo väčšie než 2 a $n \in \mathbb{N}$. Potom platí $n^{p-1} \equiv 1 \pmod{p}$.*

Všetky tri uvedené verzie sú, až na obmedzenie v poslednej verzii, navzájom ekvivalentné. Práve posledná uvedená verzia malej Fermatovej vety sa dá zapísať aj tak, že p delí výraz $(n^{p-1} - 1)$. A tento výraz sa dá rozpísať ako

$$n^{p-1} - 1 = \left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right)$$

Potom platí

$$p \mid \left(n^{p-1} - 1\right) \qquad \textbf{práve vtedy keď} \qquad p \mid \left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right).$$

To znamená, že $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, alebo $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, čiže $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, čo bolo treba dokázať.

9 bodov ♡

5A. Poškodený kalendár 1. Vstupom je dátum vo formáte `DD.MM.YYYY` (vždy 10 znakov), ktorý môže obsahovať len jeden znak `?` namiesto číslice, buď v dni (`DD`), alebo v mesiaci (`MM`). Rok je pevne daný a neobsahuje znak `?`. Roky môžu byť v rozsahu od 1600 do 9999. Tvojou úlohou je zistiť, koľko platných dátumov môže takto zadaný dátum predstavovať. Treba pritom zohľadniť počet dní v mesiaci (napr. február má 28/29 dní podľa toho, či sa jedná o priestupný rok, niektoré mesiace majú 30 dní, iné 31 dní).

Program môže byť napísaný v Pythone (preferovaný jazyk), alebo v C (nie C++).

Príklady:

- Vstup: `1?.02.2024` → Výstup: `10`
- Vstup: `31.0?.2021` → Výstup: `5`

Riešenie: Toto je klasická úloha na ošetrenie hraničných stavov a prácu s dátumami. Kľúčom k úspechu je systematický prístup: namiesto zložitého vetvenia podmienok jednoducho vyskúšame všetky možné číslice (0–9) na mieste otáznika a overíme, či vzniknutý dátum dáva zmysel.

Postup

Postupne pre každú číslicu (0–9) dosadenú na miesto otáznika overíme, či vzniknutý dátum dáva zmysel. Počas overenia musíme brať do úvahy nasledovné faktory:

1. **Pozícia otáznika:** Musíme zistiť, či je znak `?` v dni alebo v mesiaci.
2. **Validácia dátumu:** Musíme overiť, či je mesiac v rozsahu 1–12 a či deň v danom mesiaci a roku skutočne existuje.
3. **Priestupné roky:** Musíme správne určiť, či má február 28 alebo 29 dní.

Ktoré roky sú priestupné:

Rok je priestupný, ak:

- je deliteľný 400, alebo
- je deliteľný 4 a zároveň nie je deliteľný 100.

Komentované príklady

- Majme vstup `29.0?.2024`. Rok 2024 bol priestupný. Úlohou teda je zistiť koľko mesiacov od januára po september malo 29 dní. Keďže sa jedná o priestupný rok, tak všetkých 9 mesiacov malo 29 dní a teda správnou odpoveďou je číslo 9.

- Majme vstup `?1.03.2026`. V tomto prípade musíme zistiť, či sú platné všetky 4 dátumy: 01.03.2026, 11.03.2026, 21.03.2026 a 31.03.2026. Keďže mesiac marec má 31 dní, platné sú všetky a preto je správnou odpoveďou číslo 4.

Implementácia v Pythone

Tu je vzorový zdrojový kód pre Python skript, pomocou ktorého vieme túto úlohu vyriešiť. Po spustení program čaká na zadanie dátumu z klávesnice.

```
import sys

def je_priestupny(rok):
    # Rok je priestupny, ak je delitelny 400, alebo ak je delitelny 4 a nie 100
    return (rok % 400 == 0) or (rok % 4 == 0 and rok % 100 != 0)

def pocet_dni_v_mesiaci(mesiac, rok):
    # Vracia pocet dni pre dany mesiac a rok
    if mesiac in [1, 3, 5, 7, 8, 10, 12]:
        return 31
    if mesiac in [4, 6, 9, 11]:
        return 30
    if mesiac == 2:
        return 29 if je_priestupny(rok) else 28
    return 0

def pocet_platnych_datumov():
    # Nacitanie vstupu zo standardneho vstupu a odstranenie prazdnych znakov
    # Funkcia input() precita jeden riadok a skonci hned po stlaceni Enter
    try:
        vstup = input().strip()
    except EOFError:
        return

    if not vstup:
        return

    # Rozdelenie retazca DD.MM.YYYY podla bodiek
    casti = vstup.split(".")
    den_str = casti[0]
    mesiac_str = casti[1]
    rok_str = casti[2]
    rok = int(rok_str)

    platne_datumy = 0
```

Pokračovanie na ďalšej strane…

```
    # Skusame nahradit znak '?' cislami 0 az 9
    for i in range(10):
        # Ak je '?' v dni, nahradi sa. Ak nie je, retazec ostane rovnaky.
        aktualny_den_str = den_str.replace("?", str(i))
        # Ak je '?' v mesiaci, nahradi sa.
        aktualny_mesiac_str = mesiac_str.replace("?", str(i))

        # Prevod upravenych retazcov na cele cisla
        d = int(aktualny_den_str)
        m = int(aktualny_mesiac_str)

        # Kontrola validity datumu:
        # 1. Mesiac musi byt v rozsahu 1 az 12
        if 1 <= m <= 12:
            # 2. Den musi byt v rozsahu 1 az max pocet dni v danom mesiaci
            if 1 <= d <= pocet_dni_v_mesiaci(m, rok):
                platne_datumy += 1

    # Vypis celkoveho poctu najdenych platnych datumov
    print(platne_datumy)

if __name__ == "__main__":
    pocet_platnych_datumov()
```

Príklady:

	Vstup	Výstup
Príklad 1	?2.12.2000	3
Príklad 2	?9.02.1960	3
Príklad 3	30.?4.2003	1
Príklad 4	31.0?.2025	5

9 bodov

5B. Poškodený kalendár 2. Vstupom je dátum vo formáte `DD.MM.YYYY` (vždy 10 znakov), ktorý môže obsahovať ľubovoľný počet znakov `?` namiesto číslice. Znaky `?` sa môžu nachádzať v dni (`DD`), v mesiaci (`MM`) aj v roku (`YYYY`). Rok môže byť v rozsahu 1600 – 9999. Tvojou úlohou je zistiť, koľko platných dátumov môže takto zadaný dátum predstavovať. Treba pritom zohľadniť počet dní v mesiaci (napr. február má 28/29 dní podľa toho, či sa jedná o priestupný rok, niektoré mesiace majú 30 dní, iné 31 dní).

Program môže byť napísaný v Pythone (preferovaný jazyk), alebo v C (nie C++).

Príklady:

- Vstup: `29.02.????` → Výstup: 2037
- Vstup: `??.??.2025` → Výstup: 365 (rok 2025 nebol priestupný)
- Vstup: `??.??.????` → Výstup: 3 068 037

Riešenie: Toto je klasická úloha na ošetrenie hraničných stavov a prácu s dátumami.

Postup

Pre všetky roky od 1600 do 9999 budeme postupne prechádzať validné kalendárne jednotky.

1. **Generovanie platných rokov**. Namiesto dosadzovania za `????` v roku, prejdeme všetky roky v cykle od 1600 do 9999. Pre každý rok skontrolujeme, či sedí na masku (napr. ak je vstup `20?4`, rok 2024 sedí, ale 2025 nie).
2. **Generovanie mesiacov**. Pre každý vyhovujúci rok prejdeme mesiace 1 až 12. Opäť skontrolujeme, či daný mesiac sedí na masku (napr. ak je v mesiaci `?1`, vyhovujú 01 a 11).
3. **Počet dní v mesiaci**. Pre konkrétny rok a mesiac už vieme presne určiť hornú hranicu dní (napr. pre február v priestupnom roku je to 29).

Algoritmus v bodoch:

1. Inicializuj počítadlo `celkovo = 0`.
2. Spusti cyklus `rok` od 1600 do 9999:
   (a) Ak `rok` nevyhovuje maske `YYYY`, pokračuj na ďalší rok.
   (b) Zisti, či je aktuálny `rok` priestupný.
   (c) Spusti cyklus `mesiac` od 1 do 12:
      i. Ak `mesiac` nevyhovuje maske `MM`, pokračuj na ďalší mesiac.
      ii. Urči `max_dni` pre tento `mesiac` a `rok`.
      iii. Spusti cyklus `den` od 1 do `max_dni`:
         - Ak `den` vyhovuje maske `DD`, pripočítaj 1 k `celkovo`.
3. Vypíš `celkovo`.

Implementácia v Pythone

Tu je vzorový zdrojový kód pre Python skript, pomocou ktorého vieme túto úlohu vyriešiť. Po spustení program čaká na zadanie dátumu z klávesnice.

```
import sys

def je_priestupny(rok):
    # Standardna podmienka pre priestupny rok
    return (rok % 400 == 0) or (rok % 4 == 0 and rok % 100 != 0)

def ziskaj_max_dni(mesiac, rok):
    # Vracia pocet dni v danom mesiaci pre konkretny rok
    if mesiac in [1, 3, 5, 7, 8, 10, 12]:
        return 31
    if mesiac in [4, 6, 9, 11]:
        return 30
    if mesiac == 2:
        return 29 if je_priestupny(rok) else 28
    return 0

def pasuje_maska(hodnota, maska, dlzka):
    # Skontroluje, ci cislo vyhovuje maske s otaznikmi
    # zfill(dlzka) zabezpeci ze napr. mesiac 5 bude '05'
    s_hodnota = str(hodnota).zfill(dlzka)
    for i in range(dlzka):
        if maska[i] != "?" and maska[i] != s_hodnota[i]:
            return False
    return True

def pocet_platnych_datumov():
    # Nacitanie vstupu z klavesnice
    try:
        riadok = input().strip()
    except EOFError:
        return

    if len(riadok) != 10:
        return

    # Rozdelenie vstupu na casti podla bodiek
    maska_den, maska_mesiac, maska_rok = riadok.split(".")

    pocitadlo = 0
```

Pokračovanie na ďalšej strane. . .

```
    # Prechadzame vsetky roky v zadanom rozsahu 1600 - 9999
    for r in range(1600, 10000):
        if pasuje_maska(r, maska_rok, 4):
            # Pre kazdy vyhovujuci rok prejdeme vsetky mesiace
            for m in range(1, 13):
                if pasuje_maska(m, maska_mesiac, 2):
                    # Pre kazdy vyhovujuci mesiac zistime pocet dni
                    max_dni = ziskaj_max_dni(m, r)
                    # Prejdeme vsetky dni v mesiaci
                    for d in range(1, max_dni + 1):
                        if pasuje_maska(d, maska_den, 2):
                            pocitadlo += 1

    # Vypis vysledneho poctu platnych kombinacii
    print(pocitadlo)

if __name__ == "__main__":
    pocet_platnych_datumov()
```

Príklady:

	Vstup	Výstup
Príklad 1	??.??.2024	366
Príklad 2	3?.?2.19??	200
Príklad 3	??.07.????	260400
Príklad 4	31.??.??55	588

16 bodov

6A. Rozlúštite nasledujúci text **(14 bodov)**

```
PJLOL RAONY EREUA HCNVK UTLNI MTASL JVAAI KULAD ULRIY TOVJO LSENA OBVVA
SUIAV DALYK HTKDU OOLSV OSSDJ XIPLO INVIE RPASS SPSAB ZBEAT SPODA LYAPR
LSOKE AIOEN SKBVR LRJZE VEAEY MTSOE VSOAV TOVDH SIOIT HSGIC VDRAE MEOKH
EBLAH GLOHE POMAD APEOT ADNEG TTRHM LOBNO VRYLC MKVVL IOSSA IDAEO RKAAT
REONN MIOKU TCPJR NJLEB NANZO OSOMN OUNDO ZRBOV VZATM KZOAR RAEAO IADAA
ZSEMO KCKOC JESEV UENIR AZLHI KDPYU DEAEC VCYDZ ANKYL SVLYE CATVE TAREY
AAALS AISOM RUIEO JSVST EVELA EXAMS BOHTP EMSIH YDDKL GMZOO LITOC SSZNC
KAEMZ ALEYX IUMEH AOOOO NDITC NOSSL NYDKN OSMOA ALVHS IIOAZ IAALR ATLEE
LJERD TATRL VUNES TVTOM DPUNP RUOIT ORVMA N
```

Jedná sa o slovensky písaný text bez medzier a bez diakritických a interpunkčných znamienok. Text je zašifrovaný úplnou tabuľkovou transpozíciou. Šírka tabuľky je 12. Výsledný, zašifrovaný, text je rozdelený do 5-znakových skupín.
Za správne určenie knihy, z ktorej text pochádza, sú ešte bonusové **(2 body)**.

Riešenie: *Tabuľková transpozícia* spočíva v tom, že otvorený text sa zapíše do obdĺžnikovej tabuľky $m \times n$ (m riadkov, n stĺpcov) po riadkoch zľava doprava a potom sa z tejto tabuľky číta po stĺpcoch zhora nadol. Poradie, v ktorom sa jednotlivé stĺpce čítajú je dané permutáciou, ktorá je určená heslom. Tabuľka s n stĺpcami prislúcha heslu s n znakmi, alebo inak povedané, počet znakov hesla určuje šírku tabuľky.

O *úplnej tabuľkovej transpozícii* hovoríme vtedy, ak sú všetky políčka tabuľky $m \times n$ vyplnené znakmi. Ak sa stane, že otvorený text nevyplní celý posledný riadok tabuľky, tak sa zvyšné políčka vyplnia *nulami*. Pojmom *nuly* sa v kryptografii označujú znaky, ktoré nemajú žiaden iný význam, než napr. doplnenie textu na potrebnú dĺžku. Na šifrovanie a dešifrovanie nemajú žiaden vplyv. Nuly by sa správne mali vyberať náhodne zo znakov, ktoré v príslušnom jazyku majú najvyššie relatívne početnosti. Avšak pre lenivosť šifrantov sa v praxi často za nuly dávali rovnaké znaky a naviac také, ktoré sa v príslušnom jazyku nevyskytujú vôbec, alebo len veľmi zriedkavo. V slovenčine sú takými znakmi napr. `Q`, `W`, alebo `X`.

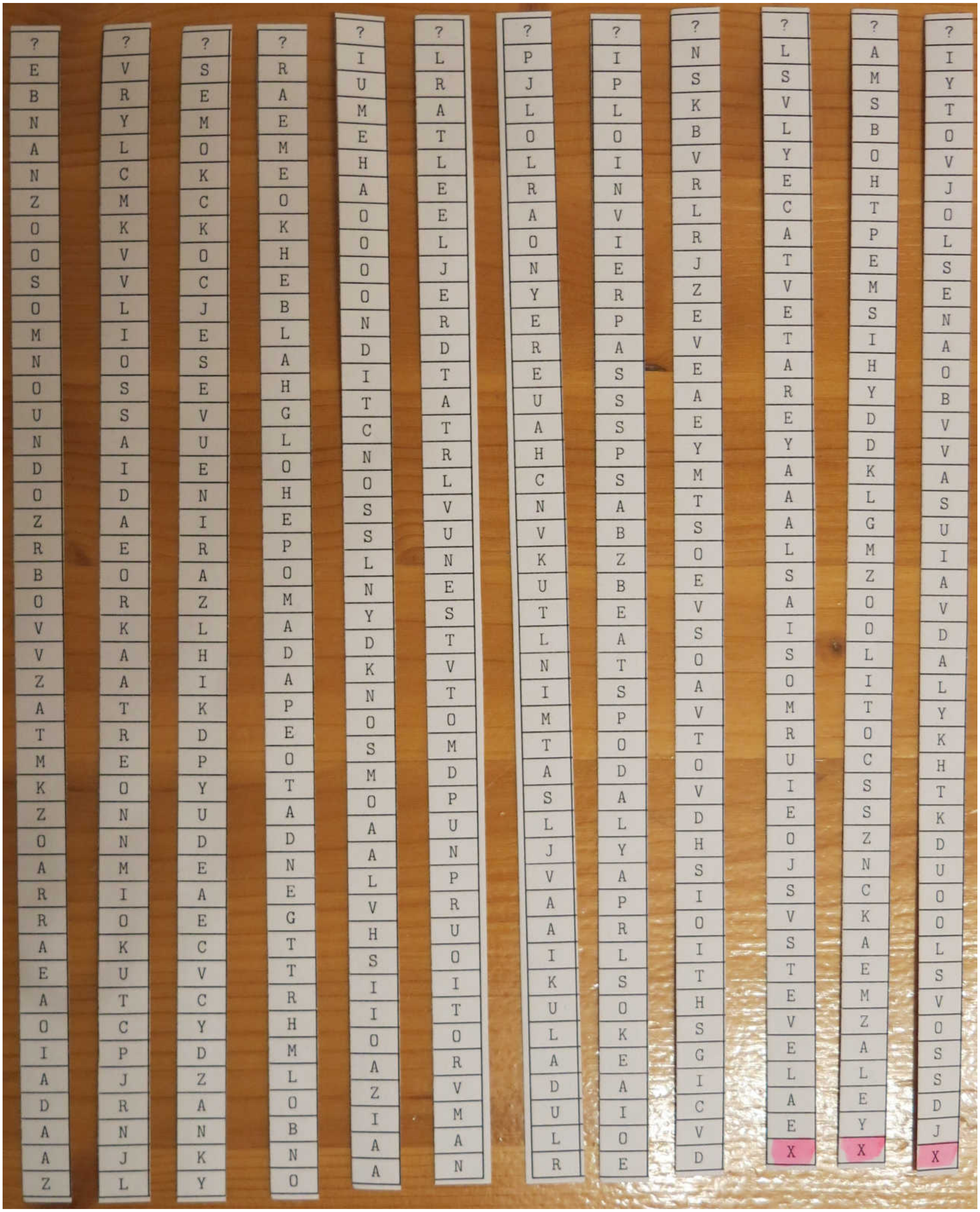
Zo zadania úlohy vieme, že šírka tabuľky je 12 znakov. To znamená, že aj heslo má 12 znakov a jemu zodpovedajúca permutácia je permutáciou 12-tice $(1, 2, 3, \ldots, 12)$. Daný zašifrovaný text má 516 znakov a $516 = 43 \cdot 12$, t. j. tabuľka bude mať rozmery 43×12. Keďže vieme, že text sa z tabuľky číta po stĺpcoch a výška stĺpcov je 43, vieme si zašifrovaný text rozdeliť na stĺpce. Takto rozdelený text vidíme na obrázku 1 na strane 14. Zatiaľ sme stĺpce naukladali v poradí, v ktorom sme ich zo zašifrovaného text čítali. Toto poradia však evidentne nie je správne.

Ďalší postup lúštenia je jednoduchý. tabuľku si nastriháme po stĺpcoch a tieto budeme permutovať (preusporiadávať) tak, aby sme dostali zmysluplný text. Za povšimnutie stoja 3 znaky `X` v poslednom riadku tabuľky. Toto sú s vysokou pravdepodobnosťou nuly. Je takmer vylúčené, aby sa v slovenskom texte s 12 znakmi (posledný riadok) 3 krát vyskytovalo písmeno `X`. To znamená, že stĺpce s `X` sú posledné 3 stĺpce tabuľky, čo výrazne zľahčí riešenie.

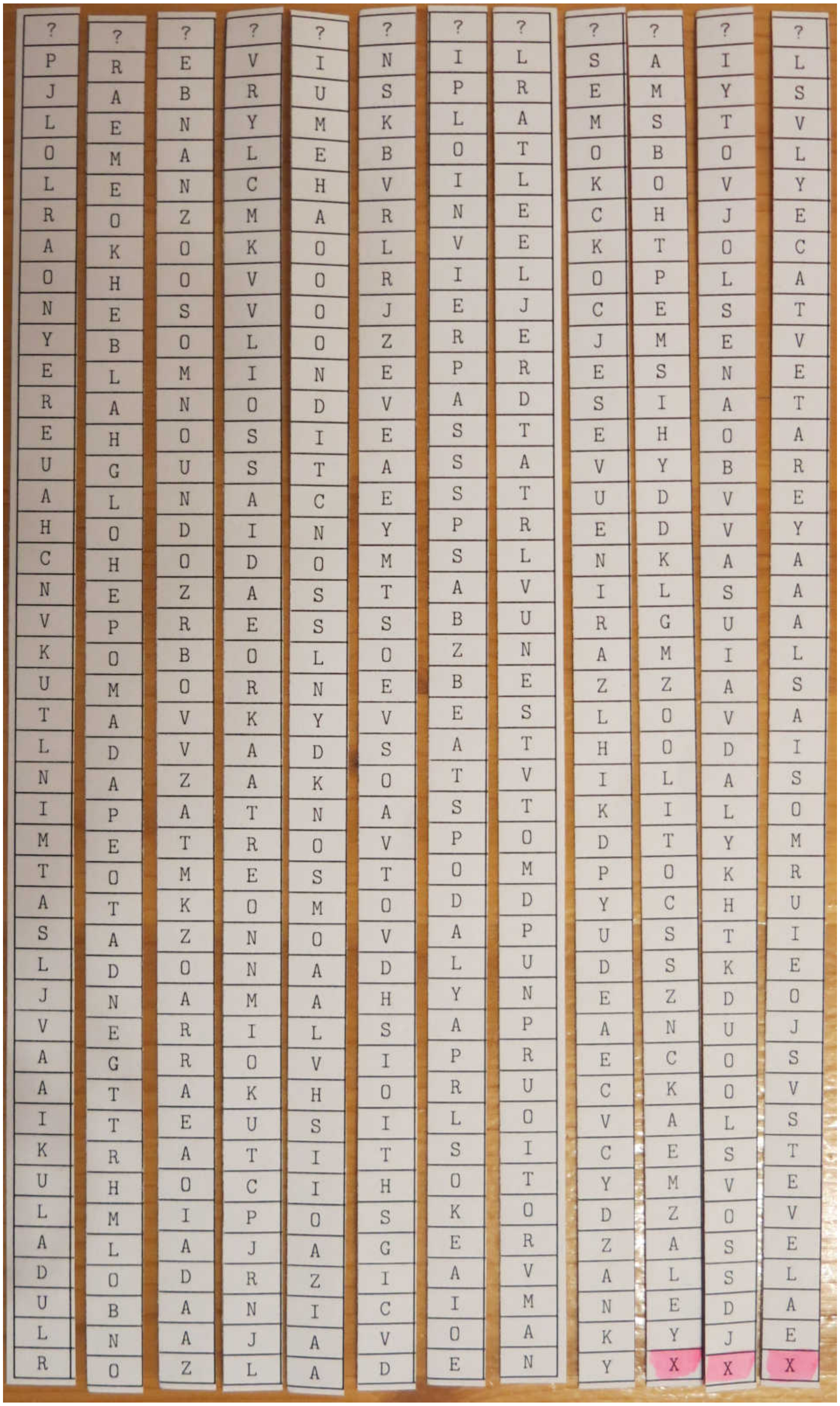
Pri permutovaní stĺpcov sa snažíme v prvom riadku zložiť zmysluplný text. Možností je samozrejme viacero. To, že sme našli ten správny text, zistíme tak, že aj v ostatných riadkoch tabuľky dostaneme zmysluplné texty. Permutácia hesla totiž platí rovnako pre všetky riadky. Táto metóda lúštenia sa nazýva *anagramová metóda*.

?	?	?	?	?	?	?	?	?	?	?	?
P	I	I	N	R	V	E	S	L	A	I	L
J	Y	P	S	A	R	B	E	S	M	U	R
L	T	L	K	E	Y	N	M	V	S	M	A
O	O	O	B	M	L	A	O	L	B	E	T
L	V	I	V	E	C	N	K	Y	O	H	L
R	J	N	R	O	M	Z	C	E	H	A	E
A	O	V	L	K	K	O	K	C	T	O	E
O	L	I	R	H	V	O	O	A	P	O	L
N	S	E	J	E	V	S	C	T	E	O	J
Y	E	R	Z	B	L	O	J	V	M	O	E
E	N	P	E	L	I	M	E	E	S	N	R
R	A	A	V	A	O	N	S	T	I	D	D
E	O	S	E	H	S	O	E	A	H	I	T
U	B	S	A	G	S	U	V	R	Y	T	A
A	V	S	E	L	A	N	U	E	D	C	T
H	V	P	Y	O	I	D	E	Y	D	N	R
C	A	S	M	H	D	O	N	A	K	O	L
N	S	A	T	E	A	Z	I	A	L	S	V
V	U	B	S	P	E	R	R	A	G	S	U
K	I	Z	O	O	O	B	A	L	M	L	N
U	A	B	E	M	R	O	Z	S	Z	N	E
T	V	E	V	A	K	V	L	A	O	Y	S
L	D	A	S	D	A	V	H	I	O	D	T
N	A	T	O	A	A	Z	I	S	L	K	V
I	L	S	A	P	T	A	K	O	I	N	T
M	Y	P	V	E	R	T	D	M	T	O	O
T	K	O	T	O	E	M	P	R	O	S	M
A	H	D	O	T	O	K	Y	U	C	M	D
S	T	A	V	A	N	Z	U	I	S	O	P
L	K	L	D	D	N	O	D	E	S	A	U
J	D	Y	H	N	M	A	E	O	Z	A	N
V	U	A	S	E	I	R	A	J	N	L	P
A	O	P	I	G	O	R	E	S	C	V	R
A	O	R	O	T	K	A	C	V	K	H	U
I	L	L	I	T	U	E	V	S	A	S	O
K	S	S	T	R	T	A	C	T	E	I	I
U	V	O	H	H	C	O	Y	E	M	I	T
L	O	K	S	M	P	I	D	V	Z	O	O
A	S	E	G	L	J	A	Z	E	A	A	R
D	S	A	I	O	R	D	A	L	L	Z	V
U	D	I	C	B	N	A	N	A	E	I	M
L	J	O	V	N	J	A	K	E	Y	A	A
R	X	E	D	O	L	Z	Y	X	X	A	N

Obr. 1: Zašifrovaný text rozdelený na stĺpce – zatiaľ v nesprávnom poradí



Obr. 2: Nastrihané stĺpce tabuľky zatiaľ v nesprávnom poradí. Stĺpce s `X` sú na konci.



Obr. 3: Nastrihané stĺpce tabuľky v správnom poradí. Po riadkoch už môžeme čítať otvorený text.

Na obrázku 2 na strane 15 vidíme nastrihané stĺpce tabuľky. Tieto sú zatiaľ v nesprávnom poradí, ale vzhľadom na malú šírku tabuľky nám potrvá nanajvýš pár minút, kým nájdeme správne poradie stĺpcov. Na obrázku 3 na strane 16 už vidíme stĺpce tabuľky usporiadané v správnom poradí a z tabuľky môžeme po riadkoch čítať otvorený text.

```
PREVINIL SA ILJA BRUS PREMYSLENYM KLAMSTVOM ALEBO TO BOL LEN CHVILKOVY
ROZMAR NECH JE AKOKOLVEK TO CO HOVORIL O PLANE SVOJEJ CESTY BOLO ZREJME
VELMI NEPRESNE RANO DVADSIATEHOSIESTEHO AUGUSTA SA VYBRAL NA CESTU DVE
HODINY PRED VYCHODOM SLNKA A NEZASTAVIL SA V PRESSBURGU AKO BOL OZNAMIL
UMORNE BEZ ZASTAVKY VESLOVAL DVADSAT HODIN A ZAKOTVIL ASI PATNAST
KILOMETROV POD TYMTO MESTOM PO KRATKOM ODDYCHU SA ZNOVA PUSTIL DO
NADLUDSKEJ NAMAHY NEZDOVERIL SA PANU JAGROVI PRECO SA TAK HORUCKOVITE
USILOVAL SKRATIT SI CESTU HOCI HO TYM VELMI POSKODZOVAL A JAGER ZASE
DODRZIAVAL SLUB A NICIM NEDAL NAJAVO AKY JE ROZLADENY
```

Rozlúštenie textu nebolo ťažké. Na rozdiel od kryptografických úloh predošlých kôl však je problém nájsť tento text na internete bežnými vyhľadávačmi. Text pochádza z knihy *Dunajský lodivod* od Julesa Verna.

16 bodov

6B. Rozlúštite nasledujúci text a zistite odkiaľ pochádza:

```
SIYID SSANK PIMEN YAAAI IZOLE TTRIB UADLO RAAOV HOPIV GYOKS
ZCDLA OAOMN ILOKK ITSEK VYZIA KSAUN DTMAA LNMTR AIOVD YILOZ
MNISL ATARA ATAOT LPSTA YALON HUOKI ASNOR NNAIO JZTEE LYJAA
AAUUO ACIJH OISVA RAALZ MDDZA ASDIE LUBAK MSVSS ABAJK ZDSLH
MEANO KRNEI TNAEO OACLH IETLI JIYAU ITRAZ ANZAC DOORA ALCCS
CIAJU OEKAI MBYIH CIMII AIAOV ATERR ERZEO OIAVN IIHJA ANHMA
TVMYD RCUSO SLTLN BILET OEIPE LBNSM ALTSA ANONU JRLAO UAUII
HTVSH BZVUZ SZANZ ODATI SKNHH IIKN
```

Jedná sa o slovensky písaný text bez medzier a bez diakritických a interpunkčných znamienok. Text je zašifrovaný neúplnou tabuľkovou transpozíciou. Šírka tabuľky je 9. Výsledný, zašifrovaný, text je rozdelený do 5-znakových skupín.

Riešenie: V tejto úlohe sa jedná o *neúplnú tabuľkovú transpozíciu*. Rozdiel oproti úplnej tabuľkovej transpozícii je v tom, že ak otvorený text nevyplní celý posledný riadok šifrovacej tabuľky, tak voľné políčka tabuľky nebudeme dopĺňať nulami. To spôsobí, že niektoré stĺpce budú vyššie a iné nižšie (rozdiel výšok je vždy 1) a skomplikuje to riešenie, pretože rozdeliť zašifrovaný text na stĺpce nebude tak jednoduché ako v predošlej úlohe.

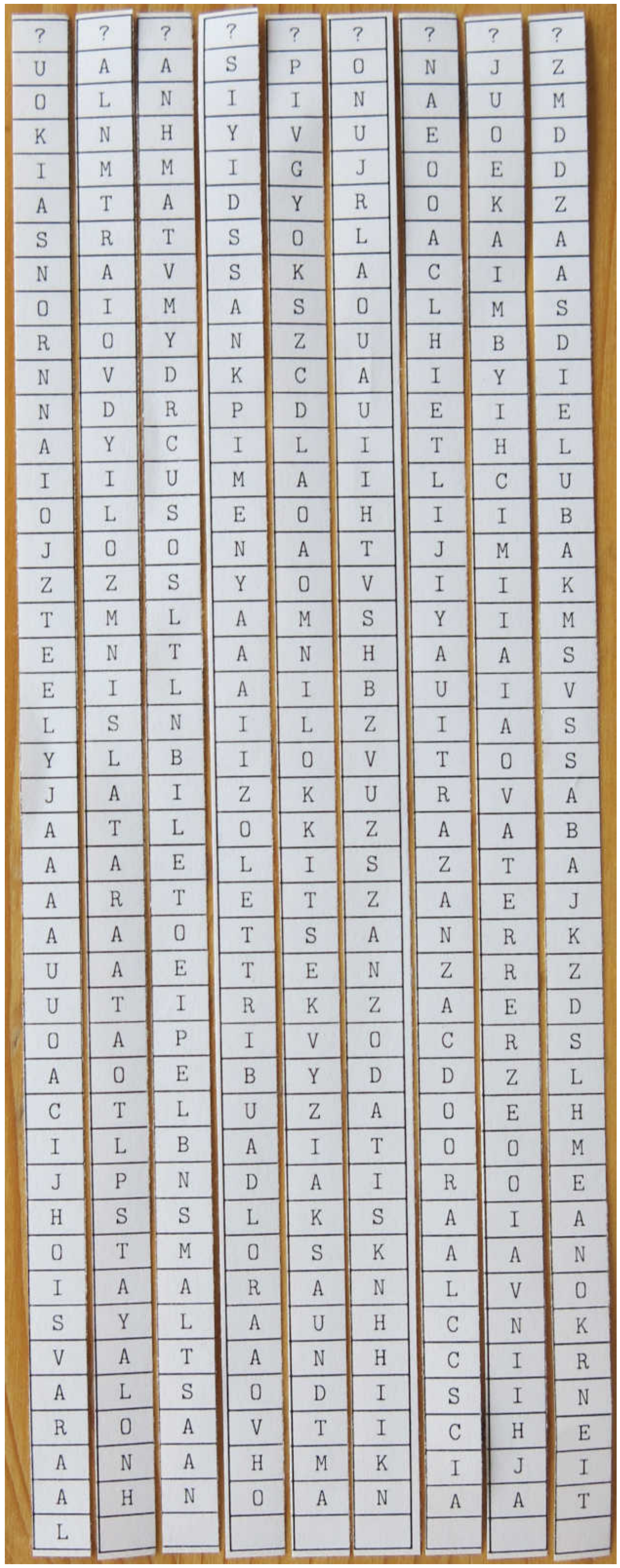
Náš zašifrovaný text má 379 znakov. Šírka šifrovacej tabuľky je 9 stĺpcov, ako je uvedené v zadaní. Platí $379 = 42 \cdot 9 + 1$ čo znamená, že v poslednom riadku tabuľky je len 1 znak a zvyšných 8 políčok je práznych. Takže 1 stĺpec bude mať výšku 43 a zvyšných 8 stĺpcov bude mať výšku 42. My však nevieme, ktorý stĺpec v zašifrovanom texte je ten dlhší, pretože pri šifrovaní sa text číta po stĺpcoch, pričom poradie stĺpcov je dané permutáciou odvodenou z hesla. Vieme však, že šírka šifrovacej tabuľky je 9, takže postupne vyskúšame všetkých 9 možností – vyšší stĺpec bude postupne na 1. až 9. mieste. Jedna z týchto možností musí byť tá správna. Zvyšný postup riešenia je rovnaký ako v predošlej úlohe pri úplnej tabuľkovej transpozícii. Takže lúštenie tejto šifry zodpovedá lúšteniu deviatich úplných tabuľkových transpozícií s rovnakou šírkou tabuľky. Určite si viete predstaviť, že pri šírke tabuľky napr. 23 a počte dlhších stĺpcov napr. 11, by počet možností, ktoré by bolo treba vyskúšať, bol viac než 4 bilióny.

Aby sme riešenie príliš nenaťahovali, prezradíme, že správne miesto dlhšieho stĺpca v zašifrovanom texte je 4. miesto. To znamená, že najskôr idú 3 kratšie stĺpce, potom dlhší stĺpec a za ním už len kratšie stĺpce. Na obrázku 4 na strane 19 potom vidíte zašifrovaný text rozdelený na stĺpce. Ďalší postup je rovnaký ako pri riešení predošlej úlohy. Stĺpce si nastriháme, najdlhší stĺec musí byť v otvorenom texte samozrejme na 1. mieste a zvyšných 8 stĺpcov budeme permutovať tak, aby sme dostali zmysluplný text.

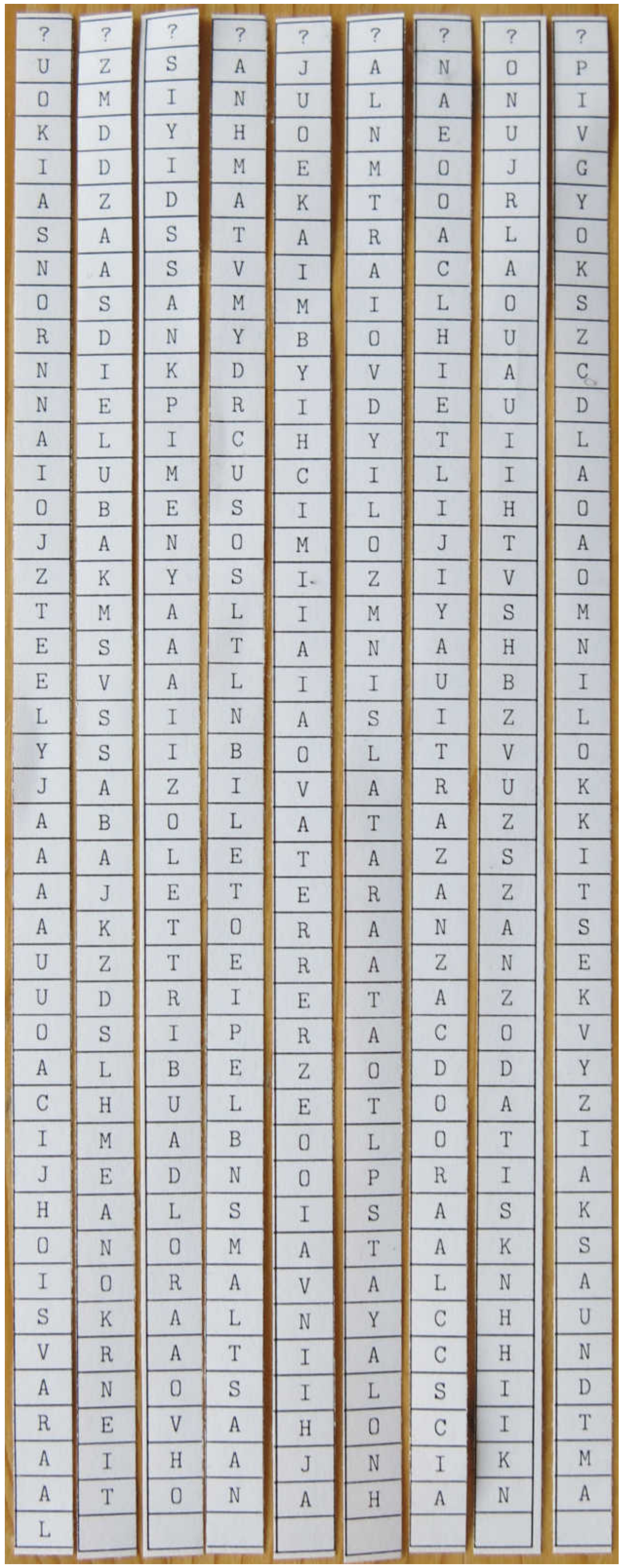
Na obrázku 5 na strane 20 vidíme nastrihané stĺpce tabuľky. Najdlhší stĺpec je už na správnom 1. mieste, ostatné stĺpce sú náhodne. Pri písmenách, ktoré sú v prvom riadku, nie je problém nájsť správne usporiadanie stĺpcov behom pár sekúnd. Na obrázku 6 na strane 21 sú už všetky stĺpce v správnom poradí a po riadkoch už môžeme čítať otvorený text.

?	?	?	?	?	?	?	?	?
S	P	A	U	Z	N	J	A	O
I	I	L	O	M	A	U	N	N
Y	V	N	K	D	E	O	H	U
I	G	M	I	D	O	E	M	J
D	Y	T	A	Z	O	K	A	R
S	O	R	S	A	A	A	T	L
S	K	A	N	A	C	I	V	A
A	S	I	O	S	L	M	M	O
N	Z	O	R	D	H	B	Y	U
K	C	V	N	I	I	Y	D	A
P	D	D	N	E	E	I	R	U
I	L	Y	A	L	T	H	C	I
M	A	I	I	U	L	C	U	I
E	O	L	O	B	I	I	S	H
N	A	O	J	A	J	M	O	T
Y	O	Z	Z	K	I	I	S	V
A	M	M	T	M	Y	I	L	S
A	N	N	E	S	A	A	T	H
A	I	I	E	V	U	I	L	B
I	L	S	L	S	I	A	N	Z
I	O	L	Y	S	T	O	B	V
Z	K	A	J	A	R	V	I	U
O	K	T	A	B	A	A	L	Z
L	I	A	A	A	Z	T	E	S
E	T	R	A	J	A	E	T	Z
T	S	A	A	K	N	R	O	A
T	E	A	U	Z	Z	R	E	N
R	K	T	U	D	A	E	I	Z
I	V	A	O	S	C	R	P	O
B	Y	O	A	L	D	Z	E	D
U	Z	T	C	H	O	E	L	A
A	I	L	I	M	O	O	B	T
D	A	P	J	E	R	O	N	I
L	K	S	H	A	A	I	S	S
O	S	T	O	N	A	A	M	K
R	A	A	I	O	L	V	A	N
A	U	Y	S	K	C	N	L	H
A	N	A	V	R	C	I	T	H
O	D	L	A	N	S	I	S	I
V	T	O	R	E	C	H	A	I
H	M	N	A	I	I	J	A	K
O	A	H	A	T	A	A	N	N
			L					

Obr. 4: Zašifrovaný text rozdelený na stĺpce – dlhší stĺpec je na správnom 4. mieste.



Obr. 5: Dlhý stĺpec je na správnom mieste, ostatné stĺpce sú náhodne.



Obr. 6: Všetky stĺpce sú už na správnych miestach a v riadkoch vidíme otvorený text.

Hľadaný otvorený text je

```
UZ SA JANO POMINUL A NIKDY HO NEUVIDIME MOJ GAZDA KTORY SA STARAL O NAS VIAC
AKO SAM MILOSRDNY BOH UZ NIKDY VIAC NEPRIDE UDALI CHYTILI UMUCILI A OBESILI
HO JANO MOJ TAZKY SI ZIVOT MAL I MY SME SA TA NAHNEVALI I UBIL SI NAS I ZLY
SI BOL TVOJA ZIVA RUKA BOLA TAZKA ALE TAZSIA JE TERAZ TA KTORA NAS UZ TERAZ
NEUDRIE TAZKO SI PRACOVAL BEZ ODDYCHU LETO A ZIMA BOLO TI JEDNO PRIAHAL SI
SA S KONOM A TAK SI ORAVAL NA SKALNYCH UVRATIACH NANOSIL SI DREVA HOCI TA
I HAJNIK MATO NAHANAL
```

Tento text by sme mali poznať už zo základnej školy a dá sa aj ľahko identifikovať pomocou vyhľadávačov. Text pochádza z románu *Adam Šangala* od Ladislava Nádaši-Jégého.