Változások a KöMaL-nál

Az Oktatási Minisztérium anyagi támogatásával sikerült a lapot kibővíteni, színesebbé tenni, valamint a szeptemberi számunkat minden középiskolába ingyen eljuttatni.

Újraindítottuk a számítástechnika rovatot.

Főszerkesztőváltás történt a lapunknál. Oláh Vera 1993 szeptemberétől 2001 júliusáig volt a KöMaL főszerkesztője. Munkáját dicséri, hogy vezetése alatt sokat fejlődött a KöMaL, és mégis sikerült megőrizni hagyományait. Az új főszerkesztő Nagy Gyula.

Reméljük, hogy azok is, akik most először veszik kézbe lapunkat, kedvet kapnak az olvasásához, és minél több diák fog bekapcsolódni valamelyik pontversenyünkbe.

Minden Olvasónknak jó tanulást, szórakozást és eredményes munkát kíván a szerkesztőség nevében

Nagy Gyula

Beszámoló a 42. Nemzetközi Matematikai Diákolimpiáról

Az idei Nemzetközi Matematikai Diákolimpiát Washingtonban, az Egyesült Államok fővárosában rendezték meg július 1. és 14. között 83 ország 473 diákjának részvételével. Az országok általában hattagú csapatokkal vettek részt, ha a csapatlétszám ennél kisebb volt, az alábbi felsorolásban az országnév után zárójelben jelzem a versenyzők számát. A résztvevők listája:

Albánia (5), Amerikai Egyesült Államok, Argentína, Ausztrália, Ausztria, Azerbajdzsán (3), Belgium, Belorusszia, Bosznia-Hercegovina, Brazília, Bulgária, Ciprus, Csehország, Dánia, Dél-Afrika, Dél-Korea, Ecuador, Észtország, Finnország, Franciaország, Fülöp-szigetek, Görögország, Grúzia, Guatemala (3), Hollandia, Hongkong, Horvátország, India, Indonézia, Irán, Írország, Izland, Izrael, Japán, Jugoszlávia, Kanada, Kazahsztán, Kína, Kirgizisztán (5), Kolumbia, Kuba, Kuvait (4), Lengyelország, Lettország, Litvánia, Luxemburg (2), Macao, Macedónia, Magyarország, Malajzia, Marokkó, Mexikó, Moldova (5), Mongólia, Nagy-Britannia, Németország, Norvégia, Olaszország, Oroszország, Örményország (5), Paraguay (5), Peru, Portugália, Románia, Spanyolország, Sri Lanka (4), Svájc, Svédország, Szingapúr, Szlovákia, Szlovénia, Tajvan, Thaiföld, Törökország, Trinidad és Tobago, Tunézia, Türkmenisztán (5), Új-Zéland, Ukrajna, Uruguay (2), Üzbegisztán, Venezuela (5), Vietnam.

A versenyen szokás szerint mindkét napon négy és fél óra alatt 3-3 feladatot kellett megoldani. (A feladatokat alább közöljük.) Mindegyik feladat helyes megoldásáért 7 pont járt, így egy versenyző maximális teljesítménnyel 42 pontot szerezhetett. (Ez egyébként négy versenyzőnek sikerült: két kínainak és két amerikainak.)

Idén a feladatok meglehetősen nehéznek bizonyultak, ennek megfelelően az egyes díjak ponthatára elég alacsony volt. Aranyérmet 30–42 ponttal, ezüstérmet 20–29 ponttal, bronzérmet pedig 11–19 ponttal lehetett szerezni.

A magyar csapatból

Harangi Viktor (Fazekas M. Főv. Gyak. Gimn., 11. o.t.) 22 ponttal,

Csóka Endre (Debrecen, Fazekas M. Gimn., 10. o.t.) pedig 21 ponttal ezüstérmet, míg

Kovács Erika (Fazekas M. Főv. Gyak. Gimn., 11. o.t.) és

KöMaL – 2001/6 MAT0106 cianmagentayellowblack2002. június 19. – 8:52 (1. lap)

Vörös László (Győr, Révai M. Gimn., 12. o.t.) egyaránt 19 ponttal,

Csikvári Péter (Fazekas M. Főv. Gyak. Gimn., 11. o.t.) pedig 14 ponttal bronzérmet nyertek.

A hatodik versenyző,

Horváth Illés (Fazekas M. Főv. Gyak. Gimn., 11. o.t.) csak kevéssel maradt le a bronzéremről.

A csapat vezetője *Pelikán József* (ELTE, Algebra és Számelmélet Tanszék), helyettes vezetője *Dobos Sándor* (Fazekas M. Főv. Gyak. Gimn.) volt.

Az országok (nem-hivatalos) pontversenyét Kína toronymagasan nyerte. Magyarország idén a 21. lett, ami rosszabb, mint az évek óta megszokott eredmények. Tudomásul kell azonban venni, hogy a mezőny egyre erősebb, és sok ország komoly összegeket áldoz a versenyzők felkészítésére.

Következzék a csapatverseny első 30 helyezettjének listája, pontszámaik feltüntetésével:

1. Kína 225, 2–3. Oroszország és USA 196, 4–5. Bulgária és Dél-Korea 185, 6. Kazahsztán 168, 7. India 148, 8. Ukrajna 143, 9. Tajvan 141, 10. Vietnam 139, 11. Törökország 136, 12. Belorusszia 135, 13. Japán 134, 14. Németország 131, 15. Románia 129, 16. Brazília 120, 17. Izrael 113, 18. Irán 111, 19–20. Hongkong és Lengyelország 107, 21. Magyarország 104, 22–23. Argentína és Thaiföld 103, 24. Kanada 100, 25. Ausztrália 97, 26. Kuba 92, 27. Üzbegisztán 91, 28. Franciaország 88, 29. Szingapúr 87, 30. Görögország 86.

A versenyzők felkészítésében Dobos Sándor mellett oroszlánrészt vállalt *Reiman István*, aki ezt a munkát már több mint 40 éve csinálja. Ezúton szeretnék köszönetet mondani neki.

Az egyes versenyzők tanárai a következők voltak:

Csikvári Péter: *Fazakas Tünde, Táborné Vincze Márta*

Csóka Endre: *Balázs Tivadar, Pósa Lajos, Reiman István, Páles Zsolt*

Harangi Viktor: *Fazakas Tünde, Táborné Vincze Márta, Pósa Lajos*

Horváth Illés: *Fazakas Tünde, Táborné Vincze Márta*

Kovács Erika: *Fazakas Tünde, Táborné Vincze Márta, Pósa Lajos*

Vörös László: *Zábrádiné Schmierer Emília, Zsebők Ottó*

A versenyről elmondható, hogy összességében jól rendezett volt. A vendéglátók kirándulásokat szerveztek a résztvevőknek (diákoknak többet, tanároknak kevesebbet). A záróünnepség a John F. Kennedy Kulturális Központban zajlott, aminek impozáns, új épülete közvetlenül a Potomac folyó partján fekszik.

A záróünnepség fényét nagymértékben emelte, hogy az aranyérmeseknek a díjat a világhírű matematikus, Andrew Wiles (a Fermat-tétel bizonyítója) adta át. A magyar csapatnak a záróbanketten sikerült megörökíttetnie magát Andrew Wiles társaságában. A fényképet a belső borítón közöljük.

A jövő évi diákolimpiát Skóciában, Glasgow-ban rendezik július 18. és 31. között.

Pelikán József

A 42. Nemzetközi Matematikai Diákolimpia feladatai

Első nap

1. Legyen az ABC hegyesszögű háromszög körülírt körének középpontja O. Legyen P az A-ból induló magasságvonal talppontja a BC oldalon.

Tegyük fel, hogy $BCA\sphericalangle \geq ABC\sphericalangle + 30^\circ$.

Bizonyítsuk be, hogy $CAB\sphericalangle + COP\sphericalangle < 90^\circ$.

2. Bizonyítsuk be, hogy

$$\frac{a}{\sqrt{a^2+8bc}}+\frac{b}{\sqrt{b^2+8ca}}+\frac{c}{\sqrt{c^2+8ab}}\geq 1$$

minden a, b, c pozitív valós számra.

3. Egy matematikaversenyen 21 lány és 21 fiú vett részt.

- Mindegyik versenyző legfeljebb hat feladatot oldott meg.
- Mindegyik fiúhoz és mindegyik lányhoz van legalább egy olyan feladat, amelyet mindketten megoldottak.

Bizonyítsuk be, hogy van olyan feladat, amelyet legalább három lány és legalább három fiú megoldott.

Második nap

4. Legyen n egy 1-nél nagyobb páratlan egész, k_1, k_2, $\ldots$, k_n pedig adott egészek. Az 1, 2, $\ldots$, n számok mind az $n!$ darab $a=(a_1,a_2,\ldots,a_n)$ permutációjára legyen

$$S(a)=\sum_{i=1}^{n} k_i a_i.$$

Bizonyítsuk be, hogy van két olyan b és c permutáció, amelyekre $b\neq c$, és $n!$ osztója $(S(b)-S(c))$-nek.

5. Az ABC háromszögben legyen AP a $BAC\sphericalangle$ szögfelezője, ahol P a BC oldalon van, BQ pedig az $ABC\sphericalangle$ szögfelezője, ahol Q a CA oldalon van. Tudjuk, hogy $BAC\sphericalangle = 60^\circ$ és hogy $AB+BP=AQ+QB$.

Mik az ABC háromszög szögeinek lehetséges értékei?

6. Legyenek a, b, c, d egészek, amelyekre $a>b>c>d>0$. Tegyük fel, hogy

$$ac+bd=(b+d+a-c)(b+d-a+c).$$

Bizonyítsuk be, hogy $ab+cd$ nem prímszám.

❄

Figyelem! Az idei Kürschák József Matematikai Tanulóverseny 2001. október 12-én pénteken 14 órától kerül megrendezésre. További információt a Bolyai János Matematikai Társulattól lehet kérni a 201-6874-es telefonszámon.

Cardano és a kriptográfia
A rejtjelező-rácsok matematikája

Girolamo Cardano születésének 500. évfordulójára ajánlva

Bevezetés

Éppen csak elkezdődött a XVI. század, amikor Girolamo Cardano (1501–1576) olasz matematikus, fizikus, filozófus, orvos, (egyszóval igazi reneszánsz tudós) megszületett. 1545-ben megjelent munkája, az Ars Magna képleteket tartalmaz az általános alakú harmadfokú egyenlet gyökeire. Az utókor számára Cardano nevével általában ezen eredményei kapcsolódnak össze, pedig a mai napig kétséges, hogy ezeket a képleteket valóban ő fedezte-e fel.[1]

Ugyanakkor kevesen ismerik Cardanot mint a XVI. századi kriptográfia egyik legjelentősebb alakját. Ez nem annyira meglepő, hiszen természeténél fogva a kriptográfiát (a titkosírást, vagy rejtjelezést) „zárt ajtók mögött” művelték. Királyok, hadvezérek szigorúan bizalmas levelezését bonyolították különböző módszerekkel titkosított levelekkel. Mivel a bonyolultabb rejtjelezési módszerek és főleg azok megfejtése legtöbbször komoly matematikai ismereteket igényel, így érthető, hogy többnyire neves matematikusok nevéhez fűződik a kriptográfia elméleti alapjainak megteremtése.

Cardano egy akkor egészen új rejtjelezést dolgozott ki, amelyet ma Cardano-rácsnak neveznek. A Cardano-rács sikerét mi sem bizonyítja jobban, mint hogy 400 évvel később, a XX. század közepén, a nyugatnémet hírszerző szerv (BND = Szövetségi Információs Szolgálat) még használta.

A következőkben rövid történeti áttekintés után bemutatjuk a Cardano-rács alapgondolatát, majd annak több irányú általánosítását és néhány matematikai tulajdonságát.

Fáklyatávíró és intervallum rejtjelezés

Cardano behatóan tanulmányozta az előző korok rejtjelezési technikáit egészen az ókorig visszatekintve. Így akadt rá az i.e. II. században élt Polübiosz nevű görög történész leírására, amelyben egy érdekes és az addig megszokottól merőben különböző eljárást ír le.

[1] A matematika-történészek szerint egy bizonyos Scipione del Ferro (1465–1526) megtalálta az általános alakú harmadfokú egyenlet megoldását, melyet közölt kollégáival. Ez 1515 körül történhetett, amikor Olaszországban gyakran tartottak matematikai versenyeket. Ferro egyik kollégája azt javasolta Niccolo Tartaglia (1500–1557) akkori nagyképzettségű matematikusnak, hogy oldjanak meg harmadfokú egyenleteket. Tartaglia a kijelölt határidő előtt megoldotta az egyenleteket, módszerét azonban titokban tartotta. Cardano kitartó érdeklődésére elmondta neki a megoldást, de megeskette, hogy hallgat róla. Cardano azonban nem tartotta meg esküjét és 1545-ben az Ars Magna-ban ismertette a harmadfokú egyenlet megoldásának módszerét. Így kezdődött a heves, ádáz vita Tartaglia és Cardano között, amelynek végére a matematika-történet a mai napig nem tudott pontot tenni.

Polübiosz fáklyatávírója

Készítsük el az *1. ábrán* látható 5 sorból és 5 oszlopból álló táblázatot.

	1.	2.	3.	4.	5.
1.	a	f	m	r	y
2.	b	g	n	s	z
3.	c	h	o	t	
4.	d	i	p	u	
5.	e	l	q	x	

1. ábra

Az üzenetet küldőnél 10 fáklya van, 5-5 mindkét kezénél. Az üzenetet betűnként küldi el úgy, hogy a bal kezével annyi fáklyát emel föl, ahányadik sorban, a jobb kezével pedig annyit, ahányadik oszlopban helyezkedik el a küldendő betű a táblázatban. Például a „t” betű esetén a bal kezében 3, míg a jobb kezében 4 fáklya van.

„Ezt a módszert Cleoxenusz és Demokritosz találta ki, de én tökéletesítettem.” – írja büszkén Polübiosz.

Joggal lehetett büszke, mert bár a fáklyával történő üzenet továbbítást már a régi kínaiak[2] is ismerték, az ő rendszere volt az első táblázatba foglalt rejtjelező eljárás, amelynek nagy előnye, hogy — a módszer megváltoztatása nélkül — könnyen cserélhető a táblázatbeli ABC, illetve a táblázatbeli betűk elhelyezése.

Kérdés: *A fenti* 22 *betűs ABC betűi hányféleképpen helyezhetők el a táblázatban? És ha kitöltjük mind a* 25 *betűhelyet a táblázatban?*

Ezt az eljárást fejlesztette tovább Cardano úgy, hogy az ABC betűinek megadásához csak két fáklyát használt (egyet-egyet mindkét kézben) és a fáklyák elhelyezkedése, illetve egymáshoz való viszonya kódolta a megfelelő sort és oszlopot.

Ez a módszer adhatta Cardanonak az ötletet, hogy megalkossa a táblázaton alapuló titkosírás két nagy családját. Az egyik az „intervallum rejtjelezés”, amelyben az üzenet titkosítása a betűk közötti távolságokon alapul. A módszert az egyszerűség kedvéért egy példán mutatjuk be. Készítsük el a *2. ábrán* látható táblázatot.

Á	a	e	r	n	c	b
B	i	o	d	l	g	q
C	u	s	m	f	p	t

2. ábra

Legyen az üzenet: *csacsi*. (A lépéseket a *3. ábrákon* követhetjük.) Írjuk az üres levélpapír bal felső sarkába az Á, B, C betűk bármelyikét. Ez csupán a szöveg kezdetét jelöli (C). Helyezzük a táblázat üres négyzetét a megjelölt betűre, majd a *csacsi* első betűjét (c) tartalmazó, nagybetűvel jelzett mező jelét (Á) írjuk a papírra pontosan a c betű fölé (lásd *3.a) ábra*). Most helyezzük a táblázat üres négyzetét az utoljára felírt nagybetűre, és keressük ki a táblázatból a következő betűt, az „s”-et. Ezzel ugyanúgy járunk el, mint az előzőkben, azaz a táblázatbeli *s* betű fölé írjuk a papírra a mező jelét (C). A fenti lépéseket addig folytatjuk, amíg van hely a levélpapír adott sorában, majd a legelső lépést megismételve új sort nyitunk, és az eljárást folytatjuk a küldendő szöveg végéig. A megfejtő dolgát azzal nehezítjük meg, hogy az üresen maradt helyeket tetszőleges, Á, B,

[2] A Kínai Nagy Falon már 2000 évvel ezelőtt, száz méterenként felállított fáklyások útján tudtak több száz kilométerre, nagyon gyorsan (és pontosan) üzeneteket eljuttatni.

	C					Á		C	Á					Á		C	B
Á		a	e	r	n	c	a	e	a	a	e	r	n	c	a	e	a
B		i	o	d	l	g	i	o	i	i	o	d	l	g	i	o	i
C		u	s	m	f	p	u	s	u	u	s	m	f	p	u	s	u
	C					**Á**		**C**	**Á**					**Á**		**C**	**B**

3.a) ábra

CSOROGATEAAFALON**Á**LMOS**C**SIGAB**Á**RELÉGLASSANKIM**Á**SZHATNA**C**SENDD**B**EN

↓ kezdőpont — ↓ (c) — ↓ (s) — ↓ (a) — ↓ (c) — ↓ (s) — ↓ (i)

3.b) ábra

C-től különböző betűkkel töltjük ki (lásd *3.b) ábra*). (Még jobb, ha értelmes szöveggé tudjuk kiegészíteni a rejtett szöveget, de ez nem feltétlenül szükséges.)

Az üzenet fogadójánál természetesen ugyanolyan táblázat van, mint a küldőnél. Így a fenti eljárást a kezdőponttól elvégezve olvashatóvá válik az üzenet. Mai szemmel ez az eljárás érdekes, de nem túl praktikus, mivel a táblázat használata elég nehézkes, és sok helyet használ az információtartalomhoz képest. Cardano a nehéz érthetőség kritikáját több kortársától is megkapta, akik akkor még nem tudhatták, hogy módszerével Cardano messze megelőzte korát, és elvetette a nem szimmetrikus rejtjelezés alapjait. A fenti eljárás ugyanis az addig szokásostól eltérően nem csupán betű-betű megfeleltetés, azaz betűhelyettesítés[3], hanem többértelmű megfeleltetés: a három nagybetű nindegyike 6-6 kisbetűt kódol, így a megfejtéshez többlet információra van szükség (a betű elhelyezkedése a sorban, vagyis távolsága a viszonyítási betűtől). Ellentétben tehát az egyszerű betűhelyettesítéssel, itt az üzenet és a rejtjelezett szöveg betűstatisztikája egyáltalán nem egyezik meg!

A Cardano-rács

A táblázaton alapuló másik módszercsalád, ami a mai napig is Cardano nevét viseli, az úgynevezett Cardano-rács. A rács itt egy betűkből álló mátrixot jelent. Hogy miről is van szó, ahhoz idézzük fel magának Cardanonak a szavait[4]:

„Végy két azonos méretű pergamen lapot, és azonos vonalak mentén készíts kivágásokat[5] *különböző helyeken. Ezek a kivágások legyenek kicsik, de mégis legalább*

[3] A betű-betű megfeleltetés azt jelenti, hogy az üzenet minden betűjéhez valamely szabály szerint egy ABC más betűjét rendeljük hozzá. A kriptográfiában ezt nevezik *helyettesítésnek*. Az így rejtjelezett szöveg betűinek eloszlása tehát pontosan megegyezik az eredeti szöveg betűinek eloszlásával.

[4] Az idézet Charles J. Mendelsohn: Cardan on cryptography [6] cikkéből származik.

[5] kis ablakokat

akkorák, mint az ABC nagybetűi. Az összes kivágásokba összesen 120 betűt lehessen elhelyezni. Az egyik pergamen lapot majd a levelező társadnak adod. Amikor alkalom adódik, először írd az üzenetedet olyan tömören, ahogy csak lehetséges, így az üzenet kevesebb betűt is tartalmazhat, mint amennyi a kivágott ablakokban elhelyezhető. Amikor beírtad az üzeneted az egyik pergamen lapra, tedd ugyanezt a másikkal is. Ezután töltsd ki az első lapon az üresen maradt helyet úgy, hogy teljes mondatokra egészítsék ki a már ráírt szöveget. Ez a kitöltés úgy történjen, hogy a teljes szöveg stílusa és tartalma összefüggő és egységes legyen. Amikor a levelező társad megkapja a te üzenetedet, ráhelyezi a megfelelő kivágásokkal ellátott pergament, és így elolvashatja az üzenetet."

A rejtjelező rács figyelemre méltó „divattá" vált a kriptográfiában. A Cardano-rács sikerét talán annak köszönheti, hogy egyszerű, de mégis fantasztikus változatosságot biztosít. Ekkora siker nagyon ritkán tapasztalható a tudomány, hát még a kriptográfia történetében. Hiszen az ismeretek állandó bővülésével a titkok megfejtésének technikája általában utoléri a titkosítók technikáját. Bár Cardano neve e téren nem vonult be a köztudatba, rejtjelező rácsa 450 éven át fennmaradt, sőt még a szépirodalomba is bevonult. *Jules Verne: Sándor Mátyás* című regényében éppen ilyen rejtjelező rács birtokába jutva fejti meg Sándor Mátyás elfogott titkos üzenetét a két gonosz, Torontál és Sárkány. A titkos levél és a megfejtéséhez szükséges rács már a regény elején megjelenik, és így a további cselekmény egyik „főszereplőjévé" válik.

Alábbi példánkban egy 6×6-os rácsot mutatunk be, amelyben felfedezhető bizonyos rokonság az úgynevezett intarzia játékkal is[6]. A *4. ábra* rácsába Karinthy Frigyes saját intarziáját írtuk be. Így még érdekesebb, hogy ugyanabban a szövegben mennyi különböző szöveg lehet elrejtve. Az *5., 6., 7. ábrákban* megvastagított számok a Cardano-rács kis ablakait jelölik, azaz a *4. ábrára* pontosan ráhelyezve és az ablakok helyén levő betűket balról jobbra haladva soronként lefelé összeolvasva megkapjuk a rejtett szöveget.

A *4. ábrába* beírt szöveg: „MAGÁT EGY ÉGI KAR INTI FRIGYE SIKERÜLNI FOG"

Az *5. ábra* rácsával kiolvasható rejtett szöveg: „MÁTÉ KINT INOG".

A *6. ábra* rácsával kiolvasható rejtett szöveg: „EGYÉK INGYEN".

A *7. ábra* rácsával kiolvasható rejtett szöveg: „AGG KINT FIGYEL".

Egy $n \times n$-es rácsba (amelyben n sor és n oszlop van) n^2 betűből álló szöveget írhatunk be. Ha az elrejtendő szöveg k betűből áll (ahol természetesen $k < n^2$) akkor a k ablakot tartalmazó rácsok száma $\binom{n^2}{k} = \dfrac{n^2!}{k!(n^2-k)!}$. Hogy ez mekkora változatosságot jelent, annak illusztrálására nézzük az *5. ábra* rácsát, itt $n = 6$, $k = 12$, a lehetséges

[6] Az intarzia játék a szórejtésnek egy sajátságos neme, amelyben az a cél, hogy bizonyos szavakat (többnyire személyneveket) kell folyamatosan elhelyezni egy másik szövegben. Karinthy, Kosztolányi, Molnár Ferenc és mások kedvelt kávéházi szórakozása volt az intarzia játék. Az egyik legsikeresebb intarzia Kosztolányié: Vendég panasza az étkezdében: *„Itt rossz a koszt, ó lány, ide zsörtölődni jár csak az ember."* Az intarzia a rejtjelezéshez képest valóban csak játék, hiszen elegendő a rejtett szöveg első betűjét megtalálni, abból már a teljes intarzia-szöveg kiolvasható, míg a Cardano-rácsnál minden ablak helyét külön-külön meg kell fejteni ahhoz, hogy a rejtett szöveg kiolvasható legyen.

M	A	G	Á	T	E
G	Y	É	G	I	K
A	R	I	N	T	I
F	R	I	G	Y	E
S	I	K	E	R	Ü
L	N	I	F	O	G

4. ábra

1	2	3	**4**	**5**	6
7	8	**9**	10	11	**12**
13	14	**15**	**16**	**17**	18
19	20	**21**	22	23	24
25	26	27	28	29	30
31	**32**	33	34	**35**	**36**

5. ábra

1	2	3	4	5	**6**
7	**8**	**9**	10	11	**12**
13	14	**15**	**16**	17	18
19	20	21	**22**	**23**	24
25	26	27	**28**	29	30
31	**32**	33	34	35	36

6. ábra

1	**2**	**3**	4	5	6
7	8	9	**10**	11	**12**
13	14	**15**	**16**	**17**	18
19	20	**21**	**22**	**23**	24
25	26	27	**28**	29	30
31	32	33	34	35	36

7. ábra

különböző rácsok száma tehát

$$\frac{36!}{12!\cdot 24!}=31\cdot 29\cdot 28\cdot 25\cdot 17\cdot 13\cdot 9=1\,251\,677\,700.$$

Ugyanígy számítható ki a *6. ábrára* ($n=6$, $k=11$) és a *7. ábrára* ($n=6$, $k=13$) a lehetséges rácsok száma.

Fordítsunk a rácson!

A Cardano-rács előzőkben leírt egyszerű képzési eljárása (ablakok tetszőleges kivágása) után — a továbbiakban ezt *egyszerű rácsnak* nevezzük — mutatunk egy másik rács-előállítási és -kitöltési módszert, amelyet forgató-rácsnak neveznek.

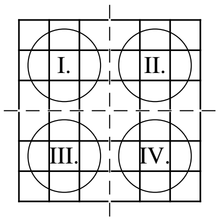
A forgató-rács olyan rejtjelező eszköz, amely 90 fokonként elforgatva ablakaival pontosan egyszer lefedi a hozzá tartozó betűmátrix összes mezőjét.

Itt tehát már nem lehet tetszőlegesen kivágni a rács ablakait, hiszen az elforgatások során ugyanarra a mezőre nem kerülhet több ablak. A rács ablakait úgy kell kijelölni, hogy elforgatáskor valamennyi ablak mindig más és más helyre kerüljön. Látható, hogy a forgató-rács előállításához szükséges, hogy a *rács mérete, n páros legyen.* Ha ugyanis a kivágható ablakok száma k, akkor ahhoz, hogy az n^2 mező mindegyikére a rács négy helyzete során pontosan egyszer kerüljön ablak, $k=\dfrac{n^2}{4}$ ablakra van szükség.

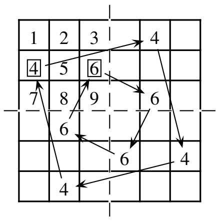
A forgató-rács előállítását is egy konkrét példán keresztül mutatjuk be.

Legyen a rács mérete $n=6$, ekkor tehát $k=9$ ablakot kell kivágnunk.

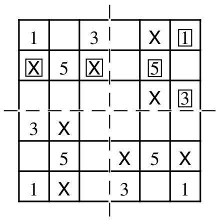
1. lépés: Osszuk fel a 6×6 mezőt tartalmazó mátrixot négy zónára a *8. ábra* szerint. Így az I–IV. zónák mindegyikébe pontosan kilenc mező esik.



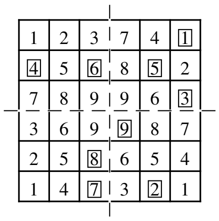
8. ábra



9. ábra



10. ábra



11. ábra

2. lépés: Válasszunk ki az I. zóna kilenc mezőjéből k_1 számút, ahol $1 \le k_1 \le 9$. Példánkban $k_1 = 2$, és a 4. és 6. mezőt választottuk (lásd *9. ábra*).

3. lépés: Forgassuk el a rácsot először 90 fokkal, és jelöljük meg a II. zónában azokat a mezőket, melyeket a kiválasztott (4. és 6.) mezők fednek. Majd forgassuk tovább a rácsot 90 fokonként, és jelöljük be ugyanígy a többi zónában is a fedett mezőket (lásd *9. ábra*). Így a k_1 ablak kijelölésével, négy forgatás után $4 \cdot k_1$ mező válik foglalttá.

4. lépés Most a II. zónában válasszunk a még nem foglaltakból $k_2 = 3$ mezőt. Példánkban ezek az 1., 3., 5. mezők (lásd *10. ábra*, ahol X jelöli a már foglalt mezőket, a bekeretezett számok jelölik az ablak-kivágásokat, a zóna számozása pedig értelemszerűen az I. zóna számozásának 90°-os elforgatottja). A négy elforgatással így újabb $4k_2$ mező válik foglalttá.

5. lépés: A fentiekhez hasonlóan végezzük el ugyanezt a III. és IV. zónákban is. Ekkor $4k_1 + 4k_2 + 4k_3 + 4k_4 = n^2$, azaz az ablakok számára valóban $k = k_1 + k_2 + k_3 + k_4 = 9$ adódik[7] (lásd *11. ábra*, ahol a bekeretezett számok jelölik a kivágott ablakokat).

Vegyük észre, hogy a k ablak mindegyikét szabadon jelölhetjük ki az I–IV. zónák valamelyikében, így az összes lehetséges (maximális számú ablakot tartalmazó) $n \times n$-es forgatórácsok száma $4^k = 4^{\frac{n^2}{4}}$. Példánkban ez $4^9 = 262\,144$.

Kérdés: *Azonos n rácsméret és k ablakszám esetén forgató-, vagy egyszerű rácsból van-e több?*

Megelőlegezzük a választ, amelyre az Olvasó jut e kérdés megválaszolása során: azonos rácsméret és ablakszám esetén nagyságrendekkel több a lehetséges egyszerű rácsok száma. Ugyanakkor rejtjelezési szempontból ez az összehasonlítás sántít, mivel az egyszerű rács betűmezőinek csak egy részében van a rejtett szöveg, míg a forgató-rácsnak mind az n^2 mezőjét felhasználhatjuk a rejtett szöveg beírására[8].

Illusztrációként bemutatjuk a *3. ábra* szövegének a *11. ábra* forgató-rácsával való rejtjelezését (lásd *12., 13., 14., 15. ábra*).

1. lépés: Rajzoljunk egy üres lapra akkora négyzetet, mint a forgató-rácsunk mérete, és helyezzük rá a rácsot.

2. lépés: Balról jobbra és fentről lefelé haladva írjuk a rács ablakaiba a szöveg kilenc betűjét.

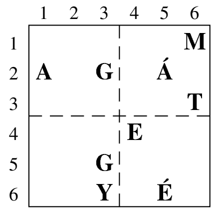
3. lépés: Forgassuk el a rácsot 90 fokkal, és ismételjük meg a 2. lépést.

4–5. lépés: Ismételjük meg a 3. lépést még kétszer.

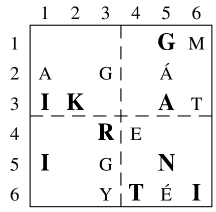
A *15. ábra* betűmátrixát kapjuk eredményül, amelyet elküldünk a címzettnek, aki a rács birtokában az 1–5. lépésekhez hasonló módszerrel el tudja olvasni az üzenetet.

[7] Természetesen az ablakok száma lehet ennél kevesebb is, de akkor a rács a négy körbeforgatás során nem fedi le az összes betűmezőt, így nem írhatjuk tele a szövegmátrixot.

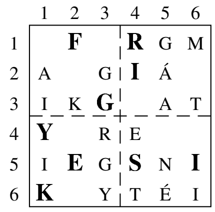
[8] Az egyszerű ráccsal történő rejtjelezésnél a rejtett szöveg betűinek sorrendje nem változik, míg a forgató-rács összekeveri a rejtendő szöveg betűit. A kriptográfiában a betűk helyettesítése és a betűk keverése a két alapvető módszercsalád, amelyeket önmagukban, vagy együttesen használ fel. A forgató-rács nagy előnye kriptográfiai szempontból, hogy lehetővé teszi a két módszer egyesítését. Érdemes tehát felfigyelni arra, hogy a rejtjelezési eljárásoknál nem elegendő csupán mennyiségi megfontolásokat figyelembe venni!



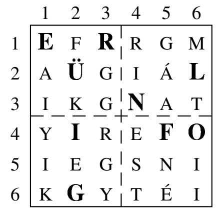
12. ábra



13. ábra



14. ábra



15. ábra

Példánkban külön érdekesség, hogy az így megfejtett szövegből az *5., 6., 7. ábra* egyszerű rácsaival újabb rejtett szövegek olvashatók ki.

A Cardano-rács történetének másik érdekessége, hogy pontosan Cardano *Ars Magna*-jának megjelenése után 250 évvel, 1795-ben jelent meg Carl Friedrich Hindenburg német matematikus könyve (lásd [4]), amelynek VI. fejezetét teljesen a rejtjelezésnek, ezen belül a rejtjelező rácsoknak szenteli. Nem a Cardano-rácsnak, mert (a tudománytörténetben nem szokatlan módon) Cardano nevét meg sem említi.

Hindenburg könyve nem csupán pontos leírását adja a Cardano-rácsnak, hanem bizonyos továbbfejlesztését is bemutatja. Ennek lényege, hogy ha a rács oldalait megjelöljük az a, b, c, d betűkkel, akkor a rácsforgatásokat megadhatjuk, mint e négy betű egy-egy permutációját. Ezzel a különböző rácsok számát $4!=24$-szeresére növelhetjük.

Kérdés: *Hogyan módosul a rácsforgató algoritmus a permutációs forgatás esetén?*

Amint azt a következőkben látni fogjuk, a permutációknak nemcsak a rácsok kitöltésében van nagy szerepe, hanem a rácsok ablakainak meghatározásában is.

Permutációk, latin négyzetek és rejtjelező rácsok

Latin négyzetnek olyan $n \times n$-es négyzetes mátrixot nevezünk, amelynek minden sora és minden oszlopa az 1, 2, ..., n számoknak egy permutációja.

Egy $n \times n$-es mátrixot *permutációs mátrixnak* nevezünk, ha a mátrix pontosan n darab 1-est tartalmaz úgy, hogy minden sorban és oszlopban pontosan egy 1-es áll, a többi elem pedig nulla.

Egyszerű, de a rejtjelező rácsok szempontjából fontos eredmény (lásd [1]) a következő:

Minden $n \times n$-es $L(n)$ latin négyzet egyértelműen felírható n darab permutációs mátrix segítségével a következő alakban:

$$L(n) = 1 \cdot P_1 + 2 \cdot P_2 + \ldots + n \cdot P_n, \tag{1}$$

éspedig úgy, hogy a P_k permutációs mátrixban éppen ott szerepel 1*, ahol $L(n)$-ben k van, a többi eleme pedig nulla.*

(Az „összeadás” művelet a mátrixok ugyanazon helyén álló elemeinek összeadását, míg a „számmal való szorzás” a mátrixok minden elemének a megszorzását jelenti.)

Az így adódó permutációs mátrixok rejtjelező rácsként használhatók fel. Az eljárást a következő példán keresztül mutatjuk be:

$$L(4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 1 & 2 \end{bmatrix}$$

$$P_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, P_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, P_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, P_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Mindegyik P_i permutációs mátrix egy olyan rejtjelező rácsként fogható fel, ahol az 1-esek helyén vannak az ablakok. Így a forgatás helyett most a permutációs mátrixokat kell – mint rácsokat – egymás után a betűmátrixra helyezni ahhoz, hogy a titkosított szöveget beírjuk, illetve kiolvassuk. Mivel a fenti egyértelmű felbontási tétel miatt az így készített rácsok ablakai pontosan lefedik a betűmátrix n^2 mezőjét, ezzel a módszerrel a teljes betűmátrixot kitölthetjük rejtjelezett szöveggel, akárcsak a forgató-rácsoknál. További előny, hogy a latin négyzet felbontásának egyértelműsége nem sérül, ha a felbontást adó permutációs mátrixok (rácsok) sorrendjét megváltoztatjuk. Így a lehetséges rácsfelhasználások száma a felbontások számának $n!$-szorosa.[9]

A rácsok tényleges alkalmazását megnehezíti terjedelmes helyigényük, hiszen n karakter betűmátrixba írásához szükség van a teljes permutációs mátrixra, és ehhez, bináris mátrix lévén, n^2 byte tárolását kell biztosítani. Ha a permutációs mátrixokat megszámozzuk, azaz bármely $n \times n$-es permutációs mátrixhoz kölcsönösen egyértelműen hozzárendeljük az 1, 2, ..., n számok egy permutációját, akkor a tárigény csökken.

Egy ilyen számozáshoz csak a mátrixban szereplő 1-esek megfeleltetésére van szükség, mivel az összes többi helyen nulla van. Legyen a permutációs mátrix i-edik sorának j-edik oszlopában 1-es. Ekkor a megfelelő permutáció i-edik eleme legyen a j. A permutációs mátrix definíciója szerint mindegyik sorban csak egy 1-es lehet, így valóban permutációt kapunk.

Ezek után a permutációkat egy megfelelő algoritmus (lásd [2]) segítségével sorszámokkal láthatjuk el 1-től $n!$-ig; ha a permutációs mátrixokat rejtjelező rácsként használjuk, akkor a mátrix, illetve az ehhez tartozó permutáció helyett elegendő a megfelelő sorszámot elküldeni a rejtjelezett üzenettel.

Az 1, 2, ..., n számok egy permutációjának a tárolásához $c(n)$ darab karakterre van szükség, ahol

$$c(n) = \left(\left[\lg n\right] + 1\right) n \tag{2}$$

[9] Helyhiány miatt csak utalni tudunk a latin négyzetek azon lényeges tulajdonságára, hogy minden latin négyzet egy művelettáblaként fogható fel, amely műveletek bizonyos feltételek mellett, a rejtjelezés szempontjából igen kedvező tulajdonságokkal rendelkeznek (nem kommutatív, nem asszociatív). Egy következő cikkben térünk ki eme előnyös tulajdonságok és a napjainkban általánosan elterjedt, „számelmélet alapú” módszerek összevetésére.

Az $n!$ szám számjegyeinek száma (jelöljük $j(n)$-nel):

(3) $$j(n) = \left[\lg n! + 1\right].$$

Ekkor

(4) $$\frac{j(n)}{c(n)} = \frac{\left[\lg n! + 1\right]}{n\left(\left[\lg n\right] + 1\right)} = \frac{\sum_{i=1}^{n} \lg i + 1}{n\left(\left[\lg n\right] + 1\right)},$$

és ezért

(5) $$\lim_{n\to\infty} \frac{j(n)}{c(n)} = 1.$$

Ez a megfeleltetés mégis jól használható a gyakorlatban, mivel a használatos értékekre az 1. táblázat értékei adódnak. Ez azt mutatja, hogy 25–50% megtakarítást érhetünk el, ha a permutáció helyett annak sorszámát tároljuk, illetve küldjük el.

n	$j(n)$	$c(n)$	$\frac{j(n)}{c(n)}$
10	7	20	.35
100	158	300	.526
200	375	600	.625
300	615	900	.683
400	869	1200	.724
500	1134	1500	.756

1. táblázat

A Cardano-rács általánosítása: k-rács (pókháló-rács)

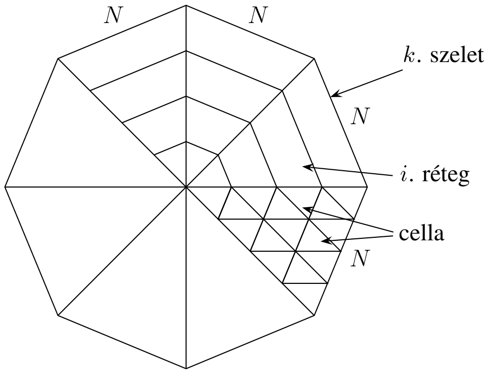
Cardano és Hindenburg is négyzet alakú rácsokkal dolgozott. Megmutatjuk, hogy tetszőleges szabályos k-szögre értelmezhető a rejtjelező rácsmodell.

Tekintsük a *16. ábra* szerinti konstrukciót. Ez egy k oldalú szabályos sokszög, amelynek mindegyik oldala N egység hosszú, azaz mindegyik szeletének legkülső rétege N darab cellát tartalmaz. Minden szeletben $\frac{N}{2}$ réteg és az i-edik rétegében $N - (2i - 1)$ cella van. Ebből következik, hogy az egy szeletben levő összes cellák száma:

$$\sum_{i=1}^{\frac{N}{2}} N - (2i - 1) = \frac{N^2}{4}.$$

A teljes k-rács celláinak száma tehát $k\frac{N^2}{4}$. (A Cardano-rács esetében $k = 4$, amelyre valóban a négyzetrács celláinak számát kapjuk.)

Természetesen a k-rács forgatási szöge most nem 90°, hanem $\dfrac{360^\circ}{k}$. Az igazi problémát a rács ablakainak elhelyezése jelenti. Tekintsük az alábbi mátrixot (lásd *17. ábra*), amelynek k sora, (ez felel meg a k-rács szeleteinek) és $N-2i+1$ oszlopa van (az i-edik réteg cellaszámának megfelelően).



16. ábra

	1	2	3	4	...	.	.	.	$N-2i+1$
1	.	X	.	X	...	.	.	.	.
2	.	.	.	.	...	.	.	.	X
3	.	.	.	.	...	.	X	.	.
.	X	.	.	.	...	.	.	.	.
⋮	⋮	⋮	⋮	⋮	⋱	⋮	⋮	⋮	⋮
.	.	.	.	.	...	.	.	X	.
$k-1$	.	.	.	.	...	.	.	.	.
k	.	.	X	.	...	X	.	.	.

17. ábra

A *17. ábrán* az X ablak kivágást jelöl. A forgató-rács szabályait figyelembe véve a mátrix minden oszlopában pontosan egy ablak lehet. Ebből adódik, hogy az i-edik rétegben k^{N-2i+1} ablak-kombináció lehetséges.

Mivel a rétegek elrendezései függetlenek egymástól, így a k-rács összes ablakkombinációinak száma, azaz a különböző k-rácsok száma:

$$FR_k^N=\prod_{i=1}^{\frac{N}{2}}k^{N-2i+1}=k^{\sum\limits_{i=1}^{\frac{N}{2}}N-2i+1}=k^{\frac{N^2}{4}}. \tag{6}$$

Láthatjuk, hogy $k=4$ esetén ez pontosan a különböző Cardano-rácsok számát adja. A Hindenburg-féle permutációs forgatás itt is alkalmazható, csak itt egy k jelből álló sorozatot használunk, és így $k!$-szorosára nő a rácsvariációk száma. Az alábbi 2. táblázatban érdekességként bemutatjuk néhány rácsmérethez tartozó k-rácsoknak a számát.

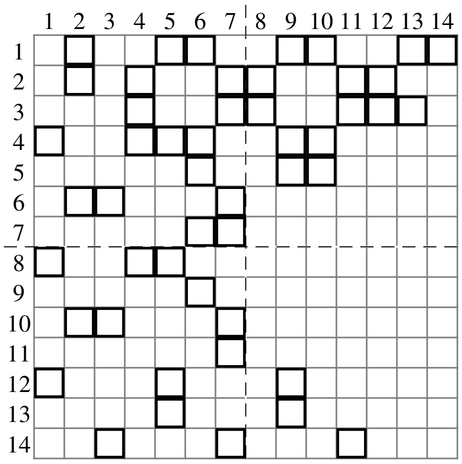
k	N	FR_k^N	k	N	FR_k^N
3	4	81	4	10	1 125 899 906 842 624
3	6	19 683	5	4	625
3	8	43 046 720	5	6	1 953 125
3	10	847 288 598 528	5	8	152 587 894 784
4	4	256	6	4	1 296
4	6	262 144	6	6	10 077 696
4	8	4 294 967 296	6	8	2 821 109 841 920

2. táblázat

Végül a *18. ábrán* megadunk egy rejtjelezett négyzetes szövegmátrixot, amelyhez tartozó Cardano-rácsot a *19. ábrán* (az ábrán a négyzetek jelölik az ablakokat) találjuk. A szöveg megfejtése (talán tartalma is) tanulságos lehet, a rácsot pedig újabb szövegek rejtjelezésére is felhasználhatja a kedves Olvasó.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	D	E	Z	E	G	Y	E		S	Z	R	S	E	R
2	E		T	V	I	O	O	L		H	T		E	M
3	B	T		H	E	A	O	L	R			N	E	E
4	M	A	Z		V	O		T	L	T	A	K	I	O
5	N		J	:		.	Á	T			R	Ö	L	T
6	N	V	O	E	M	A	L			A			K	V
7	I	É	N	L	Á	T		G	O	N	A	T		G
8	E	E	-	G	Y	E		Y	O	E	G	É	S	Y
9	S		N	Z	E	S	R	N	I	E	M		I	
10	B	Z	E	E	D	E	R	N	G	É	R		M	T
11		E	G	F	E	S		O		L	E	A		T
12	E	T		É	G	R	S		Y	D	T	V	É	U
13	L	N	Ö	P		I	R	E	E	A	N	G	G	É
14	E	N	G	?	I		Y	.	K	E	S	.	Z	R

18. ábra



19. ábra

Irodalomjegyzék

[1] *J. Dénes–A. D. Keedwell:* Latin squares and 1-factorizations of complete graphs I. Ars Combin. 25A, 1988. 109–126.

[2] *Dénes Tamás:* Algoritmusok az összes n-edfokú permutáció előállítására, Információ Elektronika, 1975. 1–2.

[3] *Philip J. Davis, Reuben Hersh:* A matematika élménye, Műszaki Könyvkiadó, Budapest 1984.

[4] *Carl Friedrich Hindenburg:* Urchid der Reinen und Angewandten Mathematic herausgegeben von Carl Friedrich Hindenburg, Leipzig, 1795.

[5] *Lukácsy András:* Elmés játékok, játékos elmék, Minerva Kiadó, Budapest, 1960.

[6] *Charles J. Mendelsohn:* Cardan on cryptography, Scripta Math., 1938.

[7] *Révay Zoltán:* Titkosírások, Zrínyi Katonai Kiadó, Budapest, 1978.

[8] *Sain Márton:* Matematikatörténeti ABC, Tankönyvkiadó, Budapest, 1974.

[9] *Sain Márton:* Nincs királyi út! (matematikatörténet), Gondolat Kiadó, 1986.

[10] *Simonyi Károly:* A fizika kultúrtörténete, Gondolat Könyvkiadó, Budapest, 1986.

[11] *B. L. van der Waerden:* Egy tudomány ébredése, Gondolat Könyvkiadó, Budapest, 1977.

Dénes Tamás

Rátz László Vándorgyűlés

Miskolc, 2001. július 4–7.

Parádés szervezés és derűs hangulat jellemezte a matematikatanárok hagyományos vándorgyűlését az idén. A szakmai előadásokat és szemináriumokat nagy érdeklődés mellett „telt házakkal” tartották a város három különböző iskolájában. A szünetekben a folyosókon szoftver-cégek matematikai termékeivel és új oktatási anyagokkal lehetett ismerkedni. A színvonalas szakmai programok után a szervezőbizottság változatos szabadidős elfoglaltságokat kínált kihasználva a város nyújtotta lehetőségeket. Orgonakoncert, kirándulás és sportprogramok: foci a Vidék csapatának győzelmével és termáluszoda látogatás gazdagították a programot. Ezúton is köszönjük a szervezőknek a kellemes napokat!

Hagyományosan a vándorgyűlés megnyitóján adja át a Beke Manó Emlékdíj Bizottság az évi Beke Manó Emlékdíjakat a matematikaoktatásban kiemelkedő teljesítményt nyújtó kollégáknak. A bizottság díjainak indoklását honlapunkon megtalálhatják.

A Beke Manó díj 1. fokozatát kapta megosztva *Szeredi Éva* és *Szendrei Julianna* a magyar matematikaoktatás megújításáért, a tanár-, illetve tanítóképzés szakmai színvonalának emeléséért, hosszú időn át végzett kiváló és eredményes munkájáért.

A Beke Manó díj 2. fokozatában részesültek: *Horváth Eszter* sok éven át végzett kiváló tanári–nevelői munkájáért és a matematikatanítás színvonalának emelését szolgáló példamutató tevékenységéért.

Katz Margit a kisiskolások értő, örömmel végzett matematikatanulását, a tanítók gyermeket és szakmát értő, örömteli matematikatanítását segítő munkájáért.

Királyné Nagy Éva a matematikaoktatás színvonalának emelését szolgáló, igényes szaktanári, szakvezetői munkájáért.

Lux Judit, aki a Budapesti Móricz Zsigmond Gimnázium egyik „legszerényebb, legműveltebb, leglelkiismeretesebb tanára” kiváló munkájáért.

Nádasi Márta több évtizedes kiváló felsőtagozatos tanári, szaktanácsadói és közoktatás-vezetői munkájáért.

Oláh Vera az általános és középiskolai matematika tanítás népszerűsítéséért, tanárok és diákok szakmai fejlődéséért a Kömal főszerkesztőjeként végzett óriási munkájáért.

Oláh Vera 1992-től tagja a KöMaL szerkesztőbizottságának, 1993 szeptembertől a lap főszerkesztője. Elévülhetetlen érdemeket szerzett a lap életbentartásában, fejlődésében, s ezzel a minőségi oktatás fejlesztésében. Részt vállalt a 100 éves Kömal rendezvényeinek szervezéséből, kiadványainak megjelentetésében. A „születésnapi” CD sok iskolában hozzáférhetővé tett minden korábbi cikket, feladatot az érdeklődő tanárok, diákok számára. 1993 óta a lap feladatmegoldó tábora szélesedett. A népszerűsítés szélesebb fokát jelzi, hogy a lap számos részlete ma már az interneten is olvasható.

Az utóbbi néhány évben a KöMaL Ifjúsági Ankétja az ifjúsági matematikai élet jelentős rendezvényévé nőtte ki magát. Ennek szervezése, anyagi és szellemi alapjának biztosítása is nagy részben Oláh Vera erőfeszítéseinek eredménye.

Nagy Gyula