

Konvex poliéderek stabil lapjai

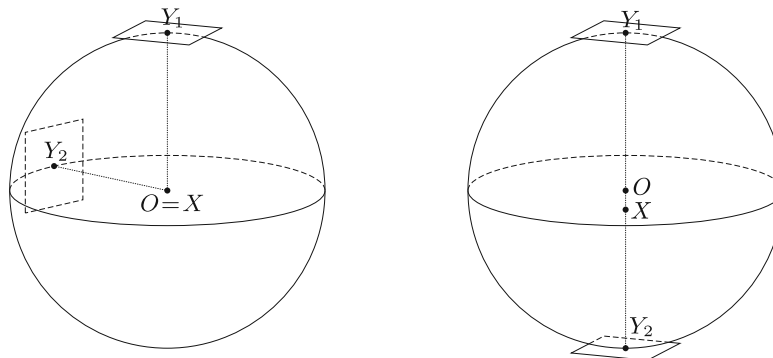
Az első, testek statikai egyensúlyával kapcsolatos eredmények Arkhimédész nevéhez fűződnek, mely eredményeket még a 17. századi hajóépítők is használták. A statikai egyensúlyi pontok vizsgálata végigvonul a fizika és a mérnöki tudományok történetén.

Mi is egy test egyensúlyi pontja? Mi az alábbi módon fogalmazzuk meg.

1. definíció. Legyen K egy konvex test, és X a test egy rögzített belső pontja. Azt mondjuk, hogy a test egy Y határpontja K egy *egyensúlyi pontja* X -re nézve, ha az Y -on átmenő, XY szakaszra merőleges sík nem metszi a K test belsejét. Ha X a K test tömegközéppontja (*homogén* sűrűséget feltételezve), azt mondjuk, hogy az Y pont K egy *egyensúlyi pontja*.

Példák egyensúlyi pontokra:

- Egy gömb minden határpontja egyensúlyi pont a gömb középpontjára nézve. Ha az X viszonyítási pont nem a gömb középpontja, akkor a gömbnek X -re nézve csak két egyensúlyi pontja van: az X -hez legközelebbi, és a vele átellenes, X -től legtávolabbi pontja.
- Egy szabályos tetraéder minden csúcsa, élközéppontja és lapközéppontja a kocka egyensúlyi pontja (a kocka középpontjára nézve).
- Általánosabban: az öt szabályos poliéder minden csúcsa, él- és lapközéppontja a poliéder egyensúlyi pontja.



1. ábra. Egy gömb minden pontja egyensúlyi pont a tömegközéppontra nézve, de más pontra nézve csak a hozzá legközelebbi, illetve a tőle legtávolabbi pontok egyensúlyi pontok

Más módon is megfogalmazhatjuk, mi is egy egyensúlyi pont: az Y pont a K test egy egyensúlyi pontja, ha a K testet alátámaszthatjuk az Y pontban

egy vízszintes síkkal, hogy ne billenjen el. Ekkor a tömegközéppont pontosan Y felett fog elhelyezkedni. Ebben a megközelítésben a tömegközépponttól különböző X viszonyítási pontot tekinthetjük úgy, mint egy *inhomogén* sűrűségű test tömegközéppontját.

Akár homogén, akár inhomogén sűrűséget feltételezve, többféle egyensúlyi pontot különböztethetünk meg. A mindennapokban leginkább *stabil* egyensúlyi pontokkal találkozunk, azaz olyan pontokkal, melyben megtámasztva a testet, az egyensúlyi helyzetből tetszőleges irányban kicsit kibillentve a test visszabilen az egyensúlyi helyzet felé. Ilyen egyensúlyi pontok például a homogén sűrűségű szabályos poliéderek lapközéppontjai, illetve inhomogén gömb esetében a gömbnek a súlyponthoz legközelebbi határpontja.

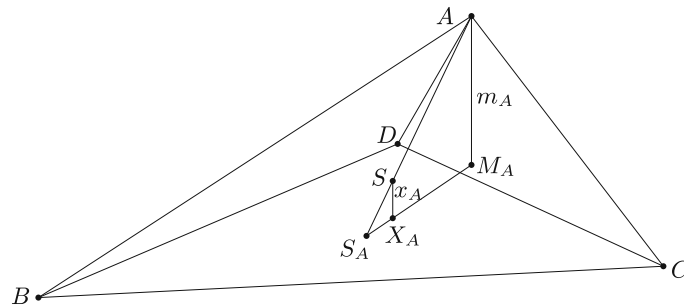
Konvex poliéder esetében a stabil egyensúlyi pontok éppen a lapok belsejében elhelyezkedő egyensúlyi pontok. Így egy P konvex poliéder azon lapjait, melyek belseje tartalmaz egyensúlyi pontot, a továbbiakban stabil lapoknak nevezzük, ezek azok a lapok, melyek síkjára merőlegesen vetítve a poliéder súlypontját, a vetület a lap belsejébe esik. Meggondolható, hogy a súlypontjához legközelebbi lap mindig stabil, így minden poliédernek van legalább egy stabil lapja. A pontosan egy stabil lappal rendelkező poliédereket *monostabil* poliédereknek nevezzük.

John Conway és Richard Guy tette fel az alábbi kérdést 1966-ban: Igaz-e, hogy minden homogén tetraédernek legalább két stabil egyensúlyi pontja van? A kérdésre az igenlő választ Goldberg [2] adta 1969-ben. Ugyanezen állításra később, 1984-ben egy egyszerűbb és érthetőbb bizonyítás jelent meg Dawson egy cikkében [3].

A továbbiakban Dawson bizonyítását ismertetjük Conway és Guy kérdésére.

1. tétel. *Minden tetraédernek van legalább két stabil lapja.*

Bizonyítás. Legyen T egy tetszőleges tetraéder, melynek csúcsai A , B , C és D . A tetraéder súlypontját jelölje S , és az A -val szemközti háromszög lap súlypontját S_A . Legyen a tetraéder A -ból induló magasságának talppontja M_A , és S -nek a BCD háromszög síkjára vett merőleges vetülete X_A . Legyen $m_A = \overline{AM_A}$ és $x_A = \overline{SX_A}$ (lásd 2. ábra). Hasonlóan definiáljuk az S_B , S_C és S_D pontokat, valamint az m_B , x_B , m_C , x_C , m_D , x_D mennyiségeket.



2. ábra. Az $ABCD$ tetraéderre vonatkozó jelölések

Ismert, hogy a tetraéder súlypontja a tetraéder minden súlyvonalát 1 : 3 arányban osztja, azaz

$$\frac{\overline{AS_A}}{\overline{SS_A}} = \frac{\overline{BS_B}}{\overline{SS_B}} = \frac{\overline{CS_C}}{\overline{SS_C}} = \frac{\overline{DS_D}}{\overline{SS_D}} = 4.$$

Vegyük észre, hogy az $SS_A X_A$ és az $AS_A M_A$ háromszögek hasonlók. A megfelelő oldalaik arányára így

$$\frac{m_A}{x_A} = \frac{\overline{AS_A}}{\overline{SS_A}} = 4$$

adódik. Hasonlóan kapjuk az

$$\frac{m_B}{x_B} = \frac{m_C}{x_C} = \frac{m_D}{x_D} = 4$$

egyenlőségeket. Mivel a tetraéder térfogatát úgy számolhatjuk ki, hogy tetszőleges lap területét megszorozzuk a hozzátartozó magasság harmadával, azt kapjuk, hogy a súlypont tetszőleges két lap közül pontosan ahhoz van közelebb, melynek a területe nagyobb.

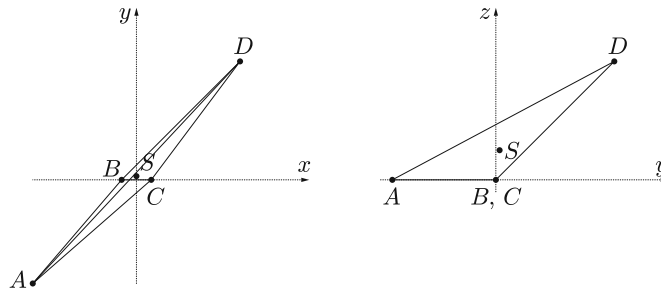
Egy lapon pontosan akkor van stabil egyensúlyi pont, ha S merőleges vetülete a lap síkjára a lap belsejébe esik. Másrészt, mivel a súlypont a tetraéder egy belső pontja, a tetraéder egyik lapjáról csak úgy billenhet át egy másik lapjára, ha a két lap közti lapszög tompaszög. A billenés után a súlypont lejjebb kerül, azaz a tetraéder csak olyan lapjára tud átbillenni, amelynek a síkjához a súlypont közelebb van. Az előző bekezdésben meg gondoltak szerint így a tetraéder csak kisebb területű lapról egy nagyobb területű lapra tud átbillenni.

Tegyük most fel, hogy T -nek csak egy stabil lapja van. Vegyük észre, hogy a fentiek szerint a stabil lap így a legnagyobb területű lap. Legyen T legnagyobb lapja BCD , és a második legnagyobb lapja ACD . A tetraéder egy harmadik lapja így vagy először az ACD lapra, és arról a BCD lapra gördül, vagy ez a lap és az ACD lap is közvetlenül a BCD lapra gördül. Mindkét esetben igaz az, hogy a két legnagyobb lap egyikéhez két derékszögnél nagyobb lapszög tartozik, és az egyik ilyen lapszög a két legnagyobb lap közti lapszög. Jelölje ezt a lapot F , és a tetraéder negyedik lapját G . Ekkor F és G szöge hegyesszög, és G merőleges vetülete F síkjára szigorúan tartalmazza F -et. De így F területe határozottan kisebb, mint G területe, ami ellentmond annak a feltevésnek, hogy F a két legnagyobb, G pedig a két legkisebb területű lap egyike. \square

1967-ben Heppes Aladár [6] konstruált egy T tetraédert egy érdekes, a fenti problémához kapcsolódó tulajdonsággal: a Heppes-féle ‘double-tipping’ tetraédernek két lapján található stabil pont, és egy harmadik lapján megtámasztva a tetraéder először a negyedik lapra gördül, mielőtt találna egy egyensúlyi helyzetet valamelyik stabil lapon. Hogyan is néz ki ez a tetraéder? Ezt mutatjuk meg a továbbiakban.

Legyen $A = (-7; -7; 0)$, $B = (-1; 0; 0)$, $C = (1; 0; 0)$ és $D = (7; 8; 8)$ egy T tetraéder négy csúcsa. Ekkor a tetraéder alaplapja az (x, y) -koordinátasíkban helyezkedik el, és súlypontja, melynek koordinátáit az egyes csúcsok megfelelő koordinátájaként számolhatjuk ki, az $S = (0; 0, 25; 2)$ pont, melynek vetülete az alaplap

síkjára $S' = (0; 0; 25; 0)$. A tetraéder alaplapja az ABC lap, amin az S' pont kívül esik, tehát T ebből a helyzetből átfordul egy másik lapra.



3. ábra. A T tetraéder vetülete az (x, y) és az (y, z) síkokra

A D csúcs vetülete az ABC lap síkjára a $D' = (7; 8; 0)$ pont, ami az A , B és C pontokkal együtt egy konvex négyszöget alkot. Ebből látható, hogy az $ABCD$ tetraéder AB és AC élénél levő lapszöge hegyesszög, tehát az ABC lapról T a BC él mentén, vagyis az x -tengely körül fordul át a BCD lapra.

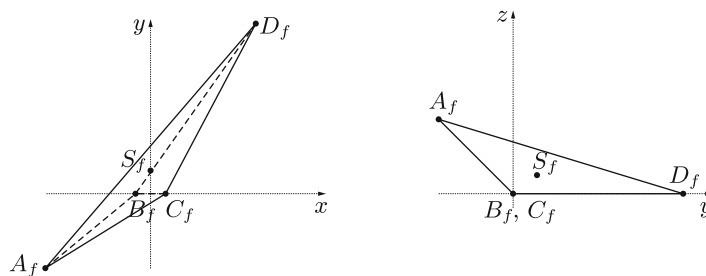
Vegyük észre, hogy mind az ABC , mind a BCD lap merőleges az (y, z) -koordinátasíkra. A tetraéder csúcsainak merőleges vetületei erre a síkra rendre $\bar{A} = (0; -7; 0)$, $\bar{B} = \bar{C} = (0; 0; 0)$ és $\bar{D} = (0; 8; 8)$. Ebből látható, hogy a T tetraéder BC élénél levő lapszöge 135° , azaz az átfordulás szöge az x -tengely körül 45° . Minthogy a forgás során a pontok x -koordinátái nem változnak, kiszámolhatóak az elfordult T_f tetraéder csúcsainak koordinátái, melyek rendre

$$A_f = (-7; -3, 5\sqrt{2}; 3, 5\sqrt{2}); \quad B_f = B = (-1; 0; 0);$$

$$C_f = C = (1; 0; 0); \quad D_f = (7; 8\sqrt{2}; 0).$$

A T_f tetraéder súlypontja, és ennek vetülete az (x, y) -koordinátasíkra rendre

$$S_f = (0; 1,125\sqrt{2}; 0,875\sqrt{2}); \quad S'_f = (0; 1,125\sqrt{2}; 0).$$



4. ábra. Az elfordult T_f tetraéder vetülete az (x, y) és az (y, z) síkokra

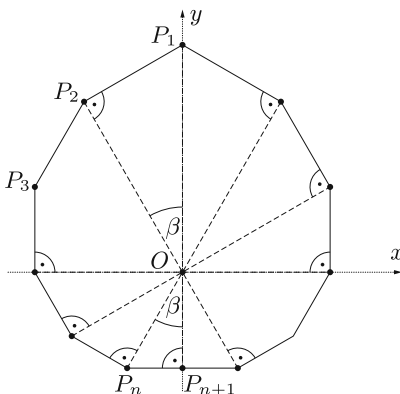
Könnyen kiszámolható, hogy S'_f kívül esik az átfordult tetraéder $B_f C_f D_f$ alaplapján. Így a tetraédernek ez a lapja sem stabil, azaz T_f ebből a helyzetből is

átfordul valamelyik éle mentén egy harmadik lapjára, mely az első tételünk szerint stabil.

Láttuk, hogy minden tetraédernek legalább két stabil lapja van. Esetleg igaz-e az is, hogy minden konvex poliédernek van legalább két stabil lapja? Conway és Guy [2] alábbi konstrukciója mutatja, hogy ez viszont nem igaz.

2. tétel. *Van olyan 19 lapú K konvex poliéder, melynek pontosan egy stabil lapja van a tömegközéppontjára nézve.*

A bizonyítás ötlete Először egy A $(2n - 1)$ -szöget definiálunk az (x, y) -síkon az alábbi módon, ahol $n \geq 2$.



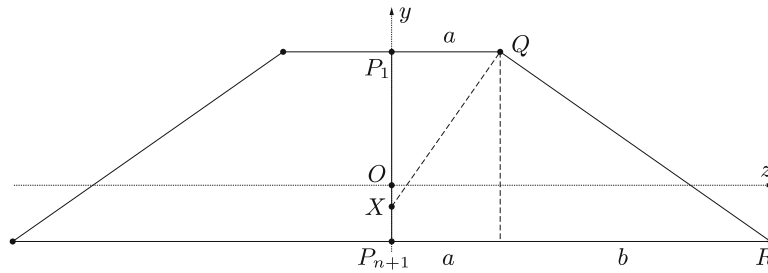
5. ábra. Az A $(2n - 1)$ -szög konstrukciója

a $P_n P_{n+1} O$ szög derékszög. Trigonometrikus függvények használatával könnyen látható, hogy $\overline{OP_2} = \cos \beta$, $\overline{OP_3} = \cos^2 \beta$, illetve általában $\overline{OP_i} = \cos^{i-1} \beta$ minden $i = 1, 2, \dots, n + 1$ esetén, azaz speciálisan P_n és P_{n+1} rajta vannak az (x, y) -sík $y = -\cos^n \beta$ egyenletű egyenesén.

A P_2, P_3, \dots, P_n pontokat tükrözzük az y -tengelyre, és jelölje a tükörképeket rendre P'_2, P'_3, \dots, P'_n . A konstruálni kívánt A sokszöget a $P_1 P_2 \dots P_n P'_n \dots P'_2$ töröttvonal határolta konvex sokszöggként definiáljuk. Vegyük észre, hogy az OP_{n+1} szakasz tetszőleges belső pontjára igaz, hogy A oldalegyenesekre vett merőleges vetületei közt egyetlenegy van, amelyik A -nak is pontja; ez a pont a P_{n+1} pont a $P_n P'_n$ oldal egyenesén. Ez az észrevétel lesz az alapja a konstrukciónknak.

Legyen G az a végtelen gúla, melyet úgy kapunk, hogy A minden pontjában merőlegest bocsátunk az (x, y) -síkra, és vesszük az összes így keletkezett egyenes unióját. Ebből a végtelen gúlából egy korlátos K gúlát fogunk konstruálni úgy, hogy elmetsszük két S_1, S_2 síkkal, melyek szimmetrikusak az (x, y) -síkra, és merőlegesek az (x, z) -síkra (ld. 6. ábra). Ezen síkok metszete az (y, z) -síkka egy-egy egyenes. Az S_1, S_2 síkokat úgy választjuk, hogy S_1 tartalmazza a $Q(0; 1; a)$ és az $R(0; -\cos^n \beta, a + b)$ pontot, ahol $a, b > 0$, és az S_2 sík S_1 tükörképe az (x, y) -síkra. $(2n - 1)$ -szög. A poliéder szimmetriái miatt látható, hogy a poliéder súlypontja a $P_1 P_{n+1}$ szakasz egy pontja.

Legyen $\beta = \frac{\pi}{n}$, és $P_1 P_2 O$ egy olyan derékszögű háromszög, melyben $\overline{OP_1} = 1$, $P_1 O P_2 \sphericalangle = \beta$ és $P_1 P_2 O \sphericalangle = \frac{\pi}{2}$ (ld. 5. ábra). Írjunk a háromszög OP_2 befogójára egy $OP_2 P_3$ háromszöget, mely hasonló az $OP_1 P_2$ háromszöghöz, átfogója OP_2 , és O -nál levő szöge β . Ezen háromszög OP_3 befogójára ugyancsak írjunk egy hasonló háromszöget, melynek átfogója OP_3 , és O -nál levő szöge β . Az eljárást folytatjuk, amíg eljutunk az $OP_n P_{n+1}$ háromszöghöz, amely ugyancsak hasonló az $OP_1 P_2$ háromszöghöz, átfogója OP_n , és O -nál levő szöge β . Ekkor β definíciója miatt a P_1, O, P_{n+1} pontok egy egyenesen vannak, és



6. ábra. A K csonkolt gúla (y, z) -síkra vett merőleges vetületének képe

Állítsunk merőlegest az S_1 síkra a Q pontban, és a merőleges egyenes y -tengellyel vett metszéspontját jelölje X . Ha a poliéder súlypontja az OX szakaszt tartalmazó lap, akkor K -nak csak egy stabil lapja van; ez a lap a $P_n P'_n$ szakaszt tartalmazó lap. Megmutatjuk, hogy ha a értéke rögzített és b értéke nagyon nagy a -hoz képest, akkor $n = 9$ esetén ez teljesül.

Ha $b \gg a$, akkor $P_{n+1} \in OX$, tehát csak azt kell megvizsgálnunk, hogy a súlypont y -koordinátája negatív-e. Kiszámolható, hogy a $t = \cos \beta$ jelöléssel a súlypont y -koordinátája

$$y_s = -\frac{t}{12 \sin \beta} \left[-2a(1+t^{3n}) \frac{(1-t^2)(1+2t^2)}{1+t^2-t^4} + \frac{b}{1+t^n} \cdot \left((1-t^{4n}) \frac{1+2t^2+4t^4+2t^6-3t^8}{(1+t^2)(1+t^2+3t^4-t^6)} - 2(1+t^{3n}) \frac{(1-t^2)(1+2t^2)}{1+t^2-t^4} \right) \right],$$

amiből látható, hogy $b \gg a$ esetén, ha a második sorban levő kifejezés pozitív, akkor y_s negatív. Számolással adódik, hogy a legkisebb n érték, melyre ez teljesül, $n = 9$. Ebben az esetben K egy 19 lapú, pontosan egy stabil lappal rendelkező poliéder. \square

A fenti eredmények több további kérdést is felvetnek.

- (1) Van-e *inhomogén* sűrűségű tetraéder, melynek pontosan egy stabil lapja van?
- (2) Mennyi a monostabil, azaz (a súlypontjukra) pontosan egy stabil lappal rendelkező konvex poliéderek lapszámának minimuma?
- (3) Speciálisan, igaz-e, hogy a négyszög alaplapú gúlák közt nincs monostabil?
- (4) Egyensúlyi ponttal rendelkező lapok helyett egyensúlyi ponttal rendelkező csúcsokat is vizsgálhatunk. Ezekre igaz-e az első tételünk „duális” változata, azaz igaz, hogy minden tetraédernek van legalább kettő egyensúlyi ponttal rendelkező csúcsa?

Az első kérdésre Conway adta meg az igenlő választ, melyről bővebb információ található a [4] cikkben.

Jelölje a monostabil poliéderek minimális lapszámát l_m . Ekkor az eddig ismertett eredményeket az $5 \leq l_m \leq 19$ egyenlőtlenségekben foglalhatjuk össze. A második kérdést illetően Conway eredménye, mely szerint $l_m \leq 19$, meglepően sokáig

a legjobb felső becslés maradt l_m értékére. Az első javítás Bezdek Andrásnak [1] köszönhető, aki, ugyancsak elemi geometriai módszerekkel, 2011-ben konstruált egy 18 lapú monostabil poliédert. Ezt 2014-ben Reshetov [7] javította 14-re számítógépes módszerek alkalmazásával. A harmadik, Conway és Guy által 1969-ben feltett kérdés, hogy a négyszöglapú gúlak közt van-e monostabil, még ma is nyitott.

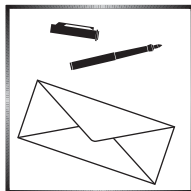
Az utolsó kérdésre igenlő a válasz (ld. [5]), de ennek tárgyalása meghaladja ezen cikk kereteit.

Hivatkozások

- [1] A. Bezdek, *On stability of polyhedra*, in: Workshop on Discrete Geometry, Sept. 13–16, 2011, Fields Institute, Canada, 2490–2491.
- [2] J. H. Conway, M. Goldberg and R. K. Guy, *Problem 66-12*, SIAM Rev. **11** (1969), 78–82.
- [3] R. Dawson, *Monostatic simplexes*, Amer. Math. Monthly, **92** (1985), 541–546.
- [4] R. Dawson and W. Finbow, *What shape is a loaded die?*, Math. Intelligencer, **22** (1999), 32–37.
- [5] G. Domokos, F. Kovács, Z. Lángi, K. Regős and P.T. Varga, *Balancing polyhedra*, arXiv:1810.05382 [math.MG], October 12, 2018.
- [6] A. Heppes *A double-tipping tetrahedron*, SIAM Rev., **9** (1967), 599–600.
- [7] A. Reshetov, *A unistable polyhedron with 14 faces (English summary)*, Internat. J. Comput. Geom. Appl., **24** (2014), 39–59.

Lángi Zsolt

BME Geometria Tanszék
zlangi@math.bme.hu



Az RSA kulcsgenerálás és a Carmichael-számok kapcsolata 1.

A nyílt kulcsú titkosító algoritmus matematikai alapjait 1976-ban fektette le Ron Rivest, Adi Shamir és Len Adleman. A nevük kezdőbetűi alapján elnevezett RSA algoritmus napjaink egyik leggyakrabban használt adattitkosító eljárása. A szakirodalomban elérhető matematikai alapok felhasználásával magam is elkészítettem a titkosító eljárás – gyakorlatban is jól használható – programját. A kulcsgenerálás algoritmusának pontosabb vizsgálatával sikerült kimutatni, hogy a prímek mellett speciális összetett számok is kiválóan alkalmazhatók kulcsok generálásához, sőt jelentősen csökkenthetik a kulcsok előállításának időtartamát.

A dolgozat megmutatja, hogy a Fermat féle prímteszt – annak ellenére, hogy prímek keresésére nem megbízható, mert átbújhatnak rajta összetett számok is – tökéletesen alkalmas megbízható RSA kulcsok generálására.