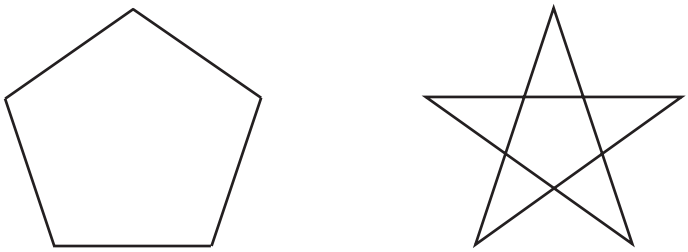
Pravilni mrežni večkotniki

Milan Hladnik

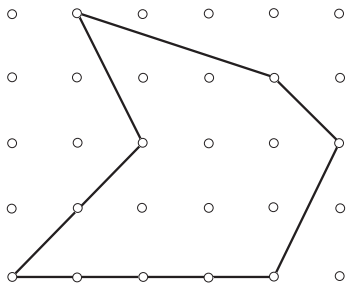
September 2010

Pod pojmom večkotnik običajno razumemo enostaven ravninski lik, omejen s sklenjeno poligonsko črto (ki sama sebe ne seka). Kaj je *pravilni* (*regularni*) večkotnik, pa tudi vemo: to je večkotnik, ki ima vse stranice in vse notranje kote enake, torej enakostraničen in enakokoten večkotnik (slika 1). Ni dovolj, da rečemo npr. samo enakokoten ali samo enakostraničen večkotnik (to zadošča samo za trikotnike, pri $n > 3$ pa je takih likov veliko: enakokotni štirikotnik je npr. vsak pravokotnik, enakostranični vsak romb, medtem ko je pravilni štirikotnik samo kvadrat). Enakokotne in enakostranične večkotnike imenujemo z eno besedo *polpravilni* (*semiregularni*) večkotniki. Zanimali nas bodo predvsem pravilni večkotniki, nekaj rezultatov bo tudi bolj splošnih.



Slika 1. Enostavni in neenostavni pravilni petkotnik

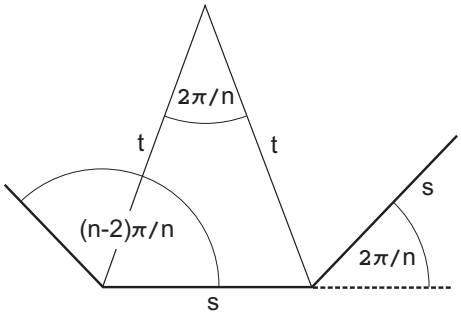
Mrežni večkotnik je tak večkotnik, ki ima za oglišča točke dane kvadratne (celoštevilske) ravninske mreže $\mathbb{Z}^2$, torej točke v koordinatni ravnini s celoštevilskimi koordinatami (glej sliko 2). Kasneje bomo potrebovali tudi kvadratno prostorsko mrežo $\mathbb{Z}^3$. Prav tako bi lahko proučevali večkotnike na drugačnih mrežah: trikotni, šestkotni (satovju), rombični itd., vendar ostanimo pri dobro znani kvadratni mreži.



Slika 2. Enostavni mrežni večkotnik

Zanima nas osnovno vprašanje, kateri pravilni n-kotniki so hkrati mrežni. Videli bomo, da jih ni prav veliko oziroma da so taki le kvadrati. Vendar bomo pogoje kasneje tudi omilili in našli še druge (npr. mrežne enakokotne ali enakostranične večkotnike, večkotnike z oglišči v kvadratni prostorski mreži itd.).

Vsak enostaven enakokotni večkotnik je nujno konveksen. Zunanji kot n-kotnika je vedno $2\pi/n$, notranji pa $\pi - 2\pi/n = (n-2)\pi/2$ (glej sliko 3).



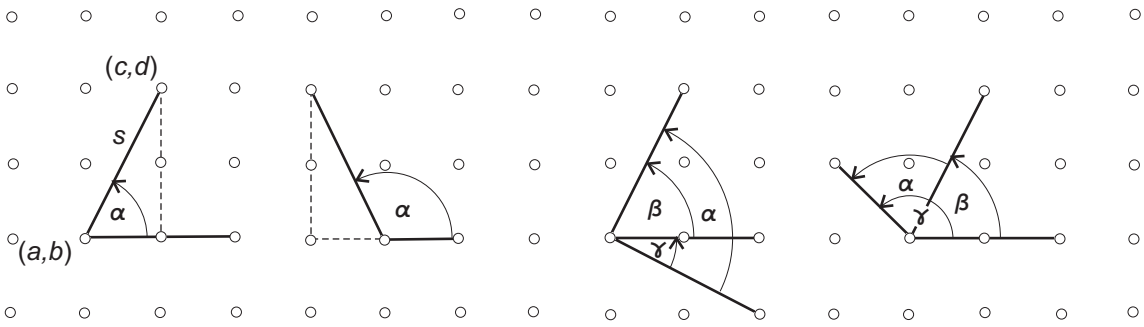
Slika 3. Notranji in zunanji koti v pravilnem večkotniku

1. Pravilni večkotniki na ravninski mreži

Mrežna daljica je daljica, katere krajišči sta mrežni točki. *Mrežni kot* je kot med dvema mrežnima daljicama s s skupnim krajiščem.

Trditev 1. *Za mrežne daljice in kote veljajo naslednja dejstva*:
(a) *Kvadrat dolžine mrežne daljice je celo število.*
(b) *Naklon mrežne daljice je racionalen.*
(c) *Tangens mrežnega kota je racionalen.*

Dokaz. Če ima mrežna daljica krajišči (a, b) in (c, d), je kvadrat njene dolžine enak $s^2 = (c-a)^2 + (d-b)^2$, njen naklon pa $k = (d-b)/(c-a) \in \mathbb{Q}$ (pri navpični daljici imamo lahko, z nekoliko nasilja, tudi neskončnost za racionalno število). Torej veljata točki (a) in (b). Za dokaz točke (c) uporabimo formulo $\operatorname{tg}\alpha = (\operatorname{tg}\gamma \pm \operatorname{tg}\beta)/(1 \mp \operatorname{tg}\gamma\operatorname{tg}\beta) \in \mathbb{Q}$ (upoštevamo več možnosti, glej sliko 4).



Slika 4. Dolžina in naklon mrežne daljice, tangens mrežnega kota

Trikotnik

Trditev 2. *Noben enakostranični trikotnik ni mrežni.*

Dokaz. Tangens notranjega kota je zdaj enak $\sqrt{3}$, kar ni racionalno število; torej tak trikotnik po trditvi 1(c) ne more biti mrežni.

Alternativni dokaz poteka s pomočjo ugotovitve, da mora biti ploščina vsakega mrežnega trikotnika racionalno število (lahko uporabimo znano determinantno formulo za ploščino trikotnika z znanimi koordinatami oglišč: $A = |det(x_1, y_1, 1; x_2, y_2, 1; x_3, y_3, 1)|/2$ ali pa Pickov izrek $A = I + B/2 - 1$, če ga poznamo). To pa pri enakostraničnem trikotniku ne drži, saj je ploščina enaka $s^2\sqrt{3}/4$, kjer je s^2 (po prvem dejstvu) naravno število.

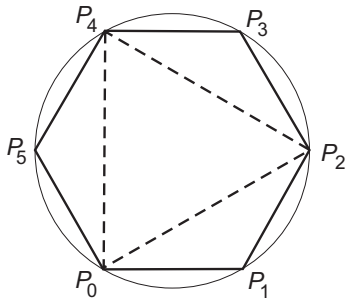
Pogosto je dokazovanje podobnih trditev, kot bomo še videli, povezano z elementarno teorijo števil. Za primer in za pokušino navedimo še en preprost številsko teoretičen dokaz zgornje trditve. Podal ga je že E. Lucas leta 1878 (glej [3]).

Drugačen dokaz trditve 2. Eno oglišče hipotetičnega pravilnega mrežnega trikotnika naj bo v izhodišču $(0,0)$, druga dva pa v celoštevilskih točkah (x,y) in (u,v). Predpostavimo, da je to najmanjši tak trikotnik, se pravi, da cela števila x,y,u,v nimajo skupnega faktorja. Iz pogoja enakostraničnosti dobimo $x^2+y^2=u^2+v^2=(x-u)^2+(y-v)^2$ oziroma $x^2+y^2=u^2+v^2=2(au+yv)$. Odtod vidimo, da je $x^2+y^2+u^2+v^2=4(au+yv)$. Ker števila x,y,u,v niso vsa soda in je vsota njihovih kvadratov deljiva s 4, morajo biti vsa liha. V tem primeru pa diofantska enačba $x^2+y^2=(x-u)^2+(y-v)^2$ nima rešitev, saj je na levi strani število, ki je deljivo z 2, ne pa s 4, na desni strani pa število, ki je deljivo s 4.

Trditev 3. *Če ni pravilnega mrežnega m-kotnika, tudi ni pravilnega mrežnega mk-kotnika* ($k \in \mathbb{N}$).

Dokaz. V vsakem takem liku z oglišči $P_0, P_1, ..., P_{mk-1}$ lahko najdemo tudi vpeti pravilni m-kotnik z oglišči $P_0, P_k, P_{2k}, ..., P_{(m-1)k}$ (glej sliko 5).

Posledica 1. *Noben pravilni šestkotnik ni mrežni.*



Slika 5. Pravilni šestkotnik z vpetim enakostraničnim trikotnikom

Opomba. Kako je z drugimi trikotniki (pravilnimi ali ne)? Kateri od njih so podobni mrežnim? Njihovo karakterizacijo je podal J. McCarthy (glej [3]): *Trikotnik je podoben mrežnemu trikotniku v $\mathbb{Z}^2$ natanko takrat, ko so tangensi vseh kotov racionalni.* M.J. Beeson je v [3] obravnaval tudi vprašanje, kdaj je trikotnik podoben mrežnemu trikotniku v večrazsežni mreži $\mathbb{Z}^k$. Ugotovil je, da je to res natanko takrat, ko so kvadrati tangensov vseh kotov racionalni. In še zanimivost: natanko isti trikotniki so podobni mrežnim trikotnikom v $\mathbb{Z}^3$ in v $\mathbb{Z}^4$ in sicer so to tisti, katerih tangensi kotov so racionalni večkratniki števila $\sqrt{m}$, kjer je m vsota kvadratov treh celih števil.

Kvadrat

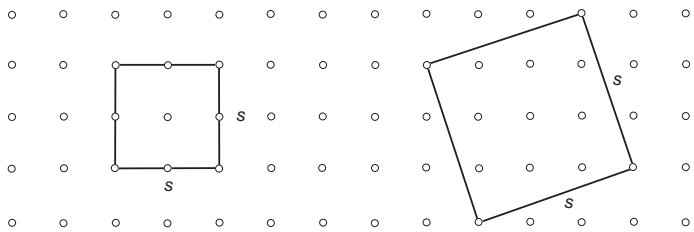
Videli smo, da pravilni mrežni trikotnik ni možen. Kako pa je s kvadratom? Naj bo s stranica kvadrata. Potem velja:

(a) *Če $s^2 \notin \mathbb{N}$, kvadrat ne more biti mrežni* (trditev 1(a)).

(b) *Če je $s^2 \in \mathbb{N}$, je kvadrat lahko mrežni, in sicer v dveh primerih*:

(i) $s \in \mathbb{N}$; tedaj je ploščina kvadrata popoln kvadrat, mrežni kvadrat ima vodoravne in navpične stranice.

(ii) $s \notin \mathbb{N}$; tedaj je $s=\sqrt{n}$, $n=a^2+b^2$, $a,b \in \mathbb{N}$, npr. $s=\sqrt{2}$ ali $s=\sqrt{5}$. Kvadrat ima zdaj poševne stranice (slika 6). Pri katerih naravnih številih n je to možno, pove izrek D1 v dodatku. Sicer pa sta poljubni mrežni točki lahko krajišči ene od stranic kvadrata.



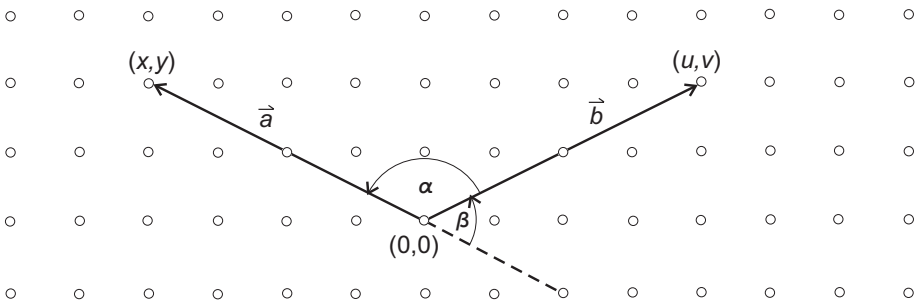
Slika 6. Dva mrežna kvadrata

Večkotniki

Poglejmo si, kako je s pravilnimi mrežnimi večkotniki pri $n > 4$. Potrebujemo trditev glede narave kosinusov notranjih ali zunanjih kotov.

Trditev 4. *V poljubnem mrežnem n-kotniku je kosinus vsakega notranjega in vsakega zunanjega kota z enako dolgima priležnima stranicama racionalen.*

Dokaz. Če je notranji kot α, je zunanji $\beta = \pi - \alpha$ in zato $\cos\beta = -\cos\alpha$, kosinus kota med enako dolgima vektorjema $\overrightarrow{a} = (x, y)$ in $\overrightarrow{b} = (u, v)$ s celimi koordinatami pa je $\cos\alpha = \overrightarrow{a} \cdot \overrightarrow{v} \,/\, |\overrightarrow{a}|\,|\overrightarrow{b}| = (xu + yv)/(x^2 + y^2) \in \mathbb{Q}$ (slika 7).



Slika 7. Kot med enako dolgima mrežnima vektorjema

Posledica 2. *Noben pravilni osemkotnik ni mrežni.*

Dokaz. Zunanji kot pri pravilnem osemkotniku je $2\pi/8 = \pi/4$, zato njegov kosinus $\cos(\pi/4) = \sqrt{2}/2$ ni racionalen.

Posledica 3. *Če je $n = 2^k$, $k \geq 3$, ni pravilnega mrežnega n-kotnika.*

Dokaz. Sledi iz prejšnje posledice in trditve 3.

Lema 1. *Naj bo $X = tg\theta$ in n liho celo število. Potem obstajajo cela števila c_n^i in d_n^i, tako da velja*

$$\operatorname{tg} n\theta = \frac{c_n^1 X - c_n^3 X^3 + ... + (-1)^{(n-1)/2} X^n}{1 - d_n^2 X^2 + ... + (-1)^{(n-1)/2} d_n^{n-1} X^{n-1}}.$$

Dokaz. V DeMoivreovi formuli $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$ uporabimo binomski obrazec, izenačimo realna in imaginarna dela na levi in desni strani enakosti, tako da izračunamo $\sin n\theta$ in $\cos n\theta$ kot polinoma v $\cos\theta$ in $\sin\theta$ ter nato $\operatorname{tg} n\theta$ kot racionalno funkcijo v $X = \operatorname{tg}\theta$. Koeficienti $c_n^i = \binom{n}{i}$ so lihi, koeficienti $d_n^i = \binom{n}{i}$ pa sodi binomski koeficienti.

Posledica 4. *Pravilni petkotnik in pravilni sedemkotnik nista mrežna večkotnika.*

Dokaz. Če je $\theta = 2\pi/5$, $\operatorname{tg}^2\theta$ in $\operatorname{tg}\theta$ nista racionalni števili. Res: ker je $\operatorname{tg} 5\theta = 0$, mora biti števec formule iz trditve enak 0, torej $X^5 - 10X^3 + 5X = 0$. Ker $X \neq 0$, iz bikvadratne enačbe $X^4 - 10X^2 + 5 = 0$ dobimo $X^2 = 5 \pm 2\sqrt{5} \notin \mathbb{Q}$. Potem tudi $X \notin \mathbb{Q}$.

Če je $\theta = 2\pi/7$, $\operatorname{tg}\theta$ ni racionalno število. Kot prej dobimo, da mora biti števec enak 0, torej $X^7 - 21X^5 + 35X^3 - 7X = 0$ oz. $X^6 - 21X^4 + 35X^2 - 7 = 0$ oz. $Y^3 - 21Y^2 + 35Y - 7 = 0$, odkoder spet takoj vidimo, da $Y = X^2$ in torej tudi X ni racionalno število.

Izrek 1. *Pravilen n-kotnik je lahko mrežni večkotnik, če in samo če je $n = 4$.*

Dokaz. Kako je v primeru $n = 3$ in $n = 4$ že vemo. Denimo, da je $n > 4$ in S mrežni n-kotnik.

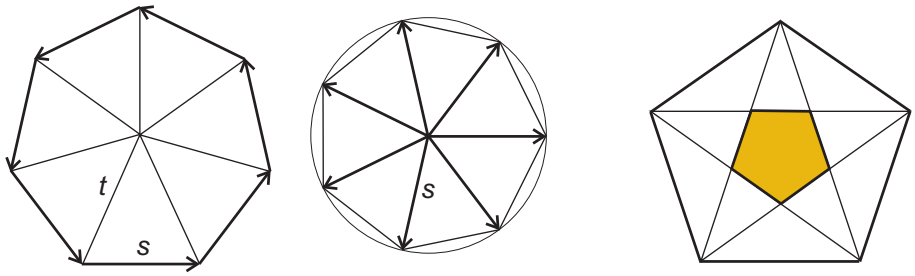
Če je n lih, mora biti $n \geq 9$, ker za $n = 5$ in $n = 7$ že vemo, da pravilnega mrežnega n-kotnika ni. Naj bo $\theta = 2\pi/n$ zunanji kot in $X = \operatorname{tg}\theta$. Ker je

$$0 = \operatorname{tg} n\theta = X(c_n^1 - c_n^3 X^2 + \ldots + (-1)^{(n-1)/2} X^{n-1}),$$

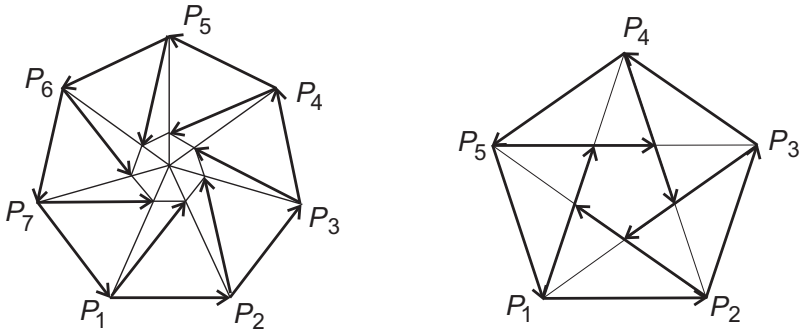
morajo biti racionalne rešitve te enačbe cele in morajo deliti koeficient c_n^1. Toda za $n \geq 9$ je $0 < \operatorname{tg}(2\pi/n) < \operatorname{tg}(\pi/4) = 1$ in racionalne rešitve ni.

Če je n sod, npr. $n = 2^r m$, kjer je $m > 1$ lih, bi obstajal v S pravilni mrežni m-kotnik, kar po prejšnjem ni mogoče. Ostane možnost $m = 1$ in $n = 2^r$, kjer je $r \geq 3$. Tedaj pa bi lahko našli v S pravilen mrežni osemkotnik, kar tudi vemo, da ni mogoče.

Preprost geometrijski dokaz izreka 1 za primer $n \geq 5$ in $n \neq 6$ (W. Scherrer [15]). Predpostavimo, da obstaja pravilen mrežni večkotnik in da je ta med vsemi najmanjši. Če je $n > 6$, je $2\pi/n < \pi/3$ in zato $t > s$ (slika 3). V tem primeru zamenjajmo t z s, tj. s premikom nanesimo zaporedne stranice pravilnega n-kotnika iz izhodišča, pa dobimo manjši pravilni mrežni večkotnik (glej sliko 8). V primeru $n = 5$ ravnamo drugače: hitro vidimo, da so vsa presečišča diagonal pravilnega petkotnika spet mrežne točke, ki tvorijo nov manjši pravilni petkotnik (glej petkotnik na sliki 8).



Slika 8. Geometrijski dokaz, da mrežni n-kotnik za $n > 6$ in za $n = 5$ ni možen



Slika 9. Alternativni geometrijski dokaz, da mrežni n-kotnik za $n \geq 5$ in $n \neq 6$ ni možen

Alternativni dokaz (premik vsakega oglišča P_i za vektor $P_{i+1}P_{i+2}$, ko ponovno najdemo manjši pravilni n-kotnik) deluje za vse $n \geq 5$, razen za $n = 6$, ko vsa premaknjena oglišča sovpadajo (glej zadnji petkotnik na sliki 9).

2. Polpravilni večkotniki na ravninski mreži

Poglejmo, koliko se zadeva spremeni, če namesto pravilnih opazujemo samo polpravilne semiregularne mrežne večkotnike. Spomnimo se, da je polpravilni (semiregularni) tak večkotnik, ki je bodisi enakostranični bodisi enakokotni.

Enakostranični mrežni večkotniki

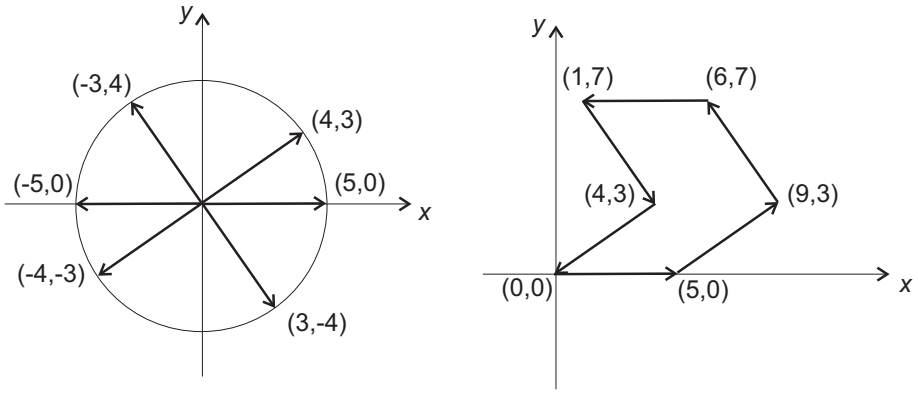
Trditev 5 (D.G. Ball [2]). *Če je n liho število, ne obstaja enakostranični mrežni n-kotnik.*

Dokaz. Denimo, da taki n-kotniki obstajajo. Med njimi izberimo minimalnega. Na zaporednih stranicah konstruirajmo vektorje $\vec{v}_1 = (x_1, y_1)$, $\vec{v}_2 = (x_2, y_2)$, ..., $\vec{v}_n = (x_n, y_n)$, tako da je $\vec{v}_1 + \vec{v}_2 + ... + \vec{v}_n = 0$ in torej tudi $x_1 + x_2 + ... + x_n = 0$ ter $y_1 + y_2 + ... + y_n = 0$. Ker so vse stranice enake, npr. s, je $x_1^2 + y_1^2 = x_2^2 + y_2^2 = ... = x_n^2 + y_n^2 = s^2 \in \mathbb{N}$. Potem imamo $0 = (x_1 + x_2 + ... + x_n)^2 + (y_1 + y_2 + ... + y_n)^2 = (x_1^2 + y_1^2) + (x_2^2 + y_2^2) + ... + (x_n^2 + y_n^2) + 2(x_1x_2 + x_1x_3 + ... + x_{n-1}x_n + y_1y_2 + y_1y_3 + ... + y_{n-1}y_n) = ns^2 + 2t$, kjer je $t = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n + y_1y_2 + y_1y_3 + ... + y_{n-1}y_n$ očitno sodo število. Torej je $ns^2 = -2t$. Ker je n liho število, je s^2 sodo število, deljivo s 4; torej sta zaradi enakosti $x_i^2 + y_i^2 = s^2$ za vsak i koordinati x_i in y_i obe sodi. To pa je v nasprotju z minimalnostjo n-kotnika.

Posledica 5. *Če ima n lihi delitelj, ni pravilnega mrežnega n-kotnika.*

Dokaz. Sledi iz trditev 3 in 5.

Izrek 2 (D. Hoffman, glej [6]). *Enakostranični mrežni n-kotnik obstaja natanko takrat, ko je n sodo število.*



Slika 10. Sestavljanje enakostraničnega večkotnika: $n = 6$, $k = 3$

Dokaz. Za lihi n enakostraničnega mrežnega trikotnika ni po trditvi 5. Naj bo zdaj n sodo število, npr. $n = 2k$. Iz teorije števil je znano, da je število (urejenih) celih rešitev (x, y) enačbe $x^2 + y^2 = m$ ($m \in \mathbb{N}$) enako $4(d_1 - d_3)$, kjer je d_1 število lihih deliteljev za m oblike $4j + 1$ in d_3 število lihih deliteljev za m oblike $4j + 3$ (glej izrek D2 v dodatku). Če je npr. $m = 5^{k-1}$, $k \in \mathbb{N}$, so delitelji $5^0, 5^1, 5^2, ..., 5^{k-1}$ vsi oblike $4j + 1$, tako da je $d_1 = k$ in $d_3 = 0$. Torej je število celih rešitev enačbe $x^2 + y^2 = 5^{k-1}$ enako $4k = 2n$. Ker je

poleg (x, y), rešitev tudi $(-x, -y)$, nastopajo rešitve v $n = 2k$ parih. Izberimo k teh parov, se pravi $n = 2k$ rešitev (x, y). Vektorje od izhodišča do celoštevilskih točk (x, y) zložimo zapored v sklenjeno pot (ker je vsota vektorjev enaka 0) in dobimo (ne nujno konveksen in enostaven) večkotnik; to lahko storimo celo na različne načine (glej sliko 10). Konveksen enostaven n-kotnik dobimo le v primeru, ko vektorje izbiramo po velikosti njihovega naklona.

Enakokotni mrežni večkotniki

Izrek 3 (D. Hoffman, glej [6]). *Enakokotni mrežni n-kotnik obstaja natanko takrat, ko je $n = 4$ ali $n = 8$.*

Dokaz. Tudi pri enakokotnem večkotniku je tangens zunanjega kota θ racionalno število. Zaradi $n\theta = 2k\pi$ (k-kratnik polnega kota), je $\theta = 2k\pi/n$. Naj bo $a = e^{i\theta} = e^{2\pi ki/n}$, eden od n-tih korenov enote. Potem a in $1/a$ oba zadoščata ciklotomski enačbi $x^n - 1 = 0$ in sta zato *celi algebraični števili*. Ker tvorijo ta števila kolobar, je tudi $a + 1/a$ celo algebraično število (neodvisen dokaz, ki uporablja polinome Čebiševa, glej spodaj). Povsem enako spoznamo, da je $a^2 + 1/a^2$ celo algebraično število, zato velja isto tudi za število $t = 4\cos^2\theta = (a + 1/a)^2 = a^2 + 1/a^2 + 2$. Toda hkrati je $t = 4/(1 + \mathrm{tg}^2\theta) \in \mathbb{Q}$, zato je t kar (običajno) celo število. Ker pa je $\cos^2\theta \leq 1$, je možno le $t = 0, 1, 2, 3, 4$. Preverimo vsak primer posebej in ugotovimo, da je tangens racionalen samo pri $\theta = \pi/2$ ali $\theta = \pi/4$. Vsak od teh dveh primerov pa se da realizirati, dokaz je končan.

Opomba. *Če je $a^n = 1$, je $a+1/a$ celo algebraično število.* Dokaz z uporabo polinomov Čebiševa, ki so definirani rekurzivno: $f_0(x) = 2$, $f_1(x) = x$ in $f_r(x) = xf_{r-1}(x) - f_{r-2}(x)$ za $r < 1$, poteka takole. Z indukcjo z lahkoto pokažemo, da je f_r polinom stopnje r s celimi koeficienti in vodilnim koeficientom 1 in da za vsak r velja $f_r(a+1/a) = a^r + 1/a^r$. Ker je $a^n = 1$, je $f_n(a+1/a) = 2$. Torej zadošča število $a+1/a$ polinomski enačbi $f_n(x) - 2 = 0$, ki ima cele koeficiente in vodilni koeficient 1, tako da je $a + 1/a$ celo algebraično število.

3. Pravilni večkotniki na prostorski mreži

Celoštevilska mreža $\mathbb{Z}^k$ v k-razsežnem prostoru $\mathbb{R}^k$ je množica celoštevilskih k-teric. Pojmi, kot so mrežna daljica, mrežni kot, mrežni večkotnik, so definirani podobno kot v ravnini. Pravilni mrežni večkotnik, je ravninski lik S, katerega oglišča pripadajo prostorski mreži $\mathbb{Z}^k$. Tudi za tak večkotnik lahko govorimo o notranjih in zunanjih kotih.

Trditev 6. *Kosinus notranjega ali zunanjega kota poljubnega enakostraničnega mrežnega večkotnika je racionalno število.*

Dokaz. Kosinus kota med enako dolgima vektorjema $\vec{a} = (x_1, ..., x_k)$ in $\vec{b} = (y_1, ..., y_k)$ je enak $\cos\alpha = -\cos\beta = \dfrac{\vec{a} \cdot \vec{b}}{|\vec{a}||\vec{b}|} = \dfrac{x_1y_1 + ... + x_ky_k}{x_1^2 + ... + x_k^2}$.

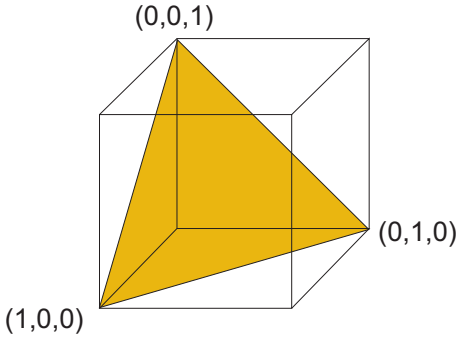
Posledica 6. *Pravilni osemkotnik in pravilni dvanajstkotnik nista mrežna večkotnika v $\mathbb{R}^k$, $k \geq 2$.*

Dokaz. Zunanji kot je pri osemkotniku enak $2\pi/8 = \pi/4$ in zato $\cos\beta = \sqrt{2}/2$, pri dvanajstkotniku pa $2\pi/12 = \pi/6$ in zato $\cos\beta = \sqrt{3}/2$; obakrat $\cos\beta \notin \mathbb{Q}$.

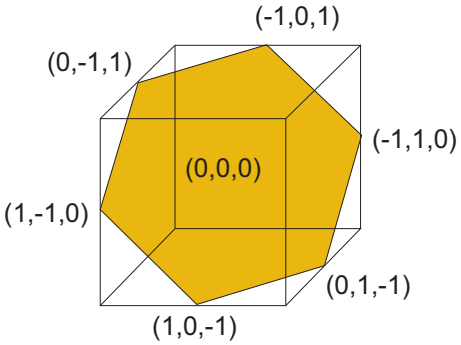
Posledica 7. *Kvadrat tangensa notranjega ali zunanjega kota poljubnega pravilnega mrežnega večkotnika je racionalen.*

Dokaz. Po trditvi 6 je $\cos\theta$ racionalen, zato velja isto za njegov kvadrat $\cos^2\theta$; se pravi tudi za $\sin^2\theta$ in za $\mathrm{tg}^2\theta$.

Vsak večkotnik, ki je mrežni v prostoru $\mathbb{R}^k$ je mrežni tudi v $\mathbb{R}^m$ za $m \geq k$. Poleg kvadrata, ki je mrežni večkotnik v $\mathbb{R}^2$ in zato tudi v večrazsežnih prostorih, so v $\mathbb{R}^3$ mrežni še drugi večkotniki. Npr. *enakostranični trikotnik* z oglišči (1,0,0), (0,1,0) in (0,0,1) v ravnini $x + y + z = 1$ (glej sliko 11) in *pravilni šestkotnik* z oglišči $(1, 0, -1), (0, 1, -1)$, $(-1, 1, 0), (-1, 0, 1)$, $(0, -1, 1)$ in $(1, -1, 0)$ v ravnini $x + y + z = 0$ (glej sliko 12) .



Slika 11. Enakostranični trikotnik na prostorski mreži



Slika 12. Pravilni šestkotnik na prostorski mreži

Izrek 4. *Pravilen n-kotnik je mrežni večkotnik v prostoru $\mathbb{R}^k$ za $k \geq 2$ natanko takrat, ko je $n = 3, 4$ ali 6.*

Dokaz. Naj bo najprej n liho število. Ker je zunanji kot $\theta = 2\pi/n$, je $\mathrm{tg}\, n\theta = 0$; zato $X = \mathrm{tg}\,\theta$ zadošča enačbi

$$0 = c_n^1 X - c_n^3 X^3 + \ldots + (-1)^{(n-1)/2} X^n,$$

kjer je $c_n = \binom{n}{i}$, njegov kvadrat $Y = X^2 = \mathrm{tg}^2\theta$ pa enačbi

$$0 = n - c_n^3 Y + \ldots + (-1)^{(n-1)/2} Y^{(n-1)/2}.$$

Racionalne rešitve so cela števila, ki delijo n, toda za $n \geq 9$ je $Y = \mathrm{tg}^2(2\pi/n) < \mathrm{tg}^2(\pi/4) = 1$, zato zadošča preveriti samo primera $n = 5$ in $n = 7$. Za ta dva pa smo že videli, da $\mathrm{tg}^2(2\pi/5)$ in $\mathrm{tg}^2(2\pi/7)$ nista racionalni števili (posledica 4).

Če je n sodo število, različno od 4 ali 6, pišimo $n = 2^r m$, kjer je r naravno in m liho število. Ker pravilni osemkotnik ni mrežni, število n ne more biti večkratnik števila 8. Torej mora biti $r < 3$ in (zaradi predpostavke $n \neq 4$) $m > 1$. Ker lihi m po prvem delu dokaza ne more biti večji ali enak 9, niti 5 niti 7, mora biti $m = 3$. Ker pa smo vzeli $n \neq 6$, mora biti $r \neq 1$, torej $r = 2$. Toda v tem primeru bi bil $n = 12$, kar smo tudi videli, da ni

mogoče.

Opomba. Podobno kot pri ravninski mreži se tudi zdaj pojavi vprašanje ali sta poljubni dve mrežni točki v $\mathbb{R}^3$ lahko oglišči pravilnega mrežnega trikotnika, kvadrata ali šestkotnika. Preprost premislek pove, da niti za kvadrat to ni več mogoče. Točki $(0,0,0)$ in $(1,1,1)$ npr. nista na isti stranici, sta pa na isti diagonali mrežnega kvadrata. Točki $(0,0,0)$ in $(1,1,2)$ tudi nista na isti stranici. Ali sta lahko na isti diagonali? Problem se v vsakem primeru prevede na reševanje kvadratičnega sistema diofantskih enačb, včasih na vprašanje ali leži na dani racionalni stožnici (elipsi) kakšna racionalna točka (glej [5]).

Alternativni dokazi

Zgornji izrek lahko dokažemo še drugače, če uporabimo naslednji rezultat, v katerem nastopa Eulerjeva funkcija ϕ ($\phi(n)$ je število naravnih števil $k \leq n$, ki so tuja proti n).

Lema 2 (D.H. Lehmer, glej [8]). *Za vsak $n > 2$ je $2\cos(2\pi/n)$ celo algebraično število stopnje $\phi(n)/2$.*

Dokaz. Od prej vemo, da je $2\cos(2\pi/n) = a + 1/a$, $a = e^{2\pi i/n}$ celo algebraično število. Toda zdaj je a primitivni n-ti koren enote, takih je ravno $\phi(n)$, in zadoščajo nad $\mathbb{Q}$ nerazcepnemu polinomu f_n s celimi koeficienti in vodilnim koeficientom 1, definiranemu s predpisom

$$f_n(x) = \Pi_{k=1,(k,n)=1}^{n-1}(x - e^{2\pi ki/n}).$$

Npr.: $f_3(x) = (x-e^{2\pi i/3})(x-e^{4\pi i/3}) = x^2+x+1$, $f_4(x) = (x-e^{2\pi i/4})(x-e^{6\pi i/4}) = x^2+1$, $f_5(x) = (x-e^{2\pi i/5})(x-e^{4\pi i/5})(x-e^{6\pi i/5})\ (x-e^{8\pi i/5}) = x^4+x^3+x^2+x+1$ itd. Torej je a celo algebraično število stopnje $\phi(n)$.

Razcep na prafaktorje $n = p_1p_2...p_k$ in multiplikativnost Eulerjeve funkcije ϕ pove, da je $\phi(n) = 2m$, se pravi sodo število. Kot je znano, je potem $x^{-m}f_n(x) = p_n(x+1/x)$, kjer je p_n nad $\mathbb{Q}$ nerazcepen polinom stopnje m s celoštevilskimi koeficienti in vodilnim koeficientom 1, npr. $x^{-1}f_3(x) = x+1+1/x = (x+1/x)+1 = p_3(x+1/x)$, kjer je $p_3(t) = t+1$, $x^{-1}f_4(x) = x+1/x = p_4(x+1/x)$, $p_4(t) = t$, ali $x^{-2}f_5(x) = x^2+x+1+1/x+1/x^2 = (x+1/x)^2+(x+1/x)-1 = p_5(x+1/x)$, $p_5(t) = t^2+t-1$. Ker je $a = e^{2\pi i/n}$ ničla polinoma f_n, je potem $a + 1/a = 2\cos(2\pi/n)$ ničla za p_n, torej celo algebraično število stopnje $m = \phi(n)/2$.

Alternativni dokaz izreka 4 [14]. Iz kosinusovega izreka za zaporedni stranici s pravilnega mrežnega n-kotnika in bližnjo diagonalo d, tj. iz enačbe $d^2 = 2s^2 + 2s^2\cos(2\pi/n)$ vidimo, da mora biti $2\cos(2\pi/n)$ racionalno število. Ker je po lemi 2 hkrati celo algebraično število stopnje $\phi(n)/2$, je celo število in zato $\phi(n) = 2$. To pa je možno samo, če je število n enako 3,4 ali 6. Vsi ti trije primeri se dajo realizirati na prostorski mreži v $\mathbb{R}^3$.

Alternativni dokaz izreka 3 [14]. Podobno kot zgoraj iz $d^2 = s_1^2 + s_2^2 + 2s_1s_2\cos(2\pi/n)$ vidimo, da mora biti zdaj $2\cos(2\pi/n)$ algebraično število oblike $r/\sqrt{t}$, kjer sta r in t celi števili. Ker zadošča polinomski enačbi $x^2 - r^2/t = 0$ za racionalnimi koeficienti, je stopnje največ 2 in je zato $\phi(n) \leq 4$ po lemi 2, se pravi, da je lahko le $n = 3,4,5,6,8,10$ ali 12. S pregledom vseh možnosti ugotovimo, da je $\mathrm{tg}(2\pi/n)$ racionalen le za $n = 4$ ali $n = 8$.

Alternativni dokaz izreka 1. Pravilni mrežni n-kotnik je enakostranični mrežni n-kotnik, kar je po trditvi 5 in njeni posledici 5 možno samo v primeru $n = 2^k$, $k \in \mathbb{N}$. Toda za $k \geq 3$ to preprečuje posledica 3, zato preostane samo še primer $n = 4$, ko pa res obstaja veliko mrežnih kvadratov.

Še en alternativni dokaz izreka 1 najdemo v [7] in poteka takole:

Ker se da vsak mrežni večkotnik triangulirati z mrežnimi trikotniki, ima racionalno ploščino. Za pravilni n-kotnik s stranico s je ploščina enaka

$$A = n(s/2)^2/\mathrm{tg}(\pi/n).$$

Če pokažemo, da je $\mathrm{tg}(\pi/n)$ racionalno število samo v primeru $n = 4$, je dokaz končan.

Lema 3. *Za $n \geq 3$ in $n \neq 4$ je $tg(\pi/n)$ iracionalno število.*

Dokaz. Z uporabo formule za tangens vsote dveh kotov je očitno, da racionalnost za $\mathrm{tg}\,\theta$ implicira racionalnost za $\mathrm{tg}\,m\theta$. Ker je npr. $\mathrm{tg}(\pi/3) = \sqrt{3}$ iracionalno število, je tako tudi število $\mathrm{tg}(\pi/m)$, $m = 3k$, za poljuben $k \in \mathbb{N}$. Od tod sledi, da zadošča dokazati iracionalnost $\mathrm{tg}(\pi/n)$ samo v primeru, ko je n liho praštevilo (saj je tudi $\mathrm{tg}(\pi/8) = \sqrt{2}-1$ iracionalno število).

Naj bo torej $p > 3$ liho praštevilo in $\mathrm{tg}(\pi/p) = a/b$, kjer sta a in b tuji si naravni števili. Zaradi $\mathrm{tg}(\pi/p) \leq \mathrm{tg}(\pi/5) < \mathrm{tg}(\pi/4) = 1$, je $a < b$. Poleg tega je

$$\sin(\pi/p) = a/\sqrt{a^2+b^2} \quad \text{in} \quad \cos(\pi/p) = b/\sqrt{a^2+b^2},$$

tako da sta $\sin(2\pi/p) = 2ab/(a^2+b^2)$ in $\cos(2\pi/p) = (b^2-a^2)/(a^2+b^2)$ racionalni števili. Iz $(\cos(2\pi/p) + i\sin(2\pi/p))^p = 1$ vidimo, da velja $(b^2 - a^2 + 2abi)^p = (a^2+b^2)^p$. Naravno število $2ab$ torej zadošča enačbi

$$(b^2 - a^2 + xi)^p = (a^2+b^2)^p$$

oziroma (s primerjanjem imaginarnih delov in krajšanjem z x) polinomski enačbi

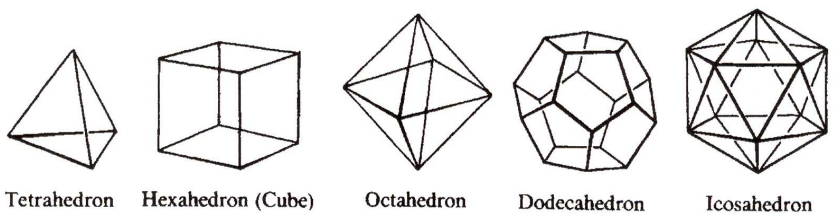
$$x^{p-1} - \binom{p}{p-2}(b^2-a^2)^2x^{p-3} + ... \pm \binom{p}{3}(b^2-a^2)^{p-3}x^2 \mp \binom{p}{1}(b^2-a^2)^{p-1} = 0.$$

To pomeni, da mora $2ab$, torej tudi b, deliti konstantni člen $p(b^2-a^2)^{p-1}$. Zaradi $\mathrm{tg}(\pi/p) > \pi/p > 1/p$ je $ap > b$. Če bi bil $a = 1$, bi od tod sklepali $b < p$. Noben faktor v takem b ne more deliti p, zato bi moral v tem primeru b deliti $(b^2-1)^{p-1} = (b-1)^{p-1}(b+1)^{p-1}$; kar pa spet ne gre, ker je b tuj tako z $b-1$ kot z $b+1$. Primer $a = 1$ trej ni možen, zato imamo situacijo $b > a > 1$. Naj bo q poljuben prafaktor v a ali b. Ker ne more deliti $(b^2-a^2)^{p-1}$ (saj deli samo a^2 ali b^2, ne pa oba), niti ne more deliti praštevila p, dobimo protislovje.

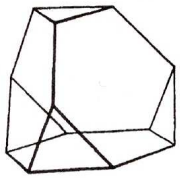
4. Pravilni mrežni poliedri

Sama po sebi se ponuja posplošitev ravninskega problema mrežnih večkotnikov v $\mathbb{R}^2$ ali $\mathbb{R}^3$ na prostorski problem mrežnih poliedrov v $\mathbb{R}^3$: Katera pravilna (regularna) telesa so mrežna? Katera polpravilna (semi regularna) so taka?

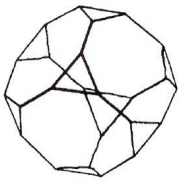
Kot je znano je pravilnih poliedrov pet. Za vse stranske ploskve imajo kongruentne pravilne večkotnike, v vsakem oglišču se jih stika enako število, kar povemo z nizom enakih k števil $(n, n, ..., n)$ (k pomeni koliko prvilnih n-kotnikov se stika v oglišču. To so t.i. platonska telesa: kocka (4,4,4), tetraeder (3,3,3), oktaeder (3,3,3,3), dodekaeder (5,5,5) in ikozaeder (3,3,3,3,3) (glej sliko 13).



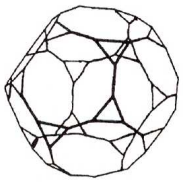
Slika 13. Platonska telesa



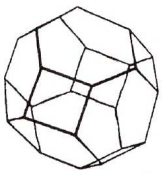
(1) Truncated Tetrahedron (3, 6, 6)



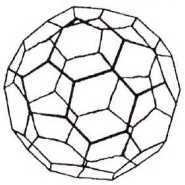
(2) Truncated Cube (3, 8, 8)



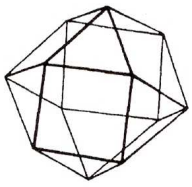
(3) Truncated dodecahedron (3, 10, 10)



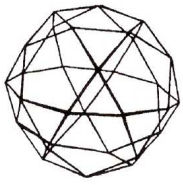
(4) Truncated Octahedron (4, 6, 6)



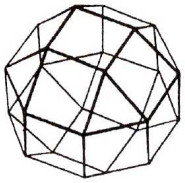
(5) Truncated Icosahedron (5, 6, 6)



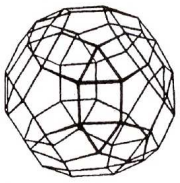
(6) Cubotahedron (3, 4, 3, 4)



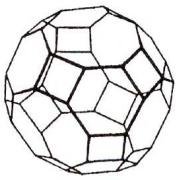
(7) Icosidodecahedron (3, 5, 3, 5)



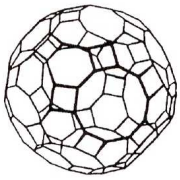
(8) Rhombicuboctahedron (3, 4, 4, 4)



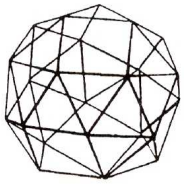
(9) Rhombicosidodecahedron (4, 3, 4, 5)



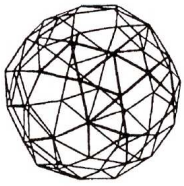
(10) Great Rhombicuboctahedron (4, 6, 8)



(11) Great Rhombicosidodecahedron (4, 6, 6)



(12) Snub Cube (3, 3, 3, 3, 4)



(13) Snub Dodecahedron (3, 3, 3, 3, 5)

SLIKA 14. Arhimedska telesa

Polpravilnih ali *semiregularnih* teles, pri katerih se v oglišču stikajo različni pravilni večkotniki, tako da v zaporedju števila niso enaka, pa je trinajst.

To so t.i. *arhimedska telesa* (glej sliko 14):

prisekani četverec (tetraeder) (3,6,6),
prisekana kocka (3,8,8),
prisekani dvanajsterec (dodekaeder) (3,10,10),
prisekani osmerec (oktaeder) (4,6,6),
prisekani dvajseterec (ikozaeder) (5,6,6),
kockin osmerec (kuboktaeder) (3,4,3,4),
dvajseterčev dvanajsterec (ikozidodekaeder) (3,5,3,5),
okrnjeni kockin osmerec (rombikuboktaeder) (3,4,4,4),
okrnjeni dvajseterčev dvanajsterec (rombikozidodekaeder) (4,3,4,5),
prisekani kockin osmerec (great rombikuboktaeder) (4,6,8),
prisekani dvajseterčev dvanajsterec (great rombikozidodekaeder) (4,6,10),
prirezana kocka (snub cube) (3,3,3,3,4),
prirezani dvanajsterec (snub dodekaeder) (3,3,3,3,5) .

Izrek 5 (E. Ehrhart [4]). *Od petih platonskih teles so mrežni poliedri le kocka, tetraeder in oktaeder.*

Dokaz. Dodekaeder ne more biti mrežni, ker se pravilni petkotnik ne da realizirati v prostorski mreži (izrek 4). Iz istega razloga tudi ikozaeder ne more biti mrežni. Če si namreč ogledamo venec petih enakostraničnih trikotnikov, ki se stikajo v enem oglišču ikozaedra, tvorijo preostala oglišča teh trikotnikov pravilni mrežni petkotnik.

Da se kocka, tetraeder in oktaeder da realizirati na prostorski mreži je jasno: kocka ima npr. oglišča (0,0,0), (1,0,0), (0,1,0), (1,1,0), (0,0,1), (1,0,1), (0,1,1) in (1,1,1), tetraeder (0,0,0), (1,1,0), (1,0,1) in (0,1,1), oktaeder pa npr. $(1,0,0), (0,1,0), (-1,0,0)$, $(0,-1,0)$, $(0,0,1)$ in $(0,0,-1)$.

Izrek 6 (P.R. Scott [14]). *Od trinajstih arhimedskih teles so mrežni poledri le prisekani tetraeder, prisekani oktaeder in kuboktaeder.*

Dokaz. Ker morajo biti stranske ploskve pravilni mrežni večkotniki, pridejo zaradi izreka 4 v poštev le tisti poliedri, ki imajo za stranske ploskve trikotnik, kvadrat ali pravilni šestkotnik, torej prisekani tetraeder (3,6,6), prisekani oktaeder (4,6,6), kuboktaeder (3,4,3,4), rombikuboktaeder (3,4,4,4) in snub kocka (3,3,3,3,4). Rombikuboktaeder hitro izločimo, ker oglišča na robu pasu kvadratov tvorjo pravilni osemkotnik, ki ne more biti mrežni (izrek 4); da snub kocka ni mrežni poleder, pa je dokazano v [14].

Ostali trije semiregularni poliedri se dajo realizirati na mreži: prisekani tetraeder nastane s tretinjenjem stranskih robov tetraedera, zato lahko za oglišča osnovnega (neprisekanega) tetraedra izberemo točke (0,0,0), (3,3,0), (3,0,3) in (0,0,3). Podobno je pri prisekanemu oktaedru. Oglišča kuboktaedra pa so razpolovišča stranskih robov kocke (ki jih spet brez težav izberemo tako, da so celoštevilska).

5. Dodatek: Predstavitev naravnega števila v obliki vsote dveh kvadratov

Znano je, da so liha praštevila bodisi oblike $4m+1$ bodisi oblike $4m+3$. Obojih je neskončno mnogo, kar je posledica netrivialnega Dirichletovega izreka: *Če sta a in b tuji si naravni števili, je v aritmetičnem zapredju $am+b$ neskončno mnogo praštevil.* Res pa je, da je števil oblike $4m+3$ v nekem smislu več kot praštevil oblike $4m+1$, čemur rečejo *pristranost Čebiševa* (glej [1] in [10]).

Da je praštevil oblike $4m+3$ neskončno mnogo se lahko takoj prepričamo neposredno z uporabo Evklidovega argumenta glede neskončno mnogo praštevil: če jih je samo končno mnogo, naj bo p_k največje praštevilo te sorte. Potem je število $N_k = 2^2 \cdot 3 \cdot 5 \cdot ... \cdot p_k - 1$ oblike $4m+3$ in mora zato imeti v svojem praštevilskem razcepu vsaj en prafaktor p oblike $4m+3$. Le-ta pa je gotovo večji od p_k, protislovje. Da je tudi praštevil oblike $4m+1$ neskončno mnogo, bomo videli potem, ko bomo dokazali izrek D1.

Naslednja trditev je znana v zvezi s kvadratnim recipročnostnim zakonom (glej npr. [16], str. 185).

Trditev D1. *Kongruenca* $x^2 \equiv -1 \pmod{p}$ *je rešljiva za* $p = 2$ *in za liha praštevila oblike* $p = 4m+1$*, ne pa za liha praštevila oblike* $p = 4m+3$.

Dokaz ([1], Chapter 4). Za $p = 2$ je rešitev $x = 1$. Naj bo p liho praštevilo. Množico $\{1, 2, ..., p-1\}$ obrnljivih ostankov po modulu p razdelimo na ekvivalenčne razrede z enačenjem elementov z njihovimi nasprotnimi in inverznimi elementi. Razredi so torej oblike $\{x, -x, x^{-1}, -x^{-1}\}$ in imajo štiri elemente, razen če je $x = -x$, $x = x^{-1}$ ali $x = -x^{-1}$, vse po modulu p. Toda $x = -x$ pri lihem p ni mogoče. Enačba $x = x^{-1}$ je ista kot $x^2 = 1$, ki ima (v obsegu $\mathbb{Z}_p$) natanko dve rešitvi $x = 1$ in $x = p-1$. Torej je v tem primeru ekvivalenčni razred, v katerem je 1 enak $\{1, p-1\}$. Enačba $x = -x^{-1}$ oziroma $x^2 = -1$ pa ima v $\mathbb{Z}_p$ natanko dve rešitvi, npr. x_0 in $p - x_0$ ali pa nobene. Ekvivalenčni razredi so torej četvorke, par $\{1, p-1\}$ ter poleg tega kvečjemu še en dodatni par $\{x_0, p - x_0\}$, kjer je x_0 eden izmed ostankov $2, 3, ..., p-1$. Če je $p - 1 = 4m+2$ tega dodatnega para ni in kongruenca $x^2 \equiv -1 \pmod{p}$ ni rešljiva. Če pa je $p - 1 = 4m$, mora biti poleg para $\{1, p-1\}$ še dodatni par; kongruenca $x^2 \equiv -1 \pmod{p}$ je tedaj rešljiva.

Npr. kongruenca $x^2 \equiv -1 \pmod{2}$ ima rešitev $x = 1$, kongruenca $x^2 \equiv -1 \pmod{5}$ ima rešitev $x = 2$, kongruenca $x^2 \equiv -1 \pmod{3}$ pa je nerešljiva.

Rečemo, da je naravno število n *vsota dveh kvadratov*, Če ga lahko zapišemo v obliki $n = x^2 + y^2$, kjer sta x, y (nenegativni) celi števili. Tako je npr. $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$ itd. Opazimo, da števila 3, 6 ali 7 niso vsote dveh kvadratov. Liha števila oblike $p = 4m+3$ niso vsota dveh kvadratov, ker je $x^2 + y^2$ lahko le sodo število ali liho število oblike $4m+1$. Zano pa je (glej npr. [16], str. 187), da je vsako praštevilo oblike $p = 4m+1$ dejansko vsota dveh kvadratov, kar je nekoliko težje videti. Naslednji preprost dokaz je vzet iz [1], Chapter 4.

Trditev D2. *Vsako praštevilo oblike* $p = 4m+1$ *je vsota kvadratov dveh naravnih števil.*

Dokaz. Naj bo $S = \{(x, y, z) \in \mathbb{N}^3;\ x^2 + 4yz = p\}$. Ker je pri pogoju $x^2 + 4yz = p$ vsaka komponenta x, y ali z naravno število, manjše od p, je množica S končna. Ravnini $x = y - z$ in $x = 2y$ množice S ne sekata (kot se hitro vidi iz ustreznih enačb), ampak jo razdelita na tri disjunktne podmnožice in sicer $S = S_1 \cup S_2 \cup S_3$, kjer je: $S_1 = \{(x, y, z) \in S;\ x < y - z\}$,
$S_2 = \{(x, y, z) \in S;\ y - z < x < 2y\}$,
$S_3 = \{(x, y, z) \in S;\ 2y < x\}$.
Definirajmo zdaj preslikavo $f:\ S \to S$, kjer je:

$$f(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & , \quad (x,y,z) \in S_1 \\ (2y-x, y, x-y+z) & , \quad (x,y,z) \in S_2 \\ (x-2y, x-y+z, y) & , \quad (x,y,z) \in S_3 \end{cases}$$

Hitro vidimo, da je $f(f(x, y, z)) = (x, y, z)$; torej je preslikava f sama sebi inverz in zato bijekcija. Če je $(x, y, z) \in S_1$, je $f(x, y, z) \in S_3$, in obratno, če je $(x, y, z) \in S_3$, je $f(x, y, z) \in S_1$, tako da preslikava f zamenjuje med seboj podmnožici S_1 in S_3.

Vse negibne točke za f morajo potemtakem ležati v podmnožici S_2. Dobimo jih iz enakosti $f(x,y,z) = (x,y,z)$ oziroma $(2y-x, y, x-y+z) = (x,y,z)$; odtod najdemo pogoj $y = x$. Edina točka iz S_2 s to lastnostjo pa zadošča enačbi $x^2 + 4xz = p$ ki iam v naravnih številih edino rešitev $x = 1$ in $z = (p-1)/4$. Edina negibna točka preslikave f je torej točka $(1, 1, (p-1)/4)$, druge točke pa preslikava f premakne. Zato je $|S_1| = |S_3|$ in $|S_2|$ liho število. Torej je tudi $|S|$ liho število.

Definirajmo zdaj še preprosto preslikavo $g: S \to S$ s predpisom $g(x,y,z) = (x,z,y)$, ki samo zamenaj zadnji komponenti in je zato tudi sama sebi inverz. Ker je $|S|$ liho število, mora imet g vsaj eno negibno točko $(x,y,y) \in S$. Toda to pomeni, da je $p = x^2 + 4y^2 = x^2 + (2y)^2$, kjer sta $x, y \in \mathbb{N}$.

Opomba. Zgornji dokaz pove malo več: število reprezentacij praštevila p v obliki $p = x^2 + (2y)^2$ je liho za vsa praštevila oblike $p = 4m + 1$. V resnici se da pokazati, da je reprezentacija ena sam (glej [9]). Obravnavani dokaz je kajpak nekonstruktiven: ni videti, kako bi tako reprezentacijo v resnici našli.

Izrek D1. *Naravno število n je vsota dveh kvadratov natanko takrat, ko vsak prafaktor oblike $p = 4m + 3$ nastopa v praštevilskem razcepu števila n le na sodo potenco.*

Dokaz ([1], str. 20). Zadostnost sledi (induktivno) iz ugotovitev:
(1) $2 = 1^2 + 1^2$, praštevilo oblike $p = 4m + 1$ je vsota dveh kvadratov.
(2) Če je $m = x^2 + y^2$ in $n = u^2 + v^2$, je $mn = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (yu - xv)^2$.
(3) Če je $n = x^2 + y^2$, je $nz^2 = (xz)^2 + (yz)^2$.
Potrebnost pa iz naslednjega dejstva:
(4) Če praštevilo p deli $n = x^2 + y^2$ in ne deli x obstajata celi števili a in b, da je $ap + bx = 1$, in zato $b^2 n = (bx)^2 + (by)^2 = (1 - ap)^2 + (by)^2$, tako da je -1 kvadrat po praštevilskem modulu p, kar je po trditvi D1 mogoče le v primeru, ko je p oblike $p = 4m + 1$.

Če je torej $n = x^2 + y^2$ in $p = 4m + 3$ praštevilo, ki deli n, potem p deli x in p deli y, tako da p^2 deli n in je $n/p^2 = u^2 + v^2$ (vsota dveh kvadratov). Tako praštevilo p lahko nastopa le na sodo potenco.

Pokažimo zdaj, da je tudi praštevil oblike $p = 4m + 1$ neskončno mnogo. V ta namen naj bo spet p_k največje tovrstno praštevilo in $N_k = (3 \cdot 5 \cdot .... \cdot p_k)^2 + 2^2$. To število je očitno oblike $4m + 1$, vsak njegov prafaktor je večji od p_k, nobeden pa po točki (4) zadnjega dokaza ni oblike $4m + 3$. Protislovje!

Vprašajmo se še, koliko urejenih predstavitev v obliki vsote dveh kvadratov ima dano naravno število n, se pravi, koliko je pri danem n takih urejenih parov (x,y) celih števil, da velja $n = x^2 + y^2$. Popoln odgovor na to vprašanje bo dal naslednji izrek. Še prej pa nekaj oznak: število iskanih reprezentacij označimo z $r_2(n)$ (standardna oznaka); naj bo $d(n)$ število pozitivnih deliteljev števila n, nadalje naj bo $d_1(n)$ število pozitivnih deliteljev oblike $4m + 1$ in $d_3(n)$ število pozitivnih deliteljev oblike $4m + 3$.

Izrek D2. *Zapišimo naravno število n v obliki $n = 2^c n_1 n_3$, kjer je faktor n_1 sestavljen samo iz praštevil oblike $4m + 1$ in n_3 iz praštevil oblike $4m + 3$. Potem velja je $r_2(n) = 0$, če n_3 ni kvadrat celega števila (tj. če nastopa vsaj eno od praštevil v n_3 na liho potenco), in $r_2(n) = 4d(n_1) = 4(d_1(n) - d_3(n))$, če je n_3 kvadrat (tj. vsa praštevila v n_3 nastopajo na sodo potenco). Natančneje, če je n_3 kvadrat in je $n_1 = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$, je $r_2(n) = 4(s_1 + 1)(s_2 + 1)...(s_k + 1)$.*

Dokaz. Glej [11], Chapter 2:

Hitro vidimo naslednje: če je $n = p_1^{s_1}p_2^{s_2}...p_k^{s_k}$ praštevilski razcep in so p_i različna praštevila, so pozitivni delitelji števila n ravno vsi sumandi v razvoju produkta

$$\prod_{1\le i\le k}(1+p_i+p_i^2+...+p_i^{s_i}) = \sum_{0\le r_i\le s_i} p_1^{r_1}p_2^{r_2}...p_k^{r_k}.$$

Poleg tega je $d(n) = \prod_{i=1}^{k}(s_i+1)$. Splošna oznaka za faktorizacijo naj bo $m = \prod_p p^s$.

Najprej pokažimo, da velja $d(n_1) = d_1(n) - d_3(n)$, kjer je $n = 2^c n_1 n_3 = 2^s \prod_{p\equiv 1} p^s \prod_{q\equiv 3} q^t$ (kongrenca vedno po modulu 4). Če z s vedno označimo najvišjo potenco praštevila p, oblike $4k+1$, ki deli n, in s t najvišjo potenco praštevila q, oblike $4k+3$, ki deli n in če upoštevamo, da je $d_1(n) = d_1(n_1n_3)$, $d_3(n) = d_3(n_1n_3)$ in pomeni $d(n_1n_3)$ število vseh lihih deliteljev za n, vidimo, da so lihi delitelji števila n ravno sumandi v razvoju naslednjega produkta:

$$\prod_{p\equiv 1}(1+p+...+p^s)\prod_{q\equiv 3}(1+q+...+q^t) = \sum_{m_i\le s_i, k_j\le t_j} p_1^{m_1}...p_u^{m_u}q_1^{k_1}...q_v^{k_v}.$$

Lihi delitelj $p_1^{m_1}...p_u^{m_u}q_1^{k_1}...q_v^{k_v}$ je kongruenten 1 po modulu 4 natanko takrat, ko je vsota $\sum_j k_j$ soda. Torej dobimo vrednost $d_1(n) - d_3(n)$ tako, da vstavimo v zgornji produkt 1 namesto vsakega p_1 in -1 namesto vsakega q_j, se pravi:

$$d_1(n) - d_3(n) = \prod_{p\equiv 1}(s+1)\prod_{q\equiv 3}(1+(-1)^t)/2.$$

Če je eden od t_j lih, je $d_1(n) - d_3(n) = 0$. Če pa so vsi t_j sodi, je $d_1(n) - d_3(n) = \prod_{p\equiv 1}(s+1) = d(n_1)$.

Pokazati moramo, da je v primeru sodih t-jev, $r_2(n) = 4d(n_1)$. Praštevilska (do asociiranosti in vrstnega reda edina) faktorizacija za n se glasi:

$$n = (1+i)^c(1-i)^c \prod_{a^2+b^2=p}(a+ib)^s(a-ib)^s \prod_{q\equiv 3} q^t.$$

Po drugi strani pa imamo za vsak razcep $n = u^2+v^2 = (u+iv)(u-iv)$ faktorizaciji za oba faktorja:

$$u+iv = i^r(1+i)^{c_1}(1-i)_2^c \prod_{a^2+b^2=p}(a+ib)^{s_1}(a-ib)^{s_2}\prod_{q\equiv 3} q^{t_1}$$

in

$$u-iv = i^{-r}(1+i)^{c_2}(1-i)_1^c \prod_{a^2+b^2=p}(a+ib)^{s_2}(a-ib)^{s_1}\prod_{q\equiv 3} q^{t_1},$$

kjer je $r\in\{0,1,2,3\}$, $c_1+c_2 = c$, $s_1+s_2 = s$ in $2t_1 = t$. Številu različnih reprezentacij za n kot vsote dveh kvadratov ustreza število različnih faktorizacij za $u+iv$ (za $u-iv$ je faktorizacija potem določena). Preštejemo možne izbire za r, c_1, s_1 in t_1: za r štiri; za c_1 nimamo več izbire, kakor hitro je r določen, ker je $(1+i)^{c_1}(1-i)_2^c = i^{-c_2}(1+i)^c$; za s_1 je $s+1$ možnosti (od 0 do s) in za t_1 ena sama ($t_1 = t/2$). Vseh skupaj je torej možnih izbir $4\prod_{p\equiv 1}(s+1)$ in tolik je možnih različnih faktorizacij za $u+iv$, torej ravno $4d(n_1)$, saj je $n_1 = prod_{p\equiv 1}p^s$. To pa pomeni, da je različnih reprezentacij za n v obliki vsote dveh kvadratov ravno $r_2(n) = d(n_1)$, kar je bilo treba videti.

Zgled. Za $n = 5$ je $c = 0$, $n_1 = 5$ ($k = 1$,$s_1 = 1$), $n_3 = 1$, zato je $d(n_1) = 2$, $d_1(n) = 2$, $d_3(n) = 0$ in $r_2(n) = 4d(n_1) = 4(d_1(n) - d_3(n)) = 4(s_1+1) = 8$ ($5 = (\pm 2)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 2)^2$).

Za $n = 6 = 2\cdot 3$ je $r_2(n) = 0$.

Za $n = 25$ je $c = 0$, $n_1 = 25$ ($k = 1$,$s_1 = 2$), $n_3 = 1$ in zato $d(n_1) = 3$, $d_1(n) = 3$, $d_3(n) = 0$ ter $r_2(n) = 12$ ($25 = (\pm 5)^2 + 0^2 = (\pm 4)^2 + (\pm 3)^2 = (\pm 3)^2 + (\pm 4)^2$).

Za $n = 45 = 3^2\cdot 5$ je $c = 0$, $n_1 = 5$ ($k = 1$,$s_1 = 1$), $n_3 = 9$, zato $d(n_1) = 2$, $d_1(n) = 4$, $d_3(n) = 2$ in torej $r_2(n) = 8$ ($45 = (\pm 6)^2 + (\pm 3)^2 = (\pm 3)^2 + (\pm 6)^2$).

Za $n = 145 = 5 \cdot 29$ je $c = 0$, $n_1 = 145$ ($k = 2$, $s_1 = 1$, $s_2 = 1$), $n_3 = 1$, zato $d(n_1) = 4$, $d_1(n) = 4$, $d_3(n) = 0$ in torej $r_2(n) = 16$ ($145 = (\pm 12)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 12)^2 = (\pm 9)^2 + (\pm 8)^2 = (\pm 8)^2 + (\pm 9)^2$).

Literatura

[1] M. Aigner, G.M. Ziegler, *Proofs from THE BOOK*, Springer, 1998.

[2] D.G. Ball, *Constructability of regular and equilateral polygons on square pinboard*, Math. Gazette **57** (1973), 119-122.

[3] M.J. Beeson, *Triangles with Vertices on Lattice Points*, The American Mathematical Monthly **99** (1992), 243-252.

[4] E. Ehrhart, *Sur les Polygones et les Poly'edres Reguliers Entiers*, L'Enseignement Math. **5** (1959), 81-85.

[5] J. Grasselli, *Osnove elementarne teorije števil*, Sigma, DMFA-založništvo, Ljubljana 2009.

[6] R. Honsberger, *Mathematical Gems*, The Two-Year College Mathematical Journal, **13** (1) (1982), 36-44.

[7] D.J. O'Loughlin, *The Scarcity of Regular Polygons on the Integer Lattice*, Math. Magazine **75** (1) (2002), 47-51.

[8] I. Niven, *Irrational numbers*, Carus Monograph 11, 1956.

[9] I. Niven, H.S. Zuckerman, *An Introduction to the Theory of Numbers*, Wiley, 1972.

[10] M. Rubinstein, P. Sarnak, *Chebyshev's bias*, Exper. Math. **3** (1994), 173-197.

[11] J.D. Sally, P.J. Sally, *Roots to Research, A Vertical Development of Mathematical Problems*, Amer. Math. Soc. 2007.

[12] P.R. Scott, *The Fascination of the Elementary*, Amer. Math. Monthly 94 (1987), 759-768.

[13] P. Scott, *Lattice Point Problems; 5. Regular Lattice Polygons*, web.me.com/paulscott.info/lattice-points/5regular.html

[14] P. Scott, *Equiangular Lattice Polygons and Semiregular Lattice Polyhedra*, The College Mathematical Journal **18** (4) (1987), 300-306.

[15] W. Scherrer, *Die Enlargerung eines regularen Vielecks in ein Gitter*, Elemente der Mathematik 1 (1946), 97-98.

[16] I. Vidav, *Algebra*, DMFA Slovenije, Ljubljana 1989.