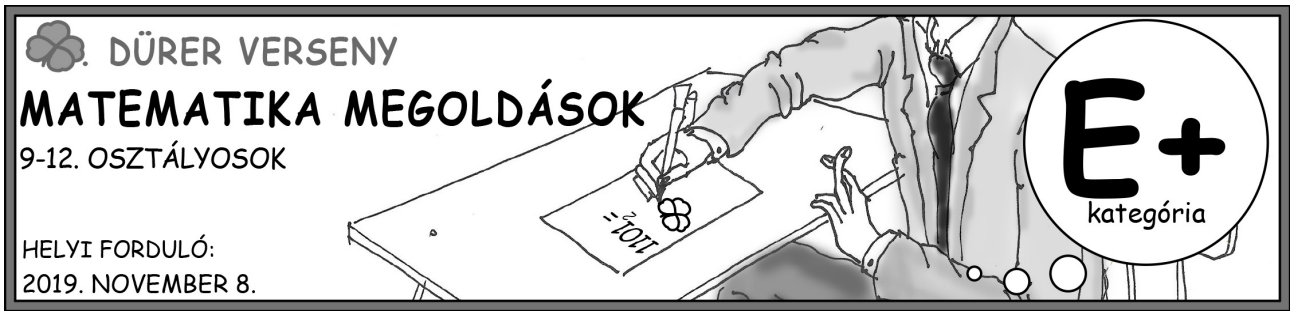


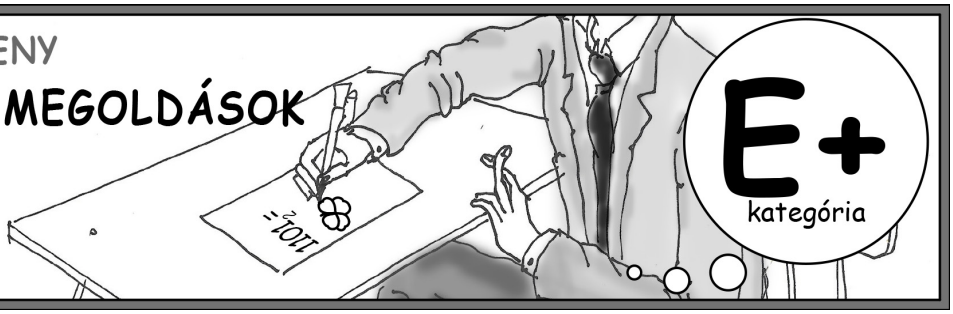
E+1. **a)** Lehetséges-e, hogy két különböző pozitív egész szám pozitív osztóinak összege megegyezik?
b) Lehetséges-e, hogy két különböző pozitív egész szám pozitív osztóinak szorzata megegyezik?

Megoldás: a) Igen, például 12 az osztók összege 6 és 11 esetén is.

b) Nem, megmutatjuk, hogy ha n és m osztóinak szorzata megegyezik, akkor $n = m$.

Először igazoljuk, hogy n osztóinak szorzata $n^{\frac{d(n)}{2}}$, ahol $d(n)$ jelöli n osztóinak számát. Az osztók osztópárokba rendeződnek, azaz ha $k \mid n$, akkor $\frac{n}{k} \mid n$ és $k \cdot \frac{n}{k} = n$. Ebből azonnal adódik a képlet.

Azt kell még igazolni, hogy ha $n^{\frac{d(n)}{2}} = m^{\frac{d(m)}{2}}$ akkor $n = m$. Látszik, hogy ekkor egy prím pontosan akkor osztja n-et, ha m-et is osztja. Vegyünk egy p prímet, mely osztja n-et. Legyen k az a pozitív egész, melyre $p^k \mid n$, de $p^{k+1} \nmid n$, és hasonlóan legyen l az a szám, melyre $p^l \mid m$, de $p^{l+1} \nmid m$. Ekkor mivel $n^{\frac{d(n)}{2}} = m^{\frac{d(m)}{2}}$, ezért p kitevője is megegyezik a két oldalon, így $\frac{k \cdot d(n)}{2} = \frac{l \cdot d(m)}{2}$, azaz $\frac{k}{l} = \frac{d(m)}{d(n)}$. Ez minden prímre igaz, így ha $d(n) < d(m)$, akkor minden p prímre, mely osztja n-et, a p kitevője n-ben nagyobb, mint m-ben, így $n > m$. Mivel m minden osztója n-et is osztja, így nem lehet egyenlő az osztók szorzata. Hasonlóan $d(n) > d(m)$ sem lehet, így $d(n) = d(m)$, azaz minden prím kitevője megegyezik n-ben és m-ben, és ez pont azt jelenti, hogy $n = m$.



E+2. Hányféleképpen lehet egy $n \times n$-es táblázatot egész számokkal kitölteni úgy, hogy a táblázat minden mezőjében az a szám álljon, amennyi a mező sorában és oszlopában rajta kívül összesen található páros számok száma?
Két kitöltést különbözőnek tekintünk, ha van olyan mező, amelyben különböző számok állnak a két kitöltésben.

1. Megoldás: Az első lényeges észrevételünk, hogy elég az egyes mezőkben álló számok paritását meghatározni, az egyértelműen megad egy kitöltést. Világos, hogy minden kitöltésből egyértelműen következik a mezők paritása, és fordítva is, csak össze kell számolnunk, hány páros elem van egy adott elem sorában és oszlopában rajta kívül. Ezentúl 0-val jelöljük a páros mezőket és 1-essel a páratlanokat.

A második észrevétel a következő: Két szomszédos oszlop vagy megegyezik, vagy minden mezőjük (soronként) ellentétes. Ebből következik, hogy bármely két oszlop megegyezik, vagy pont ellentétes. Természetesen ez a sorokra is igaz lesz. Az állítást elég igazolnunk 2×2-es résztáblázatokra. Nézzen ki a táblázatunk a következőképpen:

A	C	E
B	D	F
G	H	

Itt a betűk azt jelölik, hogy az adott tartományban hány páros mező van. Nyilván ekkor a bal felső 2×2-es résztáblázatban a mező paritása pont ellentétes a beleírt betű paritásával, de ekkor is elég megmutatnunk, hogy A, B illetve C, D megegyeznek, vagy pont ellentétesek.

Ekkor a következő kongruenciákat írhatjuk fel a bal felső 2×2 mező alapján:

$$A \equiv C + E + B + G \pmod 2$$

$$B \equiv D + F + A + G \pmod 2$$

$$C \equiv A + E + D + H \pmod 2$$

$$D \equiv B + F + C + H \pmod 2$$

Ezt a négy egyenletet összeadva:

$$A + B + C + D \equiv 2A + 2B + 2C + 2D + 2E + 2F + 2G + 2H \equiv 0 \pmod 2$$

$$A + C \equiv B + D \pmod 2$$

Ami azt jelenti, hogy ha $A \equiv C \pmod 2$, akkor $B \equiv D \pmod 2$, és ha $A \not\equiv C \pmod 2$, akkor pedig $B \not\equiv D \pmod 2$, ezt szerettünk volna belátni.

Bevezetünk néhány elnevezést és jelölést: Egy táblázatot önleírónak nevezünk, ha teljesül rá a feladat feltétele. A táblázat i-edik sorában és j-edik oszlopában található mezőt (i, j)-vel fogjuk jelölni, és egy kitöltésnél $f(i, j)$-vel jelöljük az (i, j) mezőbe írt számot. Egy mezőt egy kitöltésnél jónak nevezünk, ha teljesül rá a feltétel, azaz annyi páros van rajta kívül a sorában és az oszlopában modulo 2, mint amennyit a mezőbe írtunk. Nevezzünk egy kitöltést szépnek, ha minden oszlop megegyezik az elsővel, vagy pont ellentétes. Világos, hogy egy kitöltés pontosan akkor szép, ha minden sor megegyezik az elsővel, vagy pont ellentétes. A második észrevétel szerint minden önleíró kitöltés szép.

Most pedig megmutatjuk, hogy ha n páros, akkor a táblázatnak pontosan egy önleíró kitöltése van, amikor minden mezőjén páros szám áll (azaz $2n-2$).

Indirekten tegyük fel, hogy egy önleíró kitöltésben van páratlan mező. Mivel a táblázat sor- és oszlopcserék után is kielégíti a feltételeket, feltehetjük, hogy $f(1,1)=1$. A feladat feltétele szerint ekkor vagy az első sorban, vagy az első oszlopban kell páros számnak lennie, feltehetjük, hogy $f(1,2)=0$. Legyen x a páros mezők száma az első oszlopban. Ekkor mivel a kitöltés szép, ezért ha egy oszlopban az első mező 1, akkor ez az oszlop megegyezik az elsővel, tehát x darab páros mezőt tartalmaz, míg ha 0 az első mező, akkor az oszlop pont ellentétes, mint az első, így az oszlopban $n-1-x$ darab páros szám van még az első 0-n kívül. Legyen $k+1$ darab páros szám az első sorban.

1	0	k db ps
x db ps	$n-1-x$ db ps	

Írjuk fel az $(1,1)$ mezőre a feladat feltételét:

$$1 \equiv k+1+x \pmod 2$$

Most az $(1,2)$ mezőre:

$$0 \equiv k+n-1-x \equiv k+x+1 \pmod 2$$

Ellentmondás.

Ha n páratlan, akkor azt állítjuk, hogy 2^{2n-2}-féle önleíró kitöltés létezik.

Válasszuk meg tetszőlegesen, hogy az első oszlopot, és az első sort az utolsó mezője kivételével hogyan töltjük ki. Ez $2n-2$ szabad választás, tehát 2^{2n-2}-féleképpen tehetjük meg. Azt állítjuk, hogy minden ilyen elkezdést pontosan egyféleképpen tudjuk önleíró kitöltéssé egészíteni. Az $(1,1)$ mezőnek jónak kell lennie, ez meghatározza az $(1,n)$ mezőt. A kitöltésnek szépnek is kell lennie, és ez minden oszlopot meghatározza, mivel az első sorban lévő eleme minden oszlopnak meghatározza, hogy az első oszloppal egyeznie kell, vagy pont ellentétesnek kell lennie. Tehát egyértelműen ki tudtuk tölteni a táblázatot, már csak azt kell igazolni, hogy ez egy önleíró kitöltés. Ehhez az kell, hogy minden mező jó legyen. $(1,1)$-ről tudjuk, hogy jó, igazoljuk, hogy ekkor $(1,2)$ is jó. Ha $f(1,1)=f(1,2)$, akkor az első sorban $f(1,1)$-n kívül ugyanannyi páros van, mint $f(1,2)$-n kívül, és az oszlopuk megyegyezik, tehát $(1,2)$ is jó. Ha $f(1,1)\neq f(1,2)$ akkor az első sorban $f(1,1)$-n kívül nem annyi páros van modulo 2, mint ahány $f(1,2)$-n kívül. Ha az első oszlopban $f(1,1)$-n kívül x darab páros szám van, akkor a második oszlopában $f(1,2)$-n kívül $n-1-x$ lesz mivel a két oszlop ellentétes. $x \equiv n-1-x$, tehát $(1,2)$ ebben az esetben is jó. Ugyanígy tudjuk igazolni, hogy $(1,j)$ jó minden j-re, és hasonlóan tudjuk igazolni, hogy ha $(1,j)$ jó akkor (i,j) is az. Tehát a táblázat tényleg önleíró.

Összefoglalva: páros n esetén pontosan 1, páratlan n esetén pedig 2^{2n-2}-féle megfelelő kitöltése létezik az $n \times n$-es táblázatnak.

2. Megoldás: Az előző megoldáshoz hasonlóan elég minden mezőnek csak a parítását meghatározni, így a megoldás során végig modulo 2 számolunk. Jelölje $t_{i,j}$ az $n \times n$-es táblázat i-edik sorának j-edik elemét modulo 2. Legyen s_i és o_i rendre az i-edik sorban, illetve oszlopban lévő páros számok száma modulo 2.
Ekkor

$$t_{i,j} \equiv s_i + o_j \tag{1}$$

.
Tehát ha ismerjük s_i-t és o_i-t minden i-re, akkor ismerjük az összes értéket a táblázatban. Az s_i értéket modulo 2 ki lehet fejezni $t_{i,j}$-ből, hiszen s_i-ben $t_{i,j}$-t akkor számoltuk meg, ha $t_{i,j} \equiv 0$. Formálisan:

$$s_i \equiv \sum_{j=1}^{n} (1 + t_{i,j})$$

Ezt tovább bontva (1) segítségével:

$$s_i \equiv \sum_{j=1}^{n} (1 + t_{i,j}) \equiv \sum_{j=1}^{n} (1 + s_i + o_j) \equiv n + n s_i + \sum_{j=1}^{n} o_j \tag{2}$$

Hasonlóan o_i-re:

$$o_i \equiv \sum_{j=1}^{n} (1 + t_{j,i}) \equiv \sum_{j=1}^{n} (1 + s_j + o_i) \equiv n + n o_i + \sum_{j=1}^{n} s_j$$

Ha n páros, akkor az utóbbi két egyenlet:

$$s_i \equiv \sum_{j=1}^{n} o_j \equiv 0$$

$$o_i \equiv \sum_{j=1}^{n} s_j \equiv 0$$

Mivel a jobb oldali szummák nem függnek i-től, ezért az s_i-k és o_j-k egyenlők. Ekkor viszont a szummákban páros sokszor adtuk össze ugyanazt a számot, vagyis 0 az érték. Tehát $t_{i,j} = 0$ minden i, j-re. Ha n páros, akkor csak ez az egy jó megoldás van.

Ha n páratlan, akkor a (2)-es egyenletből:

$$1 \equiv -n + (1 - n) s_i \equiv \sum_{j=1}^{n} o_j \tag{3}$$

és hasonlóan

$$1 \equiv \sum_{j=1}^{n} s_j \tag{3}$$

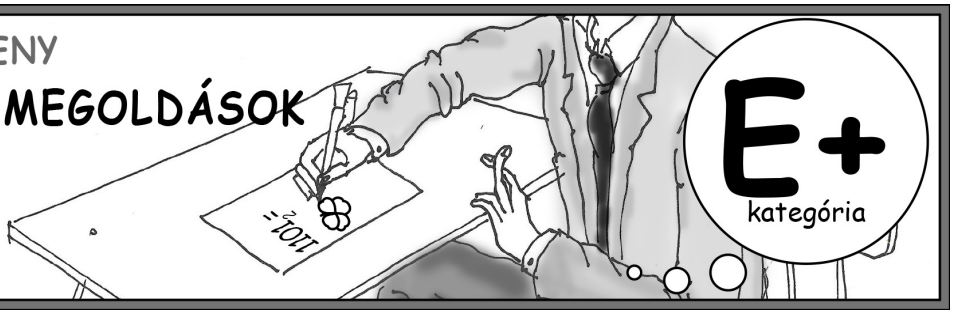
Válasszuk tetszőlegesen az első $n-1$ s_i és o_i értékét, azt állítjuk, hogy ez egyértelműen meghatároz egy megoldást. Az s_n-t és o_n-t egyértelműen meghatározzák a (3) kongruenciák, így (1)-ből minden $t_{i,j}$ meg van határozva. Minden s_i és o_i választás esetén különböző kitöltést kapunk, mivel ha adottak az s_i, o_i, s_i', o_i' számok, akkor kapom ugyanazt a kitöltést, ha $s_i = s_i'$ és $o_i = o_i'$ minden i-re vagy ha $s_i \equiv 1 + s_i'$ és $o_i \equiv 1 + o_i'$. De (3) miatt a második opció nem jön szóba, mivel $1 \equiv \sum_{j=1}^{n} s_j$ és

$1 \equiv \sum_{j=1}^{n} 1 + s_j$ nem teljesülhet egyszerre, mert n páratlan. Már csak azt kell belátni, hogy az s_i és o_i számok által meghatározott $t_{i,j}$ számok tényleg megoldást adnak. És ez igaz, mivel

$$t_{k,l} \equiv s_k + o_l \equiv 1 - \sum_{\substack{i=1 \\ i \neq k}}^{n} s_i + 1 - \sum_{\substack{j=1 \\ j \neq l}}^{n} s_i + (n-1)(s_k + o_l) \equiv \sum_{\substack{i=1 \\ i \neq k}}^{n} (s_i + o_l) + \sum_{\substack{j=1 \\ j \neq l}}^{n} (s_k + o_j) \equiv \sum_{\substack{i=1 \\ i \neq k}}^{n} t_{i,l} + \sum_{\substack{j=1 \\ j \neq l}}^{n} t_{k,j}$$

és pont ezt akartuk.

Összefoglalva ha n páros, akkor csak 1 megoldás van, ha páratlan, akkor 2^{2n-2} db megoldás van.



E+3. Legalább hány nemnulla valós számot kell kiválasztani ahhoz, hogy bármely kiválasztott szám előálljon pontosan 2019 darab másik kiválasztott szám összegeként, ha
a) lehetnek egyenlő számok a kiválasztottak között?
b) nem lehet két azonos kiválasztott szám?

Megoldás: 2019 helyett általánosan n-re oldjuk meg a feladatot, ahol $n > 3$ páratlan szám. Páros n és $n = 3$ esetén is hasonlóan megy a megoldás.

a) Válasz: $n + 3$.

Világos, hogy legalább $n+1$ szám kell. Igazolni fogjuk, hogy $n+1$ és $n+2$ szám nem elég, és $n+3$ esetén van konstrukció.

Tegyük fel, hogy $n + 1$ szám elég, legyenek a kiválasztott számok $a_1 \leq a_2 \leq ... \leq a_{n+1}$. Ekkor $a_1 = a_2 + a_3 + ... + a_{n+1}$ és $a_{n+1} = a_1 + a_2 + ... + a_n$. Az első egyenletből a másodikat kivonva azt kapjuk, hogy $a_1 - a_{n+1} = a_{n+1} - a_1$, azaz $a_1 = a_{n+1}$, ami azt jelenti, hogy az összes a_i egyenlő, ekkor azonban $a_1 = a_2 + a_3 + ... + a_{n+1} = n \cdot a_1$, ami nem lehetséges, mivel $n > 1$ és $a_1 \neq 0$.
Most tegyük fel, hogy $n+2$ szám elég, és legyenek a kiválasztott számok $a_1 \leq a_2 \leq ... \leq a_{n+2}$. Ekkor a_1 előáll másik n szám összegeként, tehát $a_1 \geq a_2+a_3+...+a_{n+1}$, és hasonlóan $a_{n+2} \leq a_2+a_3+...+a_{n+1}$. Tehát $a_1 \geq a_{n+2}$, azaz $a_1 = a_{n+2}$ és ez megint nem lehetséges, ugyanúgy, mint az előző esetben.

$n + 3$ szám pedig elég: Vegyünk $\frac{n+3}{2}$ darab (-1)-est és $\frac{n+3}{2}$ darab 1-est. Ekkor minden (-1)-es felírható úgy, mint a másik $\frac{n+1}{2}$ darab (-1)-es és $\frac{n-1}{2}$ darab 1-es összege, és hasonlóan minden 1-es felírható úgy, mint a másik $\frac{n+1}{2}$ darab 1-es és $\frac{n-1}{2}$ darab (-1)-es összege. Ez tehát tényleg jó konstrukció $n + 3$ kiválasztott számmal.

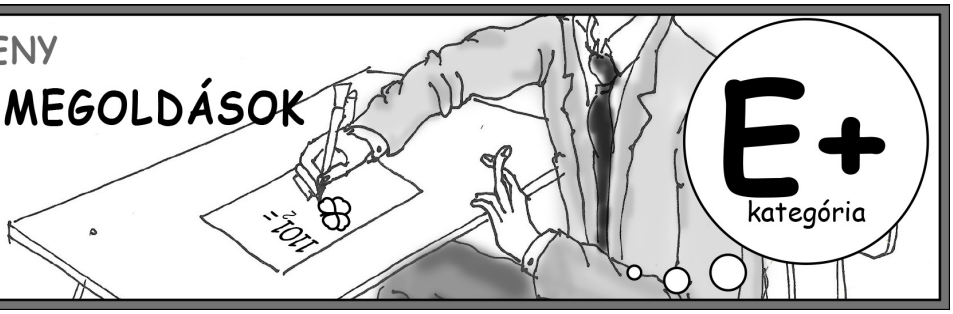
b) Válasz: $n + 4$.

Az **a)** rész alapján mindenképpen szükség van $n + 3$ számra.

Indirekten tegyük fel, hogy $n+3$ elég, legyenek a kiválasztott számok $a_1 < a_2 < ... < a_{n+3}$. Ekkor a_1 előáll, mint másik n szám összege, tehát $a_1 \geq a_2+a_3+...+a_{n+1}$ és hasonlóan $a_{n+3} \leq a_3+a_4+...+a_{n+2}$. A második egyenlőtlenségből az elsőt kivonva kapjuk, hogy $a_{n+3} - a_1 \leq a_{n+2} - a_2$, de ez nem lehet, mivel $a_1 < a_2 < a_{n+2} < a_{n+3}$.

$n + 4$ esetén van konstrukció. Írjuk n-et $2k + 1$ alakban, ahol $k > 1$ egész. Ekkor a konstrukció $n + 4 = 2k + 5$ számmal: $-k - 3,\ -k - 2,\ \ldots,\ -2,\ 1,\ 2,\ \ldots,\ k + 3$. Ez $2k + 5$ szám, melyek összege 1. Ha ezek közül egy l számhoz találunk másik $2k + 1$ darabot, melyek összege l, akkor a kimaradó 3 szám összege $1 - 2l$, és ez visszafelé is igaz, ha l-en kívül találunk 3 számot, melyek összege $1 - 2l$, akkor a további $2k + 1$ darab szám összege pont l lesz, így elég azt igazolni, hogy a fent megadott $2k+5$ számra igaz az, hogy közülük bármelyik l számhoz létezik 3 darab tőle különböző szám, melyek összege $1 - 2l$.

A $-k - 3$-hoz megfelelő a $2, k + 2, k + 3$ számhármas.
$3 \leq i \leq k + 2$ esetén $-i$-hez jó az $1, i - 1, i + 1$.
-2-höz a $-3, 3, 5$ megfelelő (itt kihasználjuk, hogy $5 \leq k + 3$ azaz $k \geq 2$).
1-hez a $4, -2, -3$ jó.
2-höz a $3, -2, -4$ számhármas a megfelelő.
$3 \leq i \leq k + 2$ esetén i-hez az $1, -i - 1, -i + 1$ jó választás.
Végül $k + 3$-hoz a $-2, -k - 1, -k - 2$ számhármast választjuk (itt is felhasználjuk hogy $k \geq 2$, ez biztosítja azt, hogy $-2 \neq -k - 1$).
Tehát tényleg minden előáll másik n összegeként.

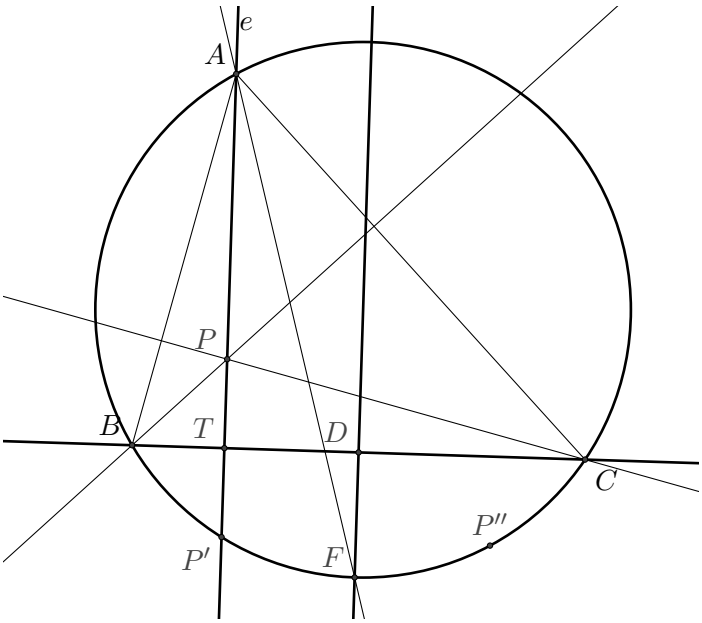


E+4. Egy ABC nem egyenlőszárú háromszögnek adott az A csúcsából induló magasságának talppontja, a háromszög körülírt körén levő, az A pontot nem tartalmazó BC ív felezőpontja, és adott még egy P pont.
Szerkesszétek meg ezekből az adatokból az ABC háromszöget, ha a P pont a háromszög
a) magasságpontja.
b) súlypontja.
c) beírt körének középpontja.

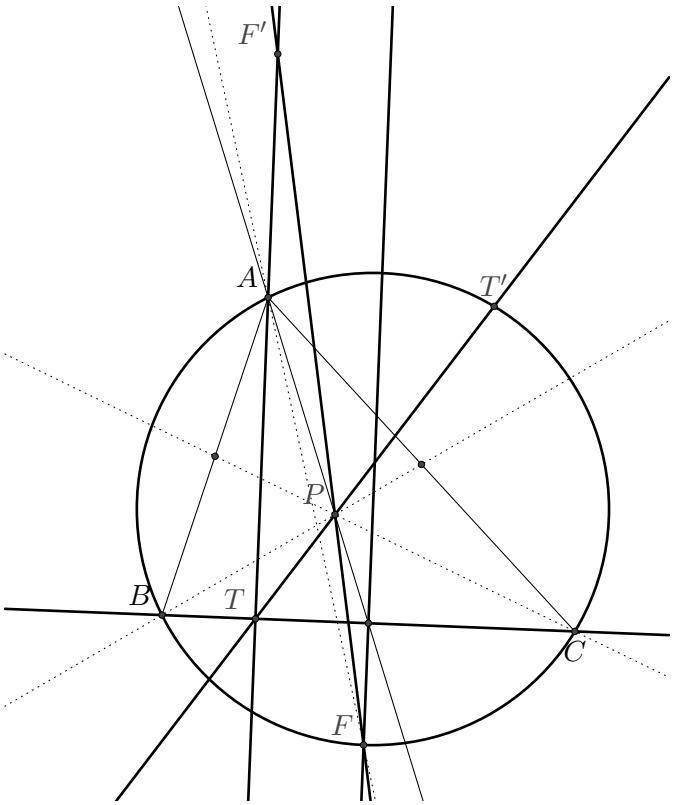
Megoldás:

A megoldás során végig T-vel jelöljük a megadott talppontot, és F-fel a megadott ívfelező pontot.

a) Szerkesszük meg a PT egyenest, ez legyen e. Legyen az F-en keresztül e-vel párhuzamos egynes, és a T-n átmenő, e-re merőleges egyenes metszéspontja D. Ekkor D a BC oldal felezőpontja. Tükrözzük P-t T-re, illetve D-re: a kapott pontok legyenek P' és P''. Ismert, hogy ekkor P' és P'' az ABC háromszög köréírt körén fekszik, ez egyszerű szögszámolással ellenőrizhető. P', F és P'' páronként különbözőek, mivel ABC nem egyenlőszárú, így megszerkesztve a $P'FP''$ kört ABC háromszög köréírt körét kapjuk, ezt elmetszve a PT és TD egyenesekkel az A, P', B és C pontokat kapjuk.

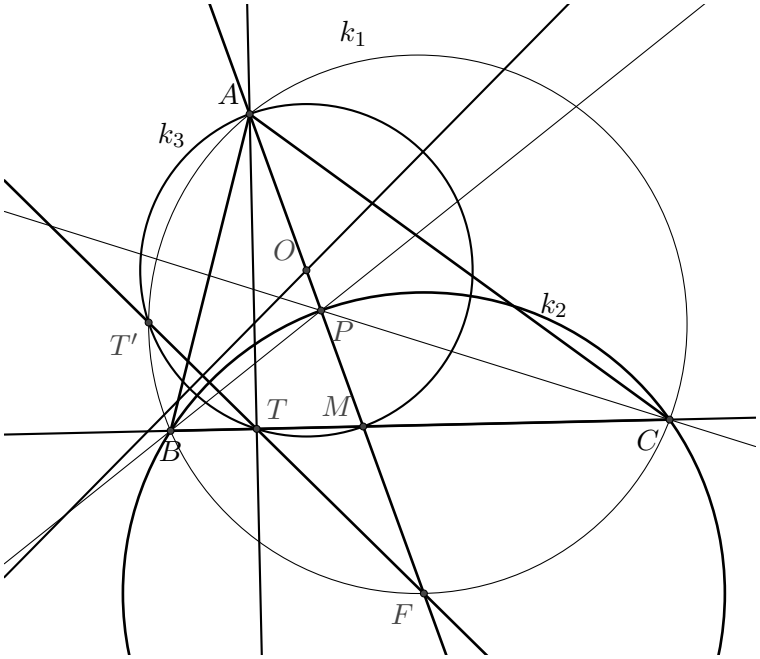


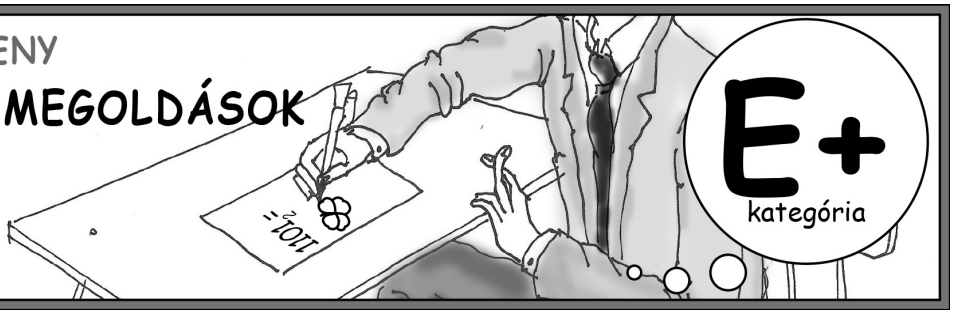
b) A megoldás során többször is ki fogjuk használni a tényt, hogy a súlypont a megfelelő súlyvonalakat, így ezek különböző vetületeit is $2:1$ arányban osztja. Előbbi tényből könnyen látszik, hogy a T' pont, amit a T pont P-re való -2-arányú nagyításával kapunk, az ABC háromszög köréírt körén fekszik, ráadásul megegyezik az A pont BC szakasz felezőmerőlegesére való tükörképével; valamint F', amit az F pont P-re való -2-arányú nyagításával kapunk, ráesik az AT egyenesre. Térjünk át a szerkesztésre. Az előbbiek szerinti F' és T' pontokat meg tudjuk szerkeszteni. Vegyük a TF' egyenes P-re való, $-1/2$-arányú nagyításával kapott egyenest! Ez éppen a BC szakasz felezőmerőlegese lesz; erre tükrözve T'-t, az előbbiek szerint A-t kapjuk. Mivel ABC háromszög nem egyenlőszárú, így $A \neq T'$, tehát tudjuk szerkeszteni az ABC háromszög köréírt körét, mivel három különböző pontját ismerjük; ezt elmetszve a TF' egyenesre T-ben állított merőlegessel, B-t és C-t kapjuk meg.



c) Megfigyelések: Legyen az ABC háromszög köréírt köre k_1. Ismert, hogy a B, P és C pontok egy F középpontú, k_2 körön fekszenek (szögszámítással könnyen ellenőrizhető). Legyen AF és BC egyenesek metszéspontja M. Legyen az AM átmérőjű kör k_3, középpontja O. Mivel T az A-ból húzott magasság talppontja, így az ATM háromszög derékszögű, így T rajta van k_3-on. Az FT egyenes k_3-mal való második metszéspontja legyen T'. Vegyük észre, hogy a k_2-re való inverzió k_1-et a BC egyenesbe viszi, így az M pont az A pontba megy, tehát ez az inverzió k_3-t önmagába viszi, emiatt T képe T'.

A szerkesztés: (Az elnevezések ugyanazok lesznek, mint a megfigyeléseknél). Szerkesszük meg k_2-t (ismerjük egy pontját, és a középpontját). Szerkesszük meg T'-t, T k_2-re vett inverz képét. Ekkor az FP egyenes és a TT' szakasz felezőmerőlegesének metszéspontja O, így meg tudjuk szerkeszteni k_3-at. Ekkor k_3 és az FP egyenes F-től távolabbi metszéspontja lesz A. Az AT-re T-ben merőleges állításával kapott egyenes és k_2 metszéspontjai lesznek a B és C pontok.





E+5. Legyen p egy prímszám és legyen $k > 1$ a $p-1$ egy osztója. Igazoljátok, hogy ha egy k-adfokú egész együtthatós polinomra teljesül, hogy az egész helyen felvett értékeinek p-vel való osztási maradékai között minden lehetséges érték (tehát $0, 1, \ldots, p-1$ mindegyike) előfordul, akkor ennek a polinomnak a főegyütthatója p-vel osztható.
Megjegyzés: Egy d-edfokú polinom főegyütthatója az x^d tag együtthatója.

Megoldás: A megoldás során végig modulo p számolunk, minden kongruencia modulo p van véve. Legyen $Q(x)$ a polinomunk. Tegyük fel, hogy $k \mid p-1$, $k > 1$ és Q felvesz minden értéket modulo p. Mivel $Q(x) \equiv Q(x+p)$, ezért elég az $x = 0, 1, 2, \ldots, p-1$ esetekre megnézni, hogy felveszi-e Q mind a p különböző maradékot.

Lemma:

$$\sum_{j=0}^{p-1} j^t \equiv \begin{cases} -1 & \text{ha } t = p-1 \\ 0 & \text{ha } t = 0, 1 \ldots p-2 \end{cases}$$

Bizonyítás: Ismert, hogy modulo p létezik g primitív egységgyök. Ha $t \neq p-1$, akkor mértani sor összegképletéből:

$$\sum_{j=0}^{p-1} j^t \equiv \sum_{j=0}^{p-2} g^{jt} \equiv \frac{g^{(p-1)t} - 1}{g^t - 1} \equiv 0$$

Ha $t = p-1$, akkor $x^t \equiv 1$, ha $x \not\equiv 0$ kis Fermat-tétel miatt. Tehát

$$\sum_{j=0}^{p-1} x^{p-1} \equiv p - 1 \equiv -1$$

Ezzel bebizonyítottuk a lemmánkat.

Most indirekten tegyünk fel, hogy Q főegyütthatója nem osztható p-vel. Legyen $c = \frac{p-1}{k}$, valamint legyen $R(x) = Q^c(x) = \sum_{i=0}^{p-1} b_i x^i$. Először is R-ben a b_{p-1} együttható nem 0 modulo p, mert Q-nak a főegyütthatója nem nulla és $b_{p-1} = a_k^c$.

Vegyük a következő összeget:

$$\sum_{j=0}^{p-1} R(j)$$

Mivel $k > 1$ és k osztója $p-1$-nek, így c $p-1$-nél kisebb pozitív egész. A feltevésünk alapján $Q(x)$ felvesz minden értéket modulo p, vagyis $Q(0), Q(1), \ldots Q(p-1)$ a $0, 1 \ldots p-1$ maradékok permutációja, tehát a szumma átírható a következő módon:

$$\sum_{j=0}^{p-1} R(j) = \sum_{j=0}^{p-1} Q^c(j) \equiv \sum_{j=0}^{p-1} j^c \equiv 0$$

Az utolsó kongruencia a lemmánkból következik. Valamint az R-re felírt szummát másik módon kibontva:

$$\sum_{j=0}^{p-1} R(j) = \sum_{j=0}^{p-1} \sum_{i=0}^{p-1} b_i j^i = \sum_{i=0}^{p-1} b_i \sum_{j=0}^{p-1} j^i \equiv -b_{p-1}$$

Ahol ismét használtuk a lemmánkat. Tehát $0 \equiv -b_{p-1}$, ami ellentmondás, mert korábban már megmutattok, hogy b_{p-1} nem lehet a 0 maradék.

Vagyis valóban Q főegyütthatója osztható p-vel.