Az 1572. feladatban[1] tetszés szerinti n páratlan oldalszám esetére nem döntöttük el, hogy a bélyegzővel előállított bűvös kövezet pándiagonális, azaz minden átlójában bűvös-e, vagy csak némely átlóiban, vagy hogy egyáltalán lehet-e a kövezetben bűvös négyzetet kijelölni a keret alkalmas elhelyezésével. Ezt és az ottani egyéb kérdéseket is más eljárással újra vizsgáljuk.

1. Valamivel kényelmesebb, ha a szokásos $1, 2, \ldots, n^2$ számok helyett az 1-gyel kisebb $0, 1, \ldots (n^2 - 1)$ számokat írjuk be bélyegzőnkre, mert ezek az n-alapú számrendszernek éppen az összes kétjegyű számai:

$$\overline{ab} = an + b,$$

ahol a-ra, b-re egyformán

$$0 \leqq a, b \leqq n - 1. \tag{1}$$

Pl. az 1572. feladat 1. ábráján az 1-estől jobbra fölfelé haladó bejegyzések helyére rendre ezek lépnek:

$$\overline{00},\ \overline{01},\ \overline{02},\ \ldots,\ \overline{0,\ n-2},\ \overline{0,\ n-1}.$$

2. Helyezzünk a lenyomatok papirosára szokásos koordináta-rendszert, origójának a $\overline{00}$ szám első lenyomatbeli példányát, tengelyirányoknak a sorok, ill. oszlopok irányát, hosszúságegységnek pedig egy kis mező oldalát véve. Legyen még a jobbra és a fölfelé mutató egységvektor $\mathbf{i}$, ill. $\mathbf{j}$, ekkor az előbbi számoknak (pontosabban az őket tartalmazó mezők középpontjainak) helyvektorai rendre

$$\mathbf{0}, \quad 2\mathbf{i} + \mathbf{j}, \quad 2(2\mathbf{i} + \mathbf{j}), \quad \ldots, \quad (n-1)(2\mathbf{i} + \mathbf{j}),$$

a $\overline{00}$-ból induló, jobbra lejtő bejegyzéseké

$$\mathbf{0}, \quad 2\mathbf{i} + \mathbf{j}, \quad 2(2\mathbf{i} + \mathbf{j}), \quad \ldots, \quad (n-1)(2\mathbf{i} + \mathbf{j}),$$

általában az $\overline{ab}$ szám első lenyomatbeli példányának helyvektora

$$a(2\mathbf{i} - \mathbf{j}) + b(2\mathbf{i} + \mathbf{j}) = 2(a + b)\mathbf{i} - (a - b)\mathbf{j},$$

és ezen szám minden további lenyomatbeli példányának helyvektora

$$(2a + 2b + g_1 n)\mathbf{i} + (-a + b + g_2 n)\mathbf{j} \tag{2}$$

alakú, ahol g_1, g_2 egészek (úgyszintén a tovább bevezetendő g_i $(i = 3, 4, \ldots)$ számok is). Mindezen alakok az összegek szempontjából ekvivalensek. Azt az alakot, amelyben a (2)-beli két koordináta 0 és $n - 1$ közé esik (a korlátokat beleértve), az $\overline{ab}$ szám redukált helyvektorának nevezzük.

3. Megmutatjuk, hogy a lenyomatok előírt megismétléseivel sohasem áll elő két szám átfedése, más kifejezéssel: az $\overline{ab}$ és $\overline{cd}$ számok redukált helyvektora csak akkor egyező, ha $a = c$ és $b = d$.

Az egyezés feltétele a vektorok végpontjaihoz tartozó koordináták egyenlősége:

$$\begin{aligned} 2a + 2b + g_1 n &= 2c + 2d + g_3 n, \\ -a + b + g_2 n &= -c + d + g_4 n, \end{aligned}$$

és ha ez teljesül, akkor

$$\begin{aligned} 2(a - c) + 2(b - d) &= (g_3 - g_1)n = g_5 n, \\ -(a - c) + (b - d) &= (g_4 - g_2)n = g_6 n. \end{aligned} \tag{3}$$

Mivel n páratlan, azért g_5 páros, $g_5 = 2g_7$, és így az elsőből

$$(a - c) + (b - d) = g_7 n, \tag{4}$$

amit (3)-hoz hozzáadva és a legutóbbi meggondolást megismételve

$$\begin{aligned} 2(b - d) &= (g_6 + g_7)n = 2g_8 n, \\ b - d &= g_8 n. \end{aligned}$$

Ámde két számjegyünk különbségére

$$-(n - 1) \leqq b - d \leqq n - 1,$$

[1]Lásd ezen számban, 103. o.

és e korlátok közt n-nek egyetlen többszöröse 0, így $b = d$. – Ugyanígy adódik (3)-ból és (4)-ből kivonással $a = c$, amint állítottuk.

4. A bélyegző által előállított kövezetben sorok, oszlopok, jobbra lejtő vagy emelkedő átlók (röviden fő-, ill. mellékátló) mentén összekerülő számok kapcsolatának meghatározása céljára kérdezzük általánosan: mely szám áll egy $\overline{cd}$ számból (pontosabban mezejének középpontjából) kiinduló $x\mathbf{i} + y\mathbf{j}$ vektor végpontjában, ahol $0 \leqq x,\ y \leqq n-1$. Az eredményt $(x,\ y) = (1;\ 0)$-ra, majd $(\mathbf{x},\ 0)$-ra alkalmazva a $\overline{cd}$-től jobbra az x-edik (más szóval balra az $n-x$-edik) mezőn álló számot fogjuk kapni; hasonlóan $(0;\ 1)$ és $(0;\ y)$ esetén a vele egy oszlopban álló számokat, $(x,\ x)$ és $(x,\ n-x)$ esetén pedig a vele egy-egy átlós vonalon állókat, hiszen $(x,\ n-x)$ ekvivalens $(x,\ -x)$-szel.

A keresett számot $\overline{ab}$-vel jelölve, $\overline{ab}$ és $\overline{cd}$ alkalmas lenyomataihoz tartozó helyvektorok különbségére fennáll

$$\{(2a+2b+g_1n)\mathbf{i} + (-a+b+g_2n)\mathbf{j}\} -$$
$$-\{(2c+2d+g_3n)\mathbf{i} + (-c+d+g_4n)\mathbf{j}\} = x\mathbf{i} + y\mathbf{j},$$

vagy rövidítésül bevezetve az $a-c = a^*$, $b-d = b^*$ jelöléseket:

$$\big(2a^* + 2b^* + g_5n\big)\mathbf{i} + \big(-a^* + b^* + g_6n\big)\mathbf{j} = x\mathbf{i} + y\mathbf{j},$$

amiből a^*-ra és b^*-ra az alábbi egyenletrendszert kapjuk. (Megjegyezzük, hogy itt $-(n-1) \leqq a^*,\ b^* \leqq (n-1)$ hiszen $a < c$ és $b < d$ is lehetséges, továbbá, hogy a^*-on, b^*-on felül tulajdonképpen a g számok is ismeretlenek.)

$$2a^* + 2b^* + g_5n = x,$$
$$-a^* + b^* + g_6n = y.$$

A második egyenletnek előbb a (-2)-szeresét, majd a 2-szeresét az elsőhöz adva

(5) $$a^* = \frac{x-2y+g_7n}{4}, \qquad b^* = \frac{x+2y+g_8n}{4}.$$

Innen a^*-ra és b^*-ra mindig kapunk egész megoldást, mert g_7 és g_8 helyére a 0, 1, 2, 3 értékeket téve, n-szeresüknek a 4-gyel való osztás utáni maradéka valamilyen sorrendben 0, 1, 2 és 3, ennélfogva bármennyi az $x-2y$ és $x+2y$ ugyanilyen osztásánál fellépő maradék, megválasztható g_7 is, g_8 is úgy, hogy a^*, b^* értéke egész legyen. (Valóban, ha $n = 4k+1$, úgy $g = 0, 1, 2, 3$ esetén gn maradéka rendre 0, 1, 2, 3, ha pedig $n = 4k+3$, akkor 0, 3, 2, 1.) Az így megválasztott g értékeket szükség esetén 4-gyel növelve, csökkentve elérhetjük, hogy a^*, b^*-ra teljesül (1).

Bemutatunk egy számpéldát, ami az 1572. feladat 3. ábráját felhasználva olyan lehetőségeket is megvilágít, ha a talált a^* vagy b^* értékkel $a = c + a^* \geqq n$, vagy $b = d + b^* \geqq n$ adódik.

Legyen $n = 9$, $x = 2$, $y = 7$, ekkor g_7, g_8 helyén megfelel 4, ill. 0, és így

$$a^* = (2 - 14 + 4\cdot 9)/4 = 6, \qquad b^* = (2+14)/4 = 4,$$

megegyezésben a mondott ábrával. Ugyanis pl. a $\overline{cd} = \overline{04}$ számnak megfelelő (1-gyel növelt, tízes rendszerbeli) 5-ös számtól, a keret alatti előfordulásától jobbra $x = 2$-t, fölfelé $y = 7$-et lépve 63-at találjuk, vagyis az 58-cal nagyobb számot, és ez a növekedés a 9-es számrendszerben $58 = 6\cdot 9 + 4 = \overline{64}$, a talált $\overline{a^*b^*}$.

Az ábra több más $\overline{cd}$ számához is az 58-cal nagyobb számot találjuk, tőle jobbra 2-t és fölfelé 7-et, vagy ami ugyanaz, lefelé is 2-t lépve, amíg csak a megnövelt $(c+6)\cdot 9 + (d+4)$ szám egyik jegye sem éri el vagy lépi túl a 9-et. Ilyen esetben viszont az $a = c + a^* = c + 6$, ill. $b = d + b^* = d + 4$ számjegy helyére a 9-cet kisebb $c-3$, ill. $d-5$ számjegy lép, ami (4)-ből $g_7 - 4 = 0$, ill. $g_8 - 4 = -4$ mellett adódó $a^* = -3$-nak, $b^* = -5$-nek felel meg. Ezek a változások külön-külön $9\cdot 9 = 81$, ill. $9\cdot 1 = 9$, együtt pedig $81 + 9 = 90$ csökkenést okoznak az 58 növeléssel várt értékhez képest, pl. 28-hoz képest (aminek $27 = \overline{30}$ felel meg, és itt $c + 6 = 9$) $28 + 58 - 81 = 5$-öt, 6-hoz képest $6 + 58 - 9 = 55$-öt, 33-hoz képest $(32 = \overline{35})$ $33 + 58 - 90 = 1$-et találjuk a mondott helyen.

Megegyezésben állnak ezek a tények azzal, hogy ha a feladat bélyegzőjét kiegészítenénk az n^2-nél nagyobb egész számokkal, éspedig az adott előírás szerint, pl. az (n^2+1)-et beírnánk az $(n-1)n+1$-től jobbra lefelé 2-t, ill. 1-et lépve található mezőre, akkor n^2+1 lenyomatai átfednék az 1-es szám lenyomatait, hiszen már magán a bélyegzőn a sorszámok különbsége a két szám oszlopaira nézve $2n$, soraira nézve n lenne. Fordítva úgyis mondhatjuk ezt, hogy egy m szám helyén olvashatunk $m + n^2$-et is, $m + gn^2$-et is.

5. Az $(x,\ y)$ pár előre közölt speciális értékeivel (5)-ből bármely páratlan n esetére táblázatunk eredményeit kapjuk a^*-ra és b^*-ra, vagyis arra, hogy a tetszés szerinti $\overline{cd}$ számtól jobbra, ill. jobbra fölfelé, ill. balra fölfelé, ill. fölfelé álló szám első, ill. második számjegye mennyivel nagyobb, mint c, ill. d. Az első három sávban – ahol x páratlan – az eredmény más és más aszerint, hogy az n alakja $4k+1$, ill. $4k+3$.

A táblázat, alsó és felső sávja alapján megmutatjuk, hogy a kövezeten bárhol letéve a keretet, bármelyik sor (vagy oszlop) összege ugyanannyi. Abból adódik majd ez, ha belátjuk, hogy az egy-egy sorban, oszlopban előforduló n szám számjegyei között az n-értékű helyen is, az 1-értékű helyen is minden fajta számjegy pontosan egyszer fordul elő, és így a

$$0 + 1 + 2 + \ldots + (n-2) + (n-1) = s$$

jelöléssel a sor összege

$$s \cdot n + s = s(n+1) = \frac{(n-1) \cdot n}{2} \cdot (n+1) = \frac{n(n^2-1)}{2};$$

ami pedig a kövezet összes számai összegének,

$$0 + 1 + 2 + \ldots + \left(n^2-2\right) + \left(n^2-1\right) = \frac{n^2\left(n^2-1\right)}{2}$$

-nek n-edrésze.

Felhasználjuk, hogy a talált a^*, b^* értékek mindegyike relatív prím a megfelelő n-hez képest, nincs 1-nél nagyobb közös osztójuk. Pl. $n = 4k+1$-nek és $a^* = 3k+1$-nek minden közös osztója egyszersmind különbségüknek, k-nak is osztója. Viszont $3k+1$-nek és k-nak minden közös osztója hasonlóan osztója $3k+1-k-k-k = 1$-nek is, tehát nem nagyobb 1-nél.

Legyen az n-edrendű kövezetből az $n \times n$ mezős kerettel kijelölt négyzet egy sorában az első számnak pl. az első számjegye c, ekkor a sor n számának első számjegye rendre

$$(6) \qquad c, \quad c + a^*, \quad c + 2a^*, \quad c + 3a^*, \ \ldots, \ c + (n-1)a^*$$

(ill. ahol ez az érték nagyobb, mint n, ott helyette az n-nel való osztásánál fellépő maradék veendő). Mármost ellentmondásra jutunk annak föltevésével, hogy e számjegyek közül kettő megegyező. Ha ugyanis az (r_2+1)-edik megegyeznék a korábbi (r_1+1)-edikkel – ahol $1 \leqq r_1 + 1 < r_2 + 1 \leqq n$, azaz $0 \leqq r_1 < r_2 \leqq n-1$–, vagyis

$$c + r_2 a^* - g_2 n = c + r_1 a^* - g_1 n$$

volna, ebből

$$(r_2 - r_1)a^* = (g_2 - g_1)n = g_3 n,$$

következnék, vagyis hogy a bal oldal osztható n-nel. Ámde a^*-nak nincs közös tényezője n-nel, tehát $r_2 - r_1$ osztható vele,

$$r_2 - r_1 = g_4 n, \qquad \text{holott} \qquad 0 < r_2 - r_1 < n-1.$$

Mindez ugyanígy érvényes a b^* értékekre.

A sor- és oszlopösszegekre vonatkozó állításunkat ezzel bebizonyítottuk. Eredményünk így is kimondható: ha a bélyegzővel készült kövezeten bárhol körülkeretezünk egy $n \times n$ mezős négyzetet, majd ennek minden számából a két számjegyet két ilyen négyzet megfelelő mezőpárjaira külön-külön írjuk fel, ezek minden sorában is, minden oszlopában is a $0, 1, \ldots, (n-1)$ számjegyek mindegyike pontosan egyszer fordul elő. Így szemléletesebb az összegek egyezésének belátása. Az ilyen elrendezéseket *Euler* nyomán *latin négyzet*eknek szokás nevezni.

6. Ha sikerülne ugyanezeket belátni az átlós irányú vonalak szám n-eseire ez azt bizonyítaná, hogy a bélyegzővel képezett n-edrendű kövezet pándiagonális, minden átlóján bűvös. Tüstént látjuk, hogy ez igaz minden olyan (páratlan) n-re, amely nem osztható 3-mal. Ugyanis a táblázatunk 2. és 3.

x, y	n=4k+1	n=4k+3
(1; 0) jobb szomszéd	$a^* = b^* = 3k+1$ (g=3) $= \frac{3n+1}{4}$ mindkét esetben $a^* - b^* = 0$	$a^* = b^* = k+1$ (g=1) $= \frac{n+1}{4}$
(1; 1) jobb felső	$a^* = k = \frac{n-1}{4}$, (relatív prím) $b^* = k+1 = \frac{n+3}{4}$	$a^* = 3k+2$, $= \frac{3n-1}{4}$, (rel.pr.) $b^* = 3k+3$ $= \frac{3n+3}{4}$
(-1; 1) bal felső	$a^* = 3k$ $= \frac{3n-3}{4}$ $b^* = 3k+1$ $= \frac{3n+1}{4}$ (rel. pr)	$a^* = k$ $= \frac{n-3}{4}$ $b^* = k+1$ $= \frac{n+1}{4}$ (rel. pr.)
(0; 1) felső	n alakjától függetlenül (vagyis $n = 2k+1$-re) $a^* = k = \frac{n-1}{2}$, $b^* = k+1 = \frac{n+1}{2}$,	$a^* + b^* = n$

sávjában talált a^* b^* értékek közül $n = 4k+1$ oszlopában $a^* = k$ és $b^* = 3k+1$ valamint $n = 4k+3$ oszlopában $a^* = 3k+2$ és $b^* = k+1$ a fentiekhez hasonlóan mindenesetre relatív prímek n-hez. A további négy értéknek pedig nem lehet más közös osztója a megfelelői n-nel, mint a 3-as szám, hiszen pl. $b^* = k+1$ esetében (az $(1;1)$ sávban)

$$4k + 1 - (k+1) = 3k,$$

és itt a k tényező relatív prím $4k+1$-hez, tehát a mondott n-ekre $3k$ is, $k+1$ is relatív prím hozzá. Ugyanezek állnak $n=4k+1$ oszlopában $a^*=3k$-ra és $n=4k+3$ oszlopában $b^*=3k+3$-ra, $a^*=k$-ra. A tekintetbe vett n-ekre tehát a jegyek szétválasztásával képezett két négyzet *átlós latin négyzet,* átlós összegei is egyezők, a keret bárhol való elhelyezése esetében. Ezt láttuk az 1572. feladatban $n=5$ és 7 esetében.

Ha viszont $n=3g$, akkor az utoljára vizsgált négy a^*, b^* kifejezés osztható 3-mal, (6)-nak már a $(g+1)$-edik tagja egyezik az elsővel, c-vel, mert ($a^*=3a^{**}$ jelöléssel)

$$c+ga^*=c+3ga^{**},$$

és tovább tagról-tagra ismétlődik a megegyezés. A kettéválasztott számjegyek négyzeteinek tehát ilyenkor nincs meg mindkét átlós irányban a „latin" tulajdonsága (az egyik irányban azonban megvan). Meg lehet mutatni, hogy ilyenkor mindkét irányban minden harmadik átlóban megfelelő az összeg, a közbülsőkben viszont attól eltér, ezt láttuk az 1572. feladatban $n=9$ esetében. $n=3$ mellett pedig az adódik, hogy a lényegében egyetlen 3-adrendű bűvös kövezet nem pándiagonális. Ezzel a bélyegzőnkkel készített kövezetek pándiagonálisságának kérdését megválaszoltuk.

Megjegyezzük, hogy legutóbbi megállapításunk korántsem jelenti azt, hogy 3-mal osztható rendszám esetén nem létezik pándiagonális kövezet. Az idézett 3. ábrából ($n=9$) pándiagonális bűvös négyzet – tehát kövezet is – képezhető a következő változtatásokkal: számait rendre 1-gyel csökkentjük és átírjuk a 9 alapú számrendszerbe, ezután a számjegyekben három alkalmas cserét hajtunk végre, pl. minden

$$0,\ 1; \qquad 3,\ 5 \qquad 7,\ 8$$

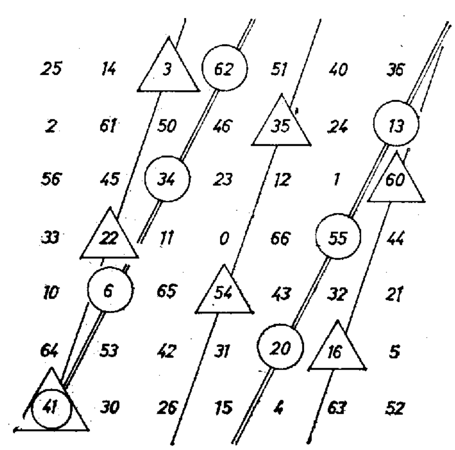
számjegy helyére a 9-es és 1-es értékű helyen egyaránt a következőt írjuk:

$$1,\ 0; \qquad 5,\ 3; \qquad 8,\ 7.$$

A számok növekvő rendjét tekintve ez már nem kétféle lépéssel, pecsételéssel képezett alakzat. Ebből is látható, hogy vannak más típusú bűvös négyzetek is. Már az 5-ödrendűekre vonatkozóan sem ismeretes ez ideig az összes bűvös négyzetek száma.

7. Az olvasóra hagyjuk annak átgondolását, hogy bélyegzőnk „jobbra 2-t és fölfelé vagy lefelé 1-et" lépései azért vezethettek *minden* páratlan n esetén soraikban és oszlopaikban latin négyzetekre bontható négyzetekhez – és az ezekből folyó eredményekhez, –, mert a lépések 2-es, ill. 1-es komponense minden páratlan n-hez képest relatív prím. Megfelelne helyettük lépéskomponensként minden páratlan n esetére bármely 2^e mezőnyi eltolódás (vízszintesen is, függőlegesen is), ahol $e \geqq 0$, egész szám – azonban természetesen a bélyegző 1-eséről a 2-esre és az $n+1$-esre vivő lépésnek és a komponensek arányának is különbözőnek kell lennie.

8. Az elmondottak gyakorlásául ajánljuk annak vizsgálatát, hogy az így előállított kövezeteken a figyelembe vett $x\mathbf{i}+y\mathbf{j}$ vektoroktól különböző lépéseket n-szer ismételve, találhatunk-e más, a bűvös állandóval egyező összegeket. Indításul bemutatjuk az $n=7$-re és a 7-es számrendszerben készült ábrát, melyen $\overline{00}$-tól a $\overline{01}$ szám $2\mathbf{i}+\mathbf{j}$-re, az $\overline{10}$ pedig $4\mathbf{i}-\mathbf{j}$-re áll (meg lehet mutatni a fenti eljárással a kövezet felírása nélkül előre is, hogy pándiagonális lesz), és pl. a kis körökbe foglalt ($\mathbf{i}+2\mathbf{j}$ lépéssel kapott) számok összege is, a kis háromszögbe foglaltak is egyenlő a bűvös állandóval, mert két összekötött szám jegyei mind a 7-es, mind az 1-es helyen különbözők.



Ebben azonban az is lényeges, hogy itt n-ként prímszámot vettünk. A megjelölt számhetesek persze sok más „nagyobb" lépéssel is összejönnek, pl. a háromszögbe foglaltak $2\mathbf{i}-\mathbf{j}$-vel, $3\mathbf{i}+2\mathbf{j}$-vel, $2\mathbf{i}+6\mathbf{j}$-vel s i. t.