ČASŤ 1: MAGICKÉ ŠTVORCE A ŠTVORCE

Definícia 1.1: Maticu veľkosti 3x3

$$\begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}$$

nazývame **magickým štvorcom**, ak obsahuje navzájom rôzne kladné celé čísla a zároveň majú výrazy

$$A + B + C, D + E + F, G + H + I, A + D + G, B + E + H, C + F + I, A + E + I, C + E + G$$

rovnakú hodnotu rovnú S. Hodnotu S nazývame **súčet magického štvorca**.

Veta 1.2: Pre každý magický štvorec platí $S = 3E$.

Dôkaz: Vyplýva priamo zo vzťahu $3S = (A + E + I) + (B + E + H) + (C + E + G) = (A + B + C) + (G + H + I) + 3E = 2S + 3E$.

Dôsledok 1.2: Pre každý magický štvorec platí $A + I = B + H = C + G = D + F = 2E$.

Veta 1.3: Pre každý magický štvorec platí

(i) $2A = F + H$
(ii) $2C = D + H$
(iii) $2G = B + F$
(iv) $2I = B + D$

Dôkaz: Dokážeme iba (i), postup dôkazu pri (ii), (iii) a (iv) je analogický.

Platí $C + F + I = G + H + I = 3E$ a zároveň $A + I = C + G = 2E$. Z prvého vzťahu postupne vyjadríme $C = 3E - F - I$ a $G = 3E - H - I$. Z druhého vzťahu najprv vyjadríme $A = 2E - I$. Dosadím do rovnice $C + G = 2E$ dostaneme

$$3E - F - I + 3E - H - I = 2E$$

čo po úprave vyjde

$$2(2E - I) = F + H$$

Keďže $A = 2E - I$, platí aj $2A = F + H$ (čo bolo treba dokázať).

Definícia 1.4: Celé číslo n sa nazýva **štvorec** ak sa dá napísať v tvare $n = k^2$, kde k je celé číslo.

ČASŤ 2: ALGEBRAICKÉ IDENTITY

Lema 2.1: Celé čísla A, B sa dajú zapísať ako $x+y, x-y$ (kde x, y sú tiež celé čísla) práve vtedy, keď sú čísla A, B obe párne alebo obe nepárne.

Dôkaz: Sústava rovníc

$$A = x + y$$

$$B = x - y$$

má riešenie $x = \frac{A+B}{2}, y = \frac{A-B}{2}$. Ak sú čísla A, B obe párne alebo obe nepárne, tak ich súčet aj rozdiel je deliteľný dvomi, teda x, y sú celé čísla. Ak je číslo A párne a číslo B nepárne (opačný prípad je analogický), ich súčet aj rozdiel je nepárny, teda x, y nemôžu byť celé čísla.

Lema 2.2: Nech n je štvorec. Potom

(i) Ak n je párne, tak n je deliteľné 4.
(ii) Ak n je nepárne, tak n dáva po delení 4 zvyšok 1.

Dôkaz: Ak n je štvorec, tak sa z definície dá napísať ako k^2, kde k je celé číslo.

(i) Ak n je párne, tak aj k je párne. To znamená, že existuje celé číslo l také, že $k = 2l$. Tým dostávame $n = k^2 = 4l^2$, takže n je deliteľné 4.
(ii) Ak n je nepárne, tak aj k je nepárne. To znamená, že existuje celé číslo l také, že $k = 2l - 1$. Tým dostávame $n = k^2 = 4l^2 - 4l + 1$, takže n dáva po delení 4 zvyšok 1.

Veta 2.3: Množina všetkých celočíselných riešení rovnice $A^2 + B^2 + C^2 = D^2 + E^2 + F^2$ je daná parametricky:

$$A = a + b \qquad C = e + f \qquad E = c - d$$

$$B = c + d \qquad D = a - b \qquad F = e - f$$

kde a, b, c, d, e, f sú celé čísla, pre ktoré platí vzťah $ab + cd + ef = 0$.

Dôkaz: Je zrejmé, že daná parametrizácia vygeneruje vždy správne riešenie – dosadením dostaneme

$$(a+b)^2 + (c+d)^2 + (e+f)^2 = (a-b)^2 + (c-d)^2 + (e-f)^2$$

z čoho automaticky vyplýva $ab + cd + ef = 0$.

Ukážeme aj to, že každé riešenie sa dá takto parametricky vyjadriť. Vidíme, že členy na ľavej a pravej strane rovnice vieme popárovať do dvojíc $x+y, x-y$, kde x, y sú celé čísla. Podľa Lemy 2.1 je to možné práve vtedy, keď sú oba členy párne alebo nepárne.

Stačí preto dokázať, že v danej rovnici musí byť na ľavej aj pravej strane rovnaký počet párnych (a teda aj nepárnych) členov. Postupujme sporom. Predpokladajme, že počet párnych členov a nepárnych členov na jednej strane rovnice je iný ako na druhej strane. Máme dve možnosti:

- Na jednej strane rovnice sú len nepárne členy a na druhej strane sú dva párne a jeden nepárny. Potom však z Lemy 2.2 vyplýva, že jedna strana rovnice dáva po delení 4 zvyšok 3, zatiaľ čo druhá strana dáva po delení 4 zvyšok 1, čo je spor.
- Na jednej strane rovnice sú len párne členy a na druhej strane sú dva nepárne a jeden párny. Potom však z Lemy 2.2 vyplýva, že jedna strana rovnice je deliteľná 4, zatiaľ čo druhá strana dáva po delení 4 zvyšok 2, čo je spor.

Veta 2.4: Množina všetkých celočíselných riešení rovnice $A^2 + B^2 + C^2 = 3D^2$ je daná parametricky:

$$A = 2x - \frac{x^2 + y^2 + z^2}{x + y + z} \qquad C = 2z - \frac{x^2 + y^2 + z^2}{x + y + z}$$

$$B = 2y - \frac{x^2 + y^2 + z^2}{x + y + z} \qquad D = \frac{x^2 + y^2 + z^2}{x + y + z}$$

kde x, y, z sú celé čísla, pre ktoré platí $x + y + z \neq 0$ a zároveň hodnota $\frac{x^2+y^2+z^2}{x+y+z}$ je celé číslo.

Dôkaz: Použitím vety 2.3 na rovnicu $A^2 + B^2 + C^2 = D^2 + D^2 + D^2$ dostaneme parametrizáciu:

$$A = a + b$$

$$B = c + d$$

$$C = e + f$$

$$D = a - b = c - d = e - f$$

Z posledného vzťahu vyjadríme $d = -a + b + c,\ f = -a + b + e$. Keďže z vety 2.3 musí platiť aj vzťah $ab + cd + ef = 0$, dostaneme:

$$ab + c(-a + b + c) + e(-a + b + e) = 0$$

$$b(a + c + e) - ac + c^2 - ae + e^2 = 0$$

$$\rightarrow b = \frac{ac - c^2 + ae - e^2}{a + c + e} = \frac{a^2 + ac + ae}{a + c + e} + \frac{-a^2 - c^2 - e^2}{a + c + e} = a - \frac{a^2 + c^2 + e^2}{a + c + e}$$

Premennú b môžeme takto vyjadriť len za podmienky $a + c + e \neq 0$ a zlomok $\frac{a^2+c^2+e^2}{a+c+e}$ musí byť celé číslo - k tomu sa vrátime na konci dôkazu. Z toho zároveň vyplýva, že:

$$d = -a + b + c = -a + a - \frac{a^2 + c^2 + e^2}{a + c + e} + c = c - \frac{a^2 + c^2 + e^2}{a + c + e}$$

$$f = -a + b + e = -a + a - \frac{a^2 + c^2 + e^2}{a + c + e} + e = e - \frac{a^2 + c^2 + e^2}{a + c + e}$$

Dosadíme do pôvodných premenných A, B, C, D:

$$A = a + b = 2a - \frac{a^2 + c^2 + e^2}{a + c + e} \qquad C = e + f = 2e - \frac{a^2 + c^2 + e^2}{a + c + e}$$

$$B = c + d = 2c - \frac{a^2 + c^2 + e^2}{a + c + e} \qquad D = a - b = \frac{a^2 + c^2 + e^2}{a + c + e}$$

Substitúciou $x = a, y = c, z = e$ dostaneme hľadaný vzťah. Skontrolujeme ešte podmienky pri vyjadrení b.

- Podmienka $a + c + e \neq 0$ je ekvivalentná s $x + y + z \neq 0$ - to platí zo zadania.
- $\frac{a^2+c^2+e^2}{a+c+e}$ je celé číslo je ekvivalentné s tým, že $\frac{x^2+y^2+z^2}{x+y+z}$ je celé číslo - to tiež platí zo zadania.

<u>Veta 2.5</u>: Množina všetkých celočíselných riešení rovnice $A^2 + B^2 = C^2 + D^2$ je daná parametricky:

$$A = pr + qs \qquad C = ps + qr$$

$$B = qr - ps \qquad D = pr - qs$$

kde $p, q, r, s \in Z$.

<u>Veta 2.6</u>: Množina všetkých celočíselných riešení rovnice $A^2 + B^2 = 2C^2$ je daná parametricky:

$$A = w(u^2 + 2uv - v^2)$$

$$B = w(-u^2 + 2uv + v^2)$$

$$C = w(u^2 + v^2)$$

kde $u, v, w \in Z$.

<u>Dôkaz</u>: Použitím vety 2.5 na rovnicu $A^2 + B^2 = C^2 + C^2$ dostaneme parametrizáciu:

$$A = pr + qs$$

$$B = qr - ps$$

$$C = ps + qr = pr - qs$$

Z posledného vzťahu vyjadríme $s = r\frac{p-q}{p+q}$. To dosadíme za A, B, C:

$$A = pr + qs = pr + qr\frac{p-q}{p+q} = \frac{p^2r + pqr + pqr - q^2r}{p+q} = \frac{r}{p+q}(p^2 + 2pq - q^2)$$

$$B = qr - ps = qr - pr\frac{p-q}{p+q} = \frac{pqr + q^2r - p^2r + pqr}{p+q} = \frac{r}{p+q}(-p^2 + 2pq + q^2)$$

$$C = ps + qr = pr\frac{p-q}{p+q} + qr = \frac{p^2r - pqr + pqr + q^2r}{p+q} = \frac{r}{p+q}(p^2 + q^2)$$

Výraz $w = \frac{r}{p+q}$ môžeme beztrestne považovať ako násobok nejakého riešenia (vieme ho regulovať premennou r). Ak vo zvyšku použijeme substitúciu $u = p, v = q$, dostaneme hľadaný výraz.

Veta 2.7: Množina všetkých celočíselných riešení rovnice $A^2 + B^2 = C(A + B)$ je daná parametricky:

$$A \in \{ki(i + j), k\, j(j - i)\}$$

$$B \in \{kj(i + j), k\, i(i - j)\}$$

$$C = k(i^2 + j^2)$$

kde $i, j, k \in Z$.

Dôkaz: Rovnicu $A^2 - CA + B^2 - CB = 0$ riešime ako kvadratickú s premennou A:

$$A = \frac{C \pm \sqrt{C^2 + 4CB - 4B^2}}{2}$$

Keďže $A, B, C \in Z$, aj $\sqrt{C^2 + 4CB - 4B^2} \in Z$. Preto nutne $C^2 + 4CB - 4B^2 = D^2$ pre nejaké $D \in Z$. To znamená, že:

$$A = \frac{C \pm D}{2}$$

Rovnicu $4B^2 - 4CB - C^2 + D^2 = 0$ riešime ako kvadratickú s premennou B:

$$B = \frac{4C \pm \sqrt{16C^2 + 16C^2 - 16D^2}}{8} = \frac{C \pm \sqrt{2C^2 - D^2}}{2}$$

Keďže $B, C \in Z$, aj $\sqrt{2C^2 - D^2} \in Z$. Preto nutne $2C^2 - D^2 = E^2$ pre nejaké $E \in Z$. To znamená, že

$$B = \frac{C \pm E}{2}$$

Dostali sme sa k rovnici $D^2 + E^2 = 2C^2$, ktorá má podľa vety 2.6 parametrizáciu:

$$D = w(u^2 + 2uv - v^2)$$

$$E = w(-u^2 + 2uv + v^2)$$

$$C = w(u^2 + v^2)$$

Podľa toho platí:

$$A = \frac{C \pm D}{2} = w\frac{u^2 + v^2 \pm (u^2 + 2uv - v^2)}{2} \to A_1 = wu(u + v),\ A_2 = wv(v - u)$$

$$B = \frac{C \pm E}{2} = w\frac{u^2 + v^2 \pm (-u^2 + 2uv + v^2)}{2} \to B_1 = wv(u + v),\ B_2 = wu(u - v)$$

To znamená, že:

$$A \in \{wu(u + v), wv(v - u)\}$$

$$B \in \{wv(u + v), wu(u - v)\}$$

Substitúciou $i = u, j = v, k = w$ dostaneme hľadaný vzťah.

ČASŤ 3: CIEĽ ROČNÍKOVÉHO PROJEKTU

Hypotéza 7: Jediný magický štvorec, pre ktorý platí, že 7 z jeho 9 prvkov sú štvorce, je

$$\begin{pmatrix} 373^2 & 289^2 & 565^2 \\ 360721 & 425^2 & 23^2 \\ 205^2 & 527^2 & 221121 \end{pmatrix}$$

a všetky jeho rotácie, symetrie, alebo k^2 násobky.

Hypotéza 8: Neexistuje magický štvorec, pre ktorý platí, že 8 z jeho 9 prvkov sú štvorce.

Hypotéza 9: Neexistuje magický štvorec, pre ktorý platí, že každý jeho prvok je štvorec.

Našou úlohou bude vytvoriť kolekciu algoritmov, ktoré budú efektívne preverovať hypotézu 7. Použijeme na to jazyk Python,

ČASŤ 4: VETY PRE HYPOTÉZU 7

Veta 4.1: Ak existuje magický štvorec v tvare

$$\begin{pmatrix} - & B^2 & C^2 \\ D^2 & - & F^2 \\ G^2 & H^2 & - \end{pmatrix}$$

tak musia existovať $p, q, r, s, u_1, v_1, u_2, v_2 \in Z$ také, že:

$$u_1 v_1 (u_1 + v_1)(u_1 - v_1) = u_2 v_2 (u_2 + v_2)(u_2 - v_2)$$

$$s = r \frac{{u_2}^2 - {v_2}^2}{2 u_1 v_1}$$

$$q = \frac{2 u_1 v_1}{r}$$

$$p = \frac{2 u_2 v_2}{r}$$

Dôkaz: Z definície magického štvorca a vety 1.3 musia platiť nasledovné vzťahy:

(i) $B^2 + H^2 = D^2 + F^2$
(ii) $D^2 + H^2 = 2C^2$
(iii) $B^2 + F^2 = 2G^2$

Aplikovaním vety 2.5 na (i) a vety 2.6 na (ii) a (iii) dostaneme:

$$B = pr + qs = {u_2}^2 + 2u_2 v_2 - {v_2}^2 \qquad F = pr - qs = -{u_2}^2 + 2u_2 v_2 + {v_2}^2$$

$$C = {u_1}^2 + {v_1}^2 \qquad G = {u_2}^2 + {v_2}^2$$

$$D = ps + qr = {u_1}^2 + 2u_1 v_1 - {v_1}^2 \qquad H = qr - ps = -{u_1}^2 + 2u_1 v_1 + {v_1}^2$$

Sčítaním vzťahov pre B, F dostaneme $pr = 2u_2 v_2$, ich odčítaním zase $qs = {u_2}^2 - {v_2}^2$.

Sčítaním vzťahov pre D, H dostaneme $qr = 2u_1 v_1$, ich odčítaním zase $ps = {u_1}^2 - {v_1}^2$.

Zo vzťahu $pr = 2u_2 v_2$ vyjadríme $p = \frac{2u_2 v_2}{r}$ a zo vzťahu $qr = 2u_1 v_1$ vyjadríme $q = \frac{2u_1 v_1}{r}$.

Dosadením do vzťahu $qs = {u_2}^2 - {v_2}^2$ dostaneme $\frac{2u_1 v_1}{r} s = {u_2}^2 - {v_2}^2$, z čoho $s = r \frac{{u_2}^2 - {v_2}^2}{2u_1 v_1}$.

Dosadením do posledného vzťahu $ps = {u_1}^2 - {v_1}^2$ dostaneme:

$$\frac{2u_2 v_2}{r} r \frac{{u_2}^2 - {v_2}^2}{2u_1 v_1} = {u_1}^2 - {v_1}^2$$

z čoho vieme odvodiť $u_1 v_1 ({u_1}^2 - {v_1}^2) = u_2 v_2 ({u_2}^2 - {v_2}^2)$. To je ekvivalentné s

$$u_1 v_1 (u_1 + v_1)(u_1 - v_1) = u_2 v_2 (u_2 + v_2)(u_2 - v_2)$$

Veta 4.2: Ak existuje magický štvorec v tvare

$$\begin{pmatrix} A^2 & B^2 & C^2 \\ - & E^2 & - \\ G^2 & H^2 & I^2 \end{pmatrix}$$

tak musia existovať navzájom rôzne celé čísla $x_1, x_2, y_1, y_2, z_1, z_2$ také, že platí:

(i) ani jeden z výrazov $x_1 + y_1 + z_1$, $x_2 + y_2 + z_2$, $x_1 + x_2$, $y_1 + y_2$, $z_1 + z_2$ nie je rovný nule

(ii) $\frac{{x_1}^2+{y_1}^2+{z_1}^2}{x_1+y_1+z_1} = \frac{{x_2}^2+{y_2}^2+{z_2}^2}{x_2+y_2+z_2} = \frac{{x_1}^2+{x_2}^2}{x_1+x_2} = \frac{{y_1}^2+{y_2}^2}{y_1+y_2} = \frac{{z_1}^2+{z_2}^2}{z_1+z_2} = E$

Dôkaz: Pre daný magický štvorec musí platiť:

$$A^2 + B^2 + C^2 = I^2 + H^2 + G^2 = 3E^2$$

$$A^2 + I^2 = B^2 + H^2 = C^2 + G^2 = 2E^2$$

Na prvú sústavu rovníc dvakrát uplatníme vetu 2.4. Tým dostaneme:

$$A = 2x_1 - \frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} \qquad G = 2z_2 - \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2}$$

$$B = 2y_1 - \frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} \qquad H = 2y_2 - \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2}$$

$$C = 2z_1 - \frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} \qquad I = 2x_2 - \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2}$$

$$E = \frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} = \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2}$$

Túto parametrizáciu na tri krát dosadíme do druhej sústavy rovníc:

$$A^2 + I^2 = 2E^2$$

$$\left(2x_1 - \frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1}\right)^2 + \left(2x_2 - \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2}\right)^2 = \left(\frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1}\right)^2 + \left(\frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2}\right)^2$$

$$4{x_1}^2 - 4x_1\frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} + 4{x_2}^2 - 4x_2\frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2} = 0$$

Keď z parametrizácie E využijeme, že $\frac{{x_1}^2+{y_1}^2+{z_1}^2}{x_1+y_1+z_1} = \frac{{x_2}^2+{y_2}^2+{z_2}^2}{x_2+y_2+z_2}$, dostaneme po úprave rovnosť

$$\frac{{x_1}^2 + {x_2}^2}{x_1 + x_2} = \frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1}$$

Analogickým postupom dostaneme po dosadení do rovníc $B^2 + H^2 = 2E^2$, resp. $C^2 + G^2 = 2E^2$ rovnosti $\frac{{y_1}^2+{y_2}^2}{y_1+y_2} = \frac{{x_1}^2+{y_1}^2+{z_1}^2}{x_1+y_1+z_1}$, resp. $\frac{{z_1}^2+{z_2}^2}{z_1+z_2} = \frac{{x_1}^2+{y_1}^2+{z_1}^2}{x_1+y_1+z_1}$. Po spojení všetkých troch rovností s parametrizáciou E získame hľadanú rovnosť.

Veta 4.3: Ak existuje magický štvorec v tvare

$$\begin{pmatrix} A^2 & B^2 & - \\ D^2 & E^2 & F^2 \\ - & H^2 & I^2 \end{pmatrix}$$

tak musia existovať $u_1, v_1, u_2, v_2, u_3, v_3 \in Z$ také, že:

$$2u_1v_1({u_1}^2 - {v_1}^2)({u_2}^2 + {v_2}^2)^2({u_3}^2 + {v_3}^2)^2 - u_2v_2({u_1}^2 + {v_1}^2)^2({u_2}^2 - {v_2}^2)({u_3}^2 + {v_3}^2)^2 + u_3v_3({u_1}^2 + {v_1}^2)^2({u_2}^2 + {v_2}^2)^2({u_3}^2 - {v_3}^2) = 0$$

Dôkaz: Pre daný magický štvorec musí platiť:

$$A^2 + I^2 = H^2 + B^2 = D^2 + F^2 = 2E^2$$

$$A^2 + B^2 = F^2 + I^2$$

Aplikovaním vety 2.6 na prvú sústavu rovníc dostaneme vzťahy:

$$A = w_1(u_1^2 + 2u_1v_1 - v_1^2) \qquad I = w_1(-u_1^2 + 2u_1v_1 + v_1^2)$$

$$H = w_2(u_2^2 + 2u_2v_2 - v_2^2) \qquad B = w_2(-u_2^2 + 2u_2v_2 + v_2^2)$$

$$D = w_3(u_3^2 + 2u_3v_3 - v_3^2) \qquad F = w_3(-u_3^2 + 2u_3v_3 + v_3^2)$$

$$E = w_1({u_1}^2 + {v_1}^2) = w_2({u_2}^2 + {v_2}^2) = w_3({u_3}^2 + {v_3}^2)$$

Zo vzťahu pre E si vyjadríme $w_2 = \frac{w_1({u_1}^2+{v_1}^2)}{({u_2}^2+{v_2}^2)}$ a $w_3 = \frac{w_1({u_1}^2+{v_1}^2)}{({u_3}^2+{v_3}^2)}$.

Dosadením do druhej rovnice dostaneme:

$$A^2 + B^2 = F^2 + I^2$$

$$\begin{aligned} {w_1}^2(u_1^2 + 2u_1v_1 - v_1^2)^2 + {w_2}^2(-u_2^2 + 2u_2v_2 + v_2^2)^2 \\ = {w_3}^2(-u_3^2 + 2u_3v_3 + v_3^2)^2 + {w_1}^2(-u_1^2 + 2u_1v_1 + v_1^2)^2 \end{aligned}$$

To vieme ekvivalentnými úpravami upraviť na tvar:

$$2u_1v_1{w_1}^2({u_1}^2 - {v_1}^2) + u_2v_2{w_2}^2({v_2}^2 - {u_2}^2) = u_3v_3{w_3}^2({v_3}^2 - {u_3}^2)$$

Keď v tomto tvare dosadíme $w_2 = \frac{w_1({u_1}^2+{v_1}^2)}{({u_2}^2+{v_2}^2)}$ a $w_3 = \frac{w_1({u_1}^2+{v_1}^2)}{({u_3}^2+{v_3}^2)}$ a potom sa zbavíme menovateľov, dostaneme rovnosť zo zadania.

Veta 4.4: Ak existuje magický štvorec v tvare

$$\begin{pmatrix} A^2 & B^2 & C^2 \\ D^2 & E^2 & F^2 \\ - & H^2 & - \end{pmatrix}$$

tak musia existovať $u_1, v_1, u_2, v_2, u_3, v_3, u_4, v_4 \in Z$ také, že výrazy

$$(-u_1^2 + 2u_1v_1 + v_1^2)({u_2}^2 + {v_2}^2)(u_3^2 + 2u_3v_3 - v_3^2)(u_4^2 + 2u_4v_4 - v_4^2)$$

$$({u_1}^2 + {v_1}^2)(-u_2^2 + 2u_2v_2 + v_2^2)(-u_3^2 + 2u_3v_3 + v_3^2)(u_4^2 + 2u_4v_4 - v_4^2)$$

$$({u_1}^2 + {v_1}^2)(u_2^2 + 2u_2v_2 - v_2^2)(u_3^2 + 2u_3v_3 - v_3^2)(-u_4^2 + 2u_4v_4 + v_4^2)$$

majú rovnakú hodnotu.

Dôkaz: Pre daný magický štvorec musí platiť:

$$B^2 + H^2 = D^2 + F^2 = 2E^2$$

$$F^2 + H^2 = 2A^2$$

$$D^2 + H^2 = 2C^2$$

Aplikovaním vety 2.6 na všetky sústavy rovníc dostaneme vzťahy:

$$A = w_3({u_3}^2 + {v_3}^2)$$
$$B = w_1(u_1^2 + 2u_1v_1 - v_1^2)$$
$$C = w_3({u_4}^2 + {v_4}^2)$$
$$D = w_2(u_2^2 + 2u_2v_2 - v_2^2) = w_4(u_4^2 + 2u_4v_4 - v_4^2)$$
$$E = w_1({u_1}^2 + {v_1}^2) = w_2({u_2}^2 + {v_2}^2)$$
$$F = w_2(-u_2^2 + 2u_2v_2 + v_2^2) = w_3(u_3^2 + 2u_3v_3 - v_3^2)$$
$$H = w_1(-u_1^2 + 2u_1v_1 + v_1^2) = w_3(-u_3^2 + 2u_3v_3 + v_3^2) = w_4(-u_4^2 + 2u_4v_4 + v_4^2)$$

Zo vzťahov pre E, F, D vyjadríme $w_1 = \frac{w_2({u_2}^2+{v_2}^2)}{({u_1}^2+{v_1}^2)}$, $w_3 = \frac{w_2(-u_2^2+2u_2v_2+v_2^2)}{(u_3^2+2u_3v_3-v_3^2)}$, $w_4 = \frac{w_2(u_2^2+2u_2v_2-v_2^2)}{(u_4^2+2u_4v_4-v_4^2)}$. Po dosadení týchto vyjadrení do vzťahu pre H a ekvivalentných úpravách dostaneme vzťah zo zadania.

<u>Veta 4.5</u>: Magické štvorce v jednom z nasledovných tvarov

$$\begin{pmatrix} A^2 & - & C^2 \\ - & E^2 & - \\ G^2 & - & I^2 \end{pmatrix} \text{alebo} \begin{pmatrix} - & B^2 & - \\ D^2 & E^2 & F^2 \\ - & H^2 & - \end{pmatrix} \text{alebo} \begin{pmatrix} A^2 & B^2 & - \\ - & E^2 & - \\ - & H^2 & I^2 \end{pmatrix}$$

vieme parametrizovať tak, že $E = x({u_1}^2 + {v_1}^2)({u_2}^2 + {v_2}^2)$ a zvyšné štyri členy sú v tvare:

$$x({u_1}^2 + {v_1}^2)(u_2^2 + 2u_2v_2 - v_2^2) \qquad x(u_1^2 + 2u_1v_1 - v_1^2)({u_2}^2 + {v_2}^2)$$
$$x({u_1}^2 + {v_1}^2)(-u_2^2 + 2u_2v_2 + v_2^2) \qquad x(-u_1^2 + 2u_1v_1 + v_1^2)({u_2}^2 + {v_2}^2)$$

<u>Dôkaz</u>: Dôkaz urobíme len pre prvý tvar magického štvorca, ostatné tvary sa dokazujú analogicky.

Musí platiť $A^2 + I^2 = C^2 + G^2 = 2E^2$. Použitím vety 2.6 dostaneme vzťahy:

$$A = w_1(u_1^2 + 2u_1v_1 - v_1^2) \qquad G = w_2(-u_2^2 + 2u_2v_2 + v_2^2)$$
$$C = w_2(u_2^2 + 2u_2v_2 - v_2^2) \qquad I = w_1(-u_1^2 + 2u_1v_1 + v_1^2)$$
$$E = w_1({u_1}^2 + {v_1}^2) = w_2({u_2}^2 + {v_2}^2)$$

Zo vzťahu pre E vyjadríme $w_2 = \frac{w_1({u_1}^2+{v_1}^2)}{({u_2}^2+{v_2}^2)}$. Potom zvolíme substitúciu $x = \frac{w_1}{({u_2}^2+{v_2}^2)}$ (môžeme, lebo všetky premenné teraz vieme regulovať pomocou w_1). Tým dostaneme parametrizáciu zo zadania.

ČASŤ 5: ALGORITMY NA HYPOTÉZU 7

Algoritmy pre vetu 4.1:

- Nájdeme celé u_1, v_1, u_2, v_2 také, že $u_1 v_1 (u_1 + v_1)(u_1 - v_1) = u_2 v_2 (u_2 + v_2)(u_2 - v_2)$. Potom nájdeme také celé r, aby boli zlomky $r \frac{{u_2}^2 - {v_2}^2}{2 u_1 v_1}, \frac{2 u_1 v_1}{r}, \frac{2 u_2 v_2}{r}$ celé čísla. To urobíme tak, že vypočítame $lcm(2u_1 v_1, 2u_2 v_2)$ a ak je deliteľný výrazom $\frac{2 u_1 v_1}{\gcd(2u_1 v_1, {u_2}^2 - {v_2}^2)}$, tak definujeme $r = \frac{2 u_1 v_1}{\gcd(2u_1 v_1, {u_2}^2 - {v_2}^2)}$. Z neho vypočítame $s = r \frac{{u_2}^2 - {v_2}^2}{2 u_1 v_1}, q = \frac{2 u_1 v_1}{r}, p = \frac{2 u_2 v_2}{r}$. Potom vypočítame členy potenciálneho magického štvorca:

$$B = (pr + qs)^2$$
$$D = (ps + qr)^2$$
$$F = (pr - qs)^2$$
$$H = (qr - ps)^2$$
$$C = ({u_1}^2 + {v_1}^2)^2$$
$$G = ({u_2}^2 + {v_2}^2)^2$$
$$E = \frac{B + H}{2}$$
$$A = D + E + F - B - C$$
$$I = D + E + F - G - H$$

Šesť členov sú určite štvorce, ostáva overiť magickosť a to, či nejaké z A, E, I sú štvorce.

Algoritmy pre vetu 4.2:

- Generujeme všetky možné $x_1, x_2, y_1, y_2, z_1, z_2$ podľa vety 4.1 a overujeme (i) a (ii).
- Generujeme všetky možné i, j, k podľa vety 2.7. Potom $K = k(i^2 + j^2)$. Snažíme sa pre rôzne i, j, k získať rovnaké K, čím získame odlišné A, B, pre ktoré platí $A^2 + B^2 = K(A + B)$. Tieto dvojice (A, B) budú postupne dvojicami $(x_1, x_2), (y_1, y_2), (z_1, z_2)$. Tým máme z vety 4.2 splnených viac rovníc a musíme overovať len podmienku $\frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} = \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2} = K$.
- Pred generovaním urobíme šikovné pozorovanie. Všimnime si, že ak platí z vety 4.2 $\frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} = \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2} = \frac{{x_1}^2 + {x_2}^2}{x_1 + x_2} = \frac{{y_1}^2 + {y_2}^2}{y_1 + y_2} = K$, tak platí aj $\frac{{z_1}^2 + {z_2}^2}{z_1 + z_2} = K$ (to nie je ťažké dokázať). Preto generujeme len rôzne dvojice $(x_1, x_2), (y_1, y_2)$ pre dané K. Potom stačí nájsť také z_1, z_2, že platí $\frac{{x_1}^2 + {y_1}^2 + {z_1}^2}{x_1 + y_1 + z_1} = \frac{{x_2}^2 + {y_2}^2 + {z_2}^2}{x_2 + y_2 + z_2} = K$.
- Ešte šikovnejší trik je prepísať si sústavu z vety 4.2 nasledovne:

$$\left(\frac{x_1}{K}\right)^2 - \frac{x_1}{K} + \left(\frac{y_1}{K}\right)^2 - \frac{y_1}{K} + \left(\frac{z_1}{K}\right)^2 - \frac{z_1}{K} = 0$$

$$\left(\frac{x_2}{K}\right)^2 - \frac{x_2}{K} + \left(\frac{y_2}{K}\right)^2 - \frac{y_2}{K} + \left(\frac{z_2}{K}\right)^2 - \frac{z_2}{K} = 0$$

$$\left(\frac{x_1}{K}\right)^2 - \frac{x_1}{K} + \left(\frac{x_2}{K}\right)^2 - \frac{x_2}{K} = 0$$

$$\left(\frac{y_1}{K}\right)^2 - \frac{y_1}{K} + \left(\frac{y_2}{K}\right)^2 - \frac{y_2}{K} = 0$$

Potom po vhodnej substitúcii riešime sústavu rovníc v obore racionálnych čísel.

Algoritmy pre vetu 4.3: Generujeme všetky možné $u_1, v_1, u_2, v_2, u_3, v_3$ podľa vety 4.3.

Algoritmy pre vetu 4.4: Generujeme všetky možné $u_1, v_1, u_2, v_2, u_3, v_3, u_4, v_4$ podľa vety 4.4.

Algoritmy pre vetu 4.5: Uvedené v nasledovnej časti.

ČASŤ 6: IMPLEMENTÁCIA PROGRAMU

Počas zimného a letného semestra sme sa zamerali na efektívnu implementáciu programu. Hľadali sme algoritmus pre vetu 4.5. Spomedzi všetkých viet sme si zvolili práve tú, lebo

1. bola flexibilná a ľahko implementovateľná
2. zaručovala, že každý skúmaný magický štvorec obsahuje aspoň 5 štvorcov (silná vlastnosť)
3. výsledok sa dal dobre graficky reprezentovať (t. j. koľko štvorcov sa našlo pre akú hodnotu)

Využitím iných viet by sme si prácu zbytočne skomplikovali.

Program sa spúšťa cez príkazový riadok. Používateľ zadá štyri parametre:

- typ vyhľadávania
  1. úplné (bruteforce) – prehľadá všetky u_1, v_1, u_2, v_2 v danom intervale
  2. náhodné (random) – prehľadá náhodné u_1, v_1, u_2, v_2 v intervale daný počet krát
- dolnú hranicu intervalu
- hornú hranicu intervalu
- počet iterácií v náhodnom prehľadávaní (dobrovoľné)

Počas behu algoritmu sa používateľovi priebežne vypisuje progress bar a údaj o tom, koľko (približne) času ostáva do konca. Všetky nájdené riešenia sa zapisujú do textového súboru. Na konci sa ukáže graf početnosti vyhovujúcich magických štvorcov (tých, čo majú aspoň 6 štvorcov) na danom intervale. Ak sa našli aj riešenia so 7 štvorcami, vypíšu sa.

Pri vymýšľaní algoritmu sme stáli pred neľahkou úlohou: ako prechádzať vyhovujúce u_1, v_1, u_2, v_2 čo najefektívnejšie (parameter x z vety slúži len ako konštantný násobok, ktorý na konečný výsledok nemá vplyv). Parametre u_1, v_1, u_2, v_2 vedeli vytvoriť túto množinu štvorcov:

$$\begin{pmatrix} ({u_1}^2+{v_1}^2)^2(u_2^2+2u_2v_2-v_2^2)^2 & - & (u_1^2+2u_1v_1-v_1^2)^2({u_2}^2+{v_2}^2)^2 \\ - & ({u_1}^2+{v_1}^2)^2({u_2}^2+{v_2}^2)^2 & - \\ (-u_1^2+2u_1v_1+v_1^2)^2({u_2}^2+{v_2}^2)^2 & - & ({u_1}^2+{v_1}^2)^2(-u_2^2+2u_2v_2+v_2^2)^2 \end{pmatrix}$$

$$\begin{pmatrix} - & ({u_1}^2+{v_1}^2)^2(u_2^2+2u_2v_2-v_2^2)^2 & - \\ (u_1^2+2u_1v_1-v_1^2)^2({u_2}^2+{v_2}^2)^2 & ({u_1}^2+{v_1}^2)^2({u_2}^2+{v_2}^2)^2 & (-u_1^2+2u_1v_1+v_1^2)^2({u_2}^2+{v_2}^2)^2 \\ - & ({u_1}^2+{v_1}^2)^2(-u_2^2+2u_2v_2+v_2^2)^2 & - \end{pmatrix}$$

$$\begin{pmatrix} ({u_1}^2+{v_1}^2)^2(u_2^2+2u_2v_2-v_2^2)^2 & (u_1^2+2u_1v_1-v_1^2)^2({u_2}^2+{v_2}^2)^2 & - \\ - & ({u_1}^2+{v_1}^2)^2({u_2}^2+{v_2}^2)^2 & - \\ - & (-u_1^2+2u_1v_1+v_1^2)^2({u_2}^2+{v_2}^2)^2 & ({u_1}^2+{v_1}^2)^2(-u_2^2+2u_2v_2+v_2^2)^2 \end{pmatrix}$$

$$\begin{pmatrix} ({u_1}^2+{v_1}^2)^2(u_2^2+2u_2v_2-v_2^2)^2 & (-u_1^2+2u_1v_1+v_1^2)^2({u_2}^2+{v_2}^2)^2 & - \\ - & ({u_1}^2+{v_1}^2)^2({u_2}^2+{v_2}^2)^2 & - \\ - & (u_1^2+2u_1v_1-v_1^2)^2({u_2}^2+{v_2}^2)^2 & ({u_1}^2+{v_1}^2)^2(-u_2^2+2u_2v_2+v_2^2)^2 \end{pmatrix}$$

Môžeme si všimnúť nasledovné štyri veci:

- Ak $u_1 = v_1$ (resp. $u_2 = v_2$), tak štvorce nevyhovujú, pretože obsahujú duplicitné prvky.
- Ak vymeníme medzi sebou u_1 a v_1 (resp. u_2 a v_2), nič nepokazíme – dostaneme rovnakú množinu možných štvorcov (akurát osovo prevrátených).

- Ak vymeníme medzi sebou u_1 a u_2 a zároveň v_1 a v_2, nič nepokazíme – dostaneme rovnakú množinu možných štvorcov (akurát osovo prevrátených).
- Ak majú u_1 a v_1 (resp. u_2 a v_2) spoločného deliteľa väčšieho ako 1, tento deliteľ sa prejaví ako konštantný násobok a nebude mať vplyv na výsledok.

Na základe týchto vlastností stačí skúmať také u_1, v_1, u_2, v_2, že

$$u_1 < v_1 \ \wedge \ u_2 < v_2 \ \wedge \ u_1 < u_2 \ \wedge \ \gcd(u_1, v_1) = 1 \ \wedge \ \gcd(u_2, v_2) = 1$$

Aby sme prechádzali naozaj len potrebné u_1, v_1, u_2, v_2, vytvoríme si pole, do ktorého pridáme všetky usporiadané dvojice čísel (u, v) také, že $u < v$ a zároveň $\gcd(u, v) = 1$. Toto pole na konci utriedime podľa hodnoty v v každej dvojici. O všetko sa stará funkcia **add_all_pairs**.

Pri vyhľadávaní potom funkcia **run_all_pairs** (resp. **run_random_pairs**) prejde všetky (resp. náhodné) páry týchto dvojíc (u_1, v_1) a (u_2, v_2). Pre každý vygeneruje funkcia **run_configuration** množinu štvorcov (tie, čo sú vypísané vyššie). Každý štvorec je najprv vykrátený a potom umocnený na druhú funkciou **normalize**. Ak sa ukáže, že štvorec neobsahuje duplicitné prvky a obsahuje aspoň šesť štvorcov, je na konci výpočtu pridaný medzi riešenia (vyhovujúce štvorce) funkciou **add_solution**.

Ostal nám problém: ako si pamätať, či sme dané riešenie už predtým nenašli? Ak nejaký štvorec vznikne rotáciou, symetriou alebo násobkom z iného nájdeného štvorca, tak sme nové riešenie nenašli. Pomôže nám nasledovná veta:

Veta 6.1: Každý magický štvorec je jednoznačne definovaný svojím stredom a dvoma najmenšími rohmi, pričom tieto tri hodnoty sú nesúdeliteľné.

Dôkaz: Vezmeme si ľubovoľný magický štvorec a ukážeme si, ako ho dať do spomínaného tvaru. Ak sú jeho hodnoty súdeliteľné, jednoducho ich vykrátime. Tým máme jednoznačne určený stred S. Teraz budeme štvorec otáčať dovtedy, kým sa jeho najmenší roh (označíme ho N) nedostane do ľavého horného rohu. Označíme druhý najmenší roh D. Teoreticky sú možné len tieto tri situácie:

$$\begin{pmatrix} N & - & D \\ - & S & - \\ - & - & - \end{pmatrix} \text{alebo} \begin{pmatrix} N & - & - \\ - & S & - \\ D & - & - \end{pmatrix} \text{alebo} \begin{pmatrix} N & - & - \\ - & S & - \\ - & - & D \end{pmatrix}$$

Dokážeme, že vždy vieme dostať D do pravého horného rohu. Prvý prípad triviálne vyhovuje, zatiaľ čo v druhom prípade môžeme štvorec osovo prevrátiť podľa vedľajšej diagonály (tej, kde je N) a dostať D na požadované miesto.

Tretí prípad nemôže nastať. Postupujme sporom. Nech $\begin{pmatrix} N & - & - \\ - & S & - \\ - & - & D \end{pmatrix}$ je magický štvorec, ktorý má stred S a jeho dva najmenšie rohy sú N, D. Na opačnej diagonále sa však potom nachádzajú dva najväčšie rohy, z čoho vyplýva, že súčet hodnôt na diagonálach je rôzny (to je spor s magickosťou).

Z troch hodnôt $\begin{pmatrix} N & - & D \\ - & S & - \\ - & - & - \end{pmatrix}$ vieme jednoznačne zrekonštruovať magický štvorec. Magický súčet je 3S (podľa vety 1.2), čím vieme dopočítať zvyšné dva rohy. Z toho už dopočítame aj ostatné hodnoty.

Ak si chceme zapamätať magický štvorec, stačí si uložiť len hodnoty S, N, D (napr. do poľa, alebo ako reťazec do asociatívneho poľa - ako je implementované v našom programe). Tento reťazec sme si pomenovali **index magického štvorca** (v programe ho vracia funkcia **get_index**).

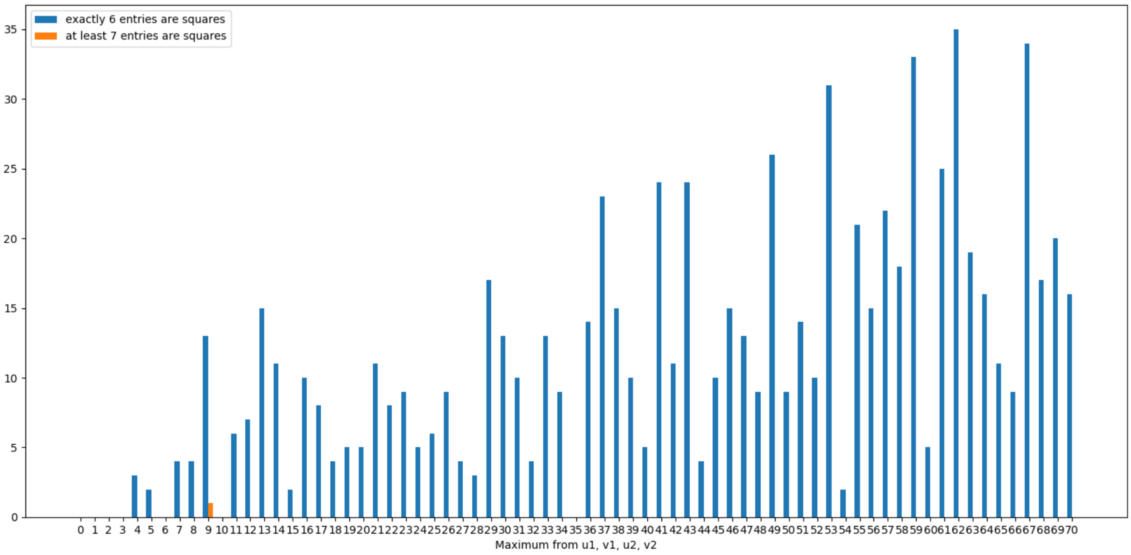
ČASŤ 7: VÝSLEDKY

V zimnom semestri sme sa zamerali na vetu 4.5. Konkrétne sme generovali všetky magické štvorce, ktoré obsahovali aspoň 5 štvorcov. Využili sme všetky tri konfigurácie z vety 4.5:

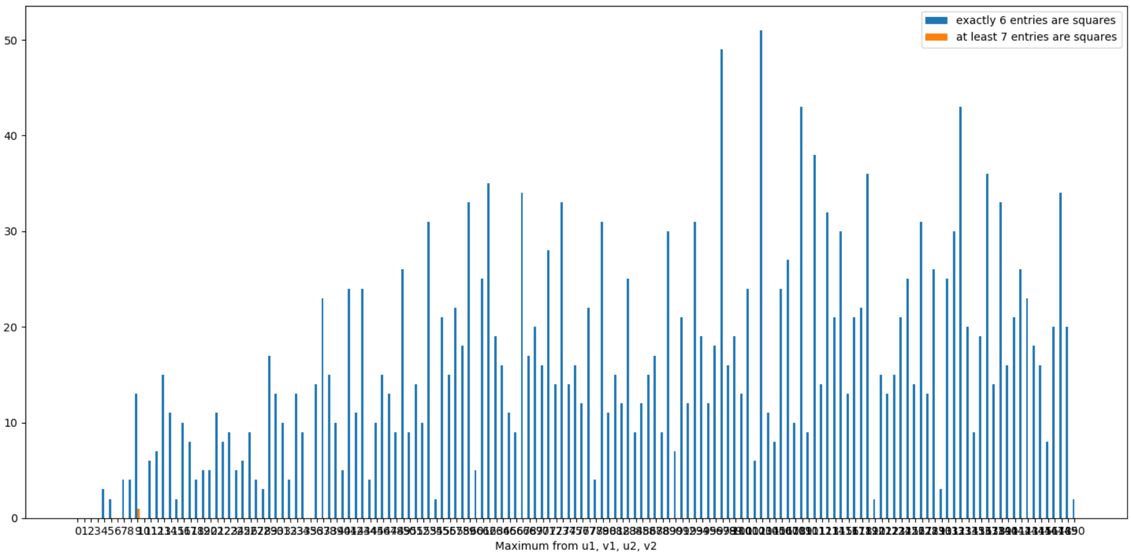
$$\begin{pmatrix} A^2 & - & C^2 \\ - & E^2 & - \\ G^2 & - & I^2 \end{pmatrix} \text{alebo} \begin{pmatrix} - & B^2 & - \\ D^2 & E^2 & F^2 \\ - & H^2 & - \end{pmatrix} \text{alebo} \begin{pmatrix} A^2 & B^2 & - \\ - & E^2 & - \\ - & H^2 & I^2 \end{pmatrix}$$

V programe je možné generovať riešenia náhodne alebo hrubou silou. Na konci výpočtu hrubou silou sa objaví graf. Ten popisuje, koľko rôznych magických štvorcov s aspoň šiestimi štvorcami existuje pre dané maximum zo štvorice u_1, v_1, u_2, v_2.

Graf riešení pre $u_1, v_1, u_2, v_2 \leq 70$:



Graf riešení pre $u_1, v_1, u_2, v_2 \leq 150$:



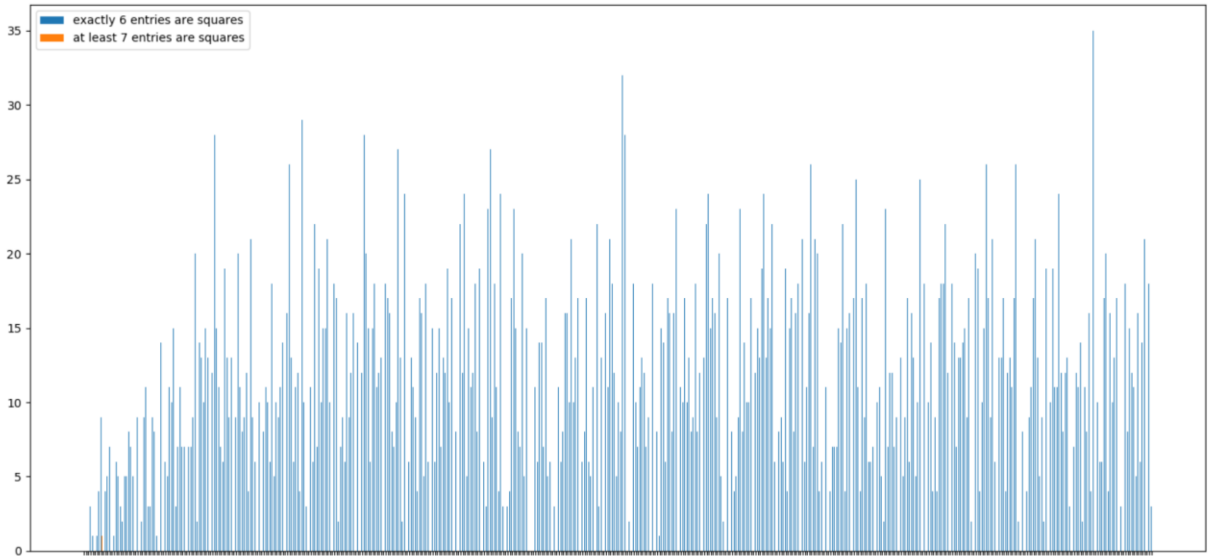
Pre $u_1, v_1, u_2, v_2 \leq 150$ teda existuje iba jediné riešenie so siedmimi štvorcami (to, ktoré poznáme).

V letnom semestri sme pokračovali s vetou 4.5. Náš program prešiel výraznými zmenami:

- Odstránili sme chybu pri počítaní, ktorá spôsobila, že sme tú istú konfiguráciu u_1, v_1, u_2, v_2 overovali viac krát. To výrazne zredukovalo počet nutných operácií.
- Pridali sme možnosť výberu spodnej hranice. Odteraz je možné hľadať riešenia v ľubovoľnom intervale od L do U (L je spodná hranica, U je vrchná hranica). Ak napr. úspešne prehľadáme všetko v intervale od 1 do 500, už sa stačí zaoberať len riešeniami väčšími ako 500.
- Parametre sa zadávajú cez argparser, nie cez štandardný vstup.
- Komplikovaný pytest nahradil lepší unittest.
- Zvýšili sme odolnosť programu voči výpadkom. Po každej iterácii sa zapíšu do logu (textového súboru) nájdené magické štvorce (tie, pre ktoré platí, že aspoň 6 ich čísel sú štvorce). Zápisy sú permanentné, čo znamená, že ak dôjde k výpadku, získané dáta sa nestratia.
- Odhad času, ktorý ostáva do konca bruteforce vyhľadávania, je omnoho presnejší. Ráta sa totiž vzhľadom na aktuálny výkon počítača.
- Najväčším zlepšením bola úspešná a efektívna implementácia multiprocessingu (paralelného programovania). Použili sme na to multiprocessing Pool a jeho metódu map (viac konfigurácií u_1, v_1, u_2, v_2 sa prechádzalo naraz). Tým sme výrazne znížili čas potrebný na prehľadávanie. Na demonštráciu: predtým trvalo prehľadávanie od 1 do 150 približne 7 hodín (teraz to zaberie menej ako 7 minút).

Od 28. 5. 2020 do 29. 5. 2020 prebehlo intenzívne prehľadávanie pre u_1, v_1, u_2, v_2 od 1 do 500. Program na 8 CPU jadrách bežal približne 11 hodín. Bolo nájdených 5862 magických štvorcov, ktoré obsahovali aspoň 6 štvorcov. Bohužiaľ, podarilo sa nájsť iba jediné riešenie obsahujúce aspoň 7 štvorcov (to, ktoré poznáme).

Zhustený graf riešení pre $u_1, v_1, u_2, v_2 \leq 500$:



Poznámky

- čas potrebný na prehľadanie sa môže líšiť v závislosti od počtu CPU jadier, výkonu a aplikácii bežiacich na pozadí počítača
- grafy z letného a zimného semestra sa líšia, pretože použili iný spôsob prehľadávania... implementácia z časti 6 sa viaže na metódu použitú v letnom semestri