Pálfy Péter Pál – Pham Ngọc Ánh: Szele Tibor és a debreceni algebrai iskola

Akit az istenek szeretnek, fiatalon hal meg.
(Menandrosz)

A Bolyai János Matematikai Társulat által adományozott legjelentősebb díj a Szele Tibor-emlékérem. *„E díj alapszabályai értelmében – Szele Tibor célkitűzéseit követve – olyan matematikusoknak ítélendő oda, akik fiatal matematikusoknak megindulásukhoz a legtöbb segítséget nyújtották, rájuk a legnagyobb hatást gyakorolták.”* – fogalmazták meg az emlékérem 1969-es alapításakor. Születésének századik évfordulóján emlékezünk az emlékérem névadójára, a fiatalon elhunyt kiváló tudósra és ifjú kutatók elhivatott mesterére. Emellett bemutatjuk a debreceni egyetemen körülötte kialakult algebrai tudományos iskola legjelentősebb eredményeit.

Életútja

Szele Tibor életéről jóval részletesebben szól a Debreceni Szemlében megjelent cikk [15], itt pályájának csak a legfontosabb, illetve a Matematikai Lapok olvasói számára legérdekesebb eseményeit ismertetjük annak az írásnak a felhasználásával. Munkásságáról további információk nyerhetők az [1], [4], [6], [11], [12] cikkekből.

Szele Tibor 1918. június 21-én született Debrecenben. Édesapja Szele Miklós (1884–1966) református lelkész volt, aki a Dóczi Intézet vallástanáraként működött. Édesanyja, Dicsőfi Gizella (1893–1978) a Gyakorló Gimnázium tanára volt. Szele Tibor szülei féltő gonddal nevelték egyetlen gyermeküket.

A debreceni Református Gimnáziumban végezte tanulmányait kitűnő eredménnyel. Érdeklődése 14 éves korában fordult a matematika felé. Ettől kezdve rendszeres feladatmegoldója lett a Középiskolai Matematikai Lapoknak. Világosan megfogalmazott megoldásait gyakran közölte a folyóirat. Abban az időben nem folyt pontverseny a KöMaL-ban, a rendszeres megoldók jutalma mindössze annyi volt, hogy fényképük megjelent a folyóirat mellékletében. Szele Tibor képe négy alkalommal szerepelt a dicsőségtablón, a gimnázium mind a négy felső osztályának tanulójaként kiérdemelte ezt az elismerést. Nyolcadikos gimnazistaként részt

vett az államilag szervezett országos tanulmányi versenyen, ahol „mennyiségtanból" a harmadik helyezést érte el. 1936-ban érettségizett, és ősszel a Matematikai és Fizikai Társulat tanulóversenyén (ma Kürschák József Matematikai Tanulóverseny) elnyerte az első díjat. A versenybizottság jelentése szerint: *„A legjobb dolgozat szerzője Szele Tibor, aki a debreceni ref. gimnáziumban dr. Mester István tanítványa. Neki javasoljuk kiadni az első b. Eötvös Loránd díjat. Bár a II. feladatra adott megoldása kissé hosszadalmas, egész dolgozata és különösen a III. feladat kidolgozása szabatos matematikai gondolkozásról tanúskodik."* A jövő algebristáját már itt felismerhetjük az algebrai feladatok megoldásának világos, célratörő megfogalmazásáról. „Kissé hosszadalmas" megoldást a geometriai feladatra adott.

Egyetemi tanulmányait a budapesti Műegyetem gépészmérnöki osztályán kezdte meg 1936 őszén. Ám ott csak egy félévet végzett el, 1937 januárjában átiratkozott a debreceni egyetem bölcsészkarára, ahol matematika-fizika szakos tanárnak készült. Itt is kitűnt diáktársai közül. Már 1937 szeptemberétől a matematikai szeminárium díjtalan gyakornoka. Negyedéves hallgatóként készített „A Hydrogén-színkép vizsgálata" című szakvizsgálati fizikai házi dolgozatáról írott bírálatában Gyulai Zoltán akadémikus, az Orvoskari Fizikai Intézet igazgatója fényes jövőt jósolt neki: *„A dolgozat kiváló tudományos képességekre mutat és remélhető, hogy a szerző tudományos életünkben idővel kiváló szerepet fog elfoglalni."* Matematikából (akkori szóhasználattal „mennyiségtanból") „Az analitikus függvényeknek az integrál fogalmára fölépített elmélete" címmel írta meg szakvizsgálati házi dolgozatát. Tanítási gyakorlatának elvégzése után 1941-ben kapta meg tanári diplomáját.

Volt tanárának, Széll Kálmánnak meghívására, aki akkor már Debrecenből elkerülve a szegedi egyetemen volt az Elméleti Fizikai Intézet igazgatója, ebbe az intézetbe kapott tanársegédi kinevezést. Bár állása fizikai tanszékhez kötötte, már ekkor is elsősorban matematikával foglalkozott. Tudományos mentorai a Matematikai Intézet oktatói, Rédei László és Kalmár László voltak. Érdeklődését mindenekelőtt az absztrakt algebra kötötte le. Behatóan tanulmányozta B. L. van der Waerden *Moderne Algebra* című, alapvető jelentőségű művét [17], egyes fejezeteit magának lefordította, sőt helyenként a tárgyalást is leegyszerűsítette. Egyidejűleg Rédei egy gráfelméleti kérdésével foglalkozott. Ezzel kapcsolatos eredményeiből készítette el doktori értekezését, amelyet benyújtott a szegedi egyetemhez. A dolgozat nyomtatásban 1943-ban jelent meg a Matematikai és Fizikai Lapokban. 1942 októberében azonban Szele Tibort behívták katonai szol-

gálatra, ami egészen a háború végéig tartott, emiatt doktori szigorlatára csak 1946-ban kerülhetett sor. A Szegedi Tudományegyetem 1947. április 23-án ünnepélyes keretek között avatta kitüntetéses (sub laurea Almae Matris) doktorrá.

Az 1946/47-es tanévtől kezdve már matematikusi állásba került a szegedi egyetemen: egy évig a Rédei László által vezetett Geometria Tanszéken volt tanársegéd, a következő tanévben pedig a Felsőbb Mennyiségtani Tanszéken, aminek élére akkor nevezték ki Kalmár Lászlót a Budapestre távozott Riesz Frigyes helyére. Bár az algebrai kutatás szempontjából Szeged volt az országban a legfontosabb centrum, Szele Tibor visszavágyott Debrecenbe, szülei közelébe. 1948-ban nyílt erre lehetősége, ekkor nevezték ki a Debreceni Tudományegyetemre az „egyetem beosztott létszámába áll. gimnáziumi tanárrá a 7. fokozatba". Gyorsan emelkedett a ranglétrán, még ugyanebben az évben egyetemi magántanár algebra és kombinatorika tárgykörből, 1950 szeptemberétől miniszteri megbízással vezette a 2. Matematikai Tanszéket, a későbbi Algebra és Számelmélet Tanszéket, végül 1952-ben – 34 évesen – megkapta a tanszékvezető egyetemi tanári kinevezést.

1952. március 15-én a Kossuth-díj ezüst fokozatával tüntették ki. Az indoklás szerint *„Szele Tibor egyetemi docens az Abel-féle csoportok elméletére vonatkozó strukturális vizsgálataiért, különös tekintettel a testelmélettel felfedezett analógiára"* részesült ebben a magas elismerésben. 1951-ben hozták létre nálunk szovjet mintára a Tudományos Minősítő Bizottságot, és vezették be a tudományok kandidátusa és a tudományok doktora fokozatokat. Az új tudományos minősítési rendszer indulásakor az arra érdemesítettek munkásságuk alapján megkapták ezeket a fokozatokat. Mindössze három matematikust nyilvánítottak ilyen módon a tudományok doktorának, közöttük Szele Tibort. A következő lépcsőfok az akadémiai levelező tagság lett volna. Bár 1953-ban és 1954-ben is jelölték erre, ez az elismerés nem jutott Szele Tibornak osztályrészül. (Ennek hátterét részletesen ismerteti a [15] cikk.)

1955. március közepén súlyosan megbetegedett. Az általa nagyon tisztelt Kalmár László ötvenedik születésnapjára rendezett konferenciára azonban betegsége ellenére elutazott Szegedre. Miután előadását megtartotta, állapota egyre rosszabbra fordult, és életét a szegedi klinikán sem tudták megmenteni, 1955. április 5-én elhunyt.

Tudományos munkássága

Szele Tibor tudományos munkásságának középpontjában az absztrakt algebra, azon belül is elsősorban a végtelen Abel-csoportok elmélete állt. Magyarországon az Abel-csoportokkal kapcsolatos kutatások Hajós György egy eredményével kezdődtek. Ő egy Minkowskitól származó geometriai problémát vezetett vissza egy véges Abel-csoportokra vonatkozó kérdésre, és aztán ezt a csoportelméleti problémát sikerült – egy igen összetett érvelés segítségével – megoldania. Erre a dolgozatára 1942-ben megkapta a Matematikai és Fizikai Társulattól a König Gyula jutalmat. A díj laudátora Rédei László volt, aki ennek hatására bekapcsolódott a téma kutatásába, és sikerült Hajós bizonyítását egyszerűsítenie. Szele Rédei révén ismerte meg a kérdést, és később maga is publikált egy még egyszerűbb bizonyítást Hajós tételére. A szakirodalom tanulmányozása során találkozott Kulikov munkáival, amelyekben a végtelen Abel-csoportok strukturális vizsgálatának új módszerét vezette be. Ebben az irányban tovább haladva vált Szele Tibor az Abel-csoportok kutatásának világviszonylatban egyik vezető alakjává. Szinte kifogyhatatlan volt az újabb és újabb kérdések felvetéséből, amelyeket aztán vagy ő, vagy tanítványai, munkatársai vizsgáltak meg, és ennek nyomán számos eredményt értek el ezen a területen. Szele érdeklődése nem korlátozódott az algebrának erre az ágára, más témákban (gyűrűelmélet, testelmélet, halmazelmélet) is több dolgozatot publikált.

Munkásságának alig tíz esztendeje alatt Szele Tibor 55 dolgozatot és egy tankönyvet írt. Ez akkor is rendkívüli alkotó teljesítmény, ha figyelembe vesszük, hogy – a kor szokásaival összhangban – a cikkek egy része igen rövid, gyakran mindössze egyetlen tétel bizonyítását tartalmazza, illetve néhány olyan munka is szerepel Szele műveinek jegyzékében, amelyben egy-egy ismert eredményre (például a Zorn-lemmára) ad új, egyszerűbb bizonyítást.

Mint említettük, doktori disszertációjában Rédei László egy kombinatorikai problémájával foglalkozott. Közérthetően úgy lehet fogalmazni a kérdést, hogy egy körmérkőzéses verseny lebonyolítása után oly módon kell sorba állítani a résztvevőket, hogy mindenki mögött közvetlenül egy olyan versenyző álljon a sorban, akit ő legyőzött. (Azaz matematikailag egy turnamentben keresünk irányított Hamilton-utat.) Könnyű bebizonyítani, hogy ez mindig lehetséges. Rédei azt mutatta meg, hogy minden esetben páratlan számú lehetőség van. Szele Tibor dolgozatának egyik fő eredménye a lehetőségek maximális számának becslésére vonatkozik.

Nehéz olyan szituációkat pontosan leírni, amikor a lehetőségek száma nagy, ezért a becsléshez azt az ötletet használja, hogy viszonylag könnyen ki lehet számítani a feltételnek megfelelő sorba rendezések átlagos számát, és akkor nyilvánvalóan léteznie kell olyan szituációnak, amikor a lehetséges sorba rendezések száma nagyobb, mint ez az átlag (ami egyébként $n!/2^{n-1}$). Ezt a bizonyítást tekintik a később Erdős Pál által nagy sikerre vitt valószínűségi módszer első példájának, lásd [2, Theorem 2.1.1].

A debreceni algebrai iskola

Szele Tibor nemcsak végzettségét, hanem lelki alkatát tekintve is tanár, vérbeli tanáregyéniség volt. 1948-ban, harmincéves korában kezdte oktatói pályafutását a debreceni egyetemen. Hét év alatt, 1955 tavaszán bekövetkezett tragikusan korai haláláig egy virágzó, világszínvonalú algebrai iskolát hozott létre Debrecenben, egy nagyon nehéz, nélkülözéssel, zaklatással terhes, a friss tudományos információktól elzárt korszakban. Bár ő maga is nagyon fiatal volt, huszonéves tanítványai lelkesen követték. Kutatásaik különösen három területen voltak kiemelkedőek.

Az Abel-csoportok elmélete. A Budapesten élő Fuchs Lászlóval és Hajós Györggyel, valamint a Szegeden dolgozó Rédei Lászlóval együttműködve Szele Tibornak és tanítványainak: Kertész Andornak, Erdős Jenőnek, Gacsályi Sándornak és Erdélyi Máriának eredményei jelentősen hozzájárultak az Abel-csoportok elméletének fejlődéséhez. A. G. Kuros Csoportelmélet című könyvének [13] 1955-ben megjelent magyar fordításához írt előszavában kiemeli, hogy a magyar algebrai kutatások számos kérdésben, *„különösen pedig az Abel-féle csoportok elméletében nagy lendületet vettek az utóbbi évek során, és tanúi vagyunk annak, hogy miként alakul ki Magyarországon az algebrai kutatások egy új, nagy központja"*. A könyv harmadik orosz nyelvű kiadásában Kuros Szelének már 20 dolgozatára hivatkozik. Fuchs László *Infinite Abelian Groups* című könyvének [5] irodalomjegyzékében Szelének 32 cikkét sorolja fel. Kaplansky a korszakot nyitó *Infinite abelian groups* című könyvének második kiadásában [10] elismerte, hogy Szele Tibornak igaza volt a „basic subgroup" fogalmának fontosságát illetően, továbbá a debreceni iskola több dolgozatára is hivatkozott. Külön kiemeljük Gacsályi Sándor két dolgozatát [7],[8], amelyekben az algebrailag kompakt csoportokra vonatkozó fontos eredményeket közölt. Ez a kutatási téma

feltehetőleg az algebrailag zárt testek Szele Tibortól származó zseniális megközelítéséből ered. Az algebrai (lineáris) egyenletrendszer megoldhatóságának segítségével jellemezték később a tiszta („pure") részcsoport fogalmát, a tiszta-injektivitást, a modulusok laposságát és az univerzális algebrában az algebrai kompaktságot. Szele Tibor halála után az ő ösztönző, biztató és összefogó szerepe, szakmai irányítása hiányában Gacsályi kimaradt a téma további fejlődéséből, és hasonlóan Erdélyi Mária is, aki a nemkommutatív csoportok körében foglalkozott ugyanezzel a kérdéssel.

Szele Tibor halála után a debreceni Abel-csoportos iskola felbomlott. Tanítványai rövid időn belül más területekre mentek át, vagy felhagytak a matematikai kutatással. Azt is érdemes megjegyezni, hogy Szele vezetésével a debreceni algebrai iskola a magyar matematikai közélet aktív, szerves résztvevője volt. Sajnálatos, hogy halála után a debreceni algebrai közösség fokozatosan bezárkózott, hosszú időn át lényegében nem vett részt a magyar matematikai társadalomban. Aztán 1985-ben, Szele Tibor halálának harmincadik évfordulójára emlékezve, a Kossuth Lajos Tudományegyetem Algebra és Számelmélet Tanszéke – a tanszék akkori vezetőjének, Buzási Károlynak a kezdeményezésére – nemzetközi csoportelméleti konferenciát szervezett, amelyen a téma neves nyugati és szovjet kutatói is részt vettek, ezáltal nagyszerű alkalom nyílt a személyes kapcsolatok kialakítására. A rendezvény sikerén felbuzdulva, 1987-ben és 1990-ben két további csoportelméleti konferenciát is szerveztek a tanszék munkatársai.

Gyűrűelmélet. A Szele-iskola hozzájárulása a gyűrűelmélethez is nagyon jelentős. Úgy tűnik, hogy maga az „Artin-gyűrű" elnevezés is Szele találmánya, először egy 1955-ös dolgozatában szerepel. Jacobson [9] és van der Waerden [17] könyveiben következetesen „minimumfeltételes gyűrűk"-ről beszélnek. Míg a Noether-gyűrű elnevezés McCoy könyvében [14] már 1948-ban megjelent, és utána gyorsan meghonosodott, az Artin-gyűrű elnevezés csak az 1960-as években vált általánosan elfogadottá.

A Szele-iskola eredményei akkoriban határozottan az egyik legjobb gyűrűelméleti iskolává tették őket a világon. Párhuzamot lehet felfedezni a témák és az eredmények tekintetében a debreceni és a Kaplansky által vezetett chicagói iskola között. A chicagói iskolának előnyére szolgált, hogy ott dolgozott Saunders Mac Lane, a homologikus algebra és a kategóriaelmélet egyik megteremtője. Ezzel szemben – Wiegandt Richárd meglátása szerint – a magyar algebristák ebben az időben kategóriaelméleti ismeretek

hiányában homologikus algebrai módszereket nem használtak, mivel Steinitz nyomán a testelméletből indultak ki, ahol nincs homomorf kép. Ennélfogva bővítésekben gondolkodtak, a struktúrákat „alulról" építették fel, és a struktúrák általuk adott jellemzői nem voltak homomorf invariánsok.

Szele Tibor egyik legismertebb eredménye is ferdetestekre vonatkozik. A kommutatív esetre vonatkozó feltételt általánosítva bizonyította, hogy egy ferdetest pontosan akkor rendezhető, ha -1 nem áll elő négyzetek szorzatainak összegeként.

A homologikus algebrai megközelítéssel kapcsolatban példaként említhetjük, hogy Hyman Bassnak sikerült homologikusan jellemeznie a főideálokra vonatkozó minimumfeltételnek eleget tevő gyűrűket, más néven a perfekt gyűrűket. Szász Ferenc egy személyes beszélgetés során elmondta, hogy 1955 táján Kertész Andor javaslatára kezdett foglalkozni ezekkel a gyűrűkkel. Érthetetlen, hogy miért nem ment tovább Szász Ferenc a végesen generált ideálokra vonatkozó minimum-feltétel irányába. A két feltétel ekvivalenciáját majdnem húsz évvel később mutatta meg Björk. Nem kizárt, hogy éppen Szele Tibor szakmai bátorítása hiányzott ahhoz, hogy Szász homologikus módszerekkel közelítsen a problémához, a gyenge dimenzió és a lapos modulusok kapcsolatán keresztül. Szász Ferenc eljutott a transzfinit nilpotenciához, de lemaradt a T-nilpotenciáról, ami pedig alkalmasabb a gyenge dimenzió tanulmányozásához. Talán ebben az esetben is Szele inspirációja hiányzott a legjobb megközelítés megtalálásához.

A fenti kérdések azért is figyelemre méltóak, mert magától adódik az a felvetés, hogy vajon Szele eljutott volna-e a homologikus algebra tanulmányozásához. Válasz erre természetesen nincs, csak találgatni lehet, de hajlunk arra, hogy feltehetően eljutott volna. Injektív modulusokkal és a velük rokon lapos vagy tiszta-injektív modulusokkal implicite már foglalkozott Szele és Gacsályi az egyenletrendszerek megoldhatósága kapcsán. Kertész Andor – igaz, lényegében csak féligegyszerű modulusok körében – szintén még Cartan és Eilenberg 1956-ban megjelent, korszakot nyitó homologikus algebrai monográfiája előtt végzett ilyen vizsgálatokat. Még egy további érv is felhozható az igenlő válasz mellett, mégpedig Papp Zoltán cikke [16], amelyben a nem kommutatív Noether-gyűrűket injektív modulusok segítségével jellemezte. Kaplansky egyik tanítványa, E. Matlis a Mathematical Reviewsban megjelent ismertetésében elismerte Papp Zoltán elsőbbségét Hyman Bass-szal szemben, akinek a doktori disszertációjából ez az eredmény Stephen Chase egy cikkében [3] kapott nyilvánosságot. Sajnos ez a kutatási irány sem folytatódott Magyarországon, pedig a nem-

kommutatív Noether-gyűrűk vizsgálata ma is dinamikusan fejlődő fejezete az asszociatív gyűrűk elméletének.

Nemkommutatív csoportok elmélete. Szele halálával a debreceni algebrai iskola fokozatos bezárkózása következtében a kezdeti sikerek után ez a kutatási irány sem tudott kibontakozni. Nem volt kapcsolatuk a Budapesten dolgozó Szép Jenővel. Kovács László emigrálása után ez a kutatási irány lényegében megszűnt Debrecenben.

További oktatói tevékenysége

De nem csak a kutatók képzésére volt Szelének gondja, bevezető egyetemi előadásait is alaposan kidolgozta, a hallgatók felkészültségéhez igazította. Ebből született kitűnő tankönyve, a Bevezetés az algebrába, ami 1953 és 1975 között nyolc kiadást ért meg, nemzedékek tanulták belőle az algebra alapjait, és kaptak kedvet az algebra magasabb fejezeteinek megismeréséhez.

Egyetemi munkája mellett még középiskolai matematikai délutánokat is szervezett rendszeresen a Bolyai János Matematikai Társulat keretében, ahol a debreceni tagozat alelnökeként tevékenykedett.

Zárszó

Az életében virágzó debreceni algebrai iskola világszínvonalú eredményei, majd a halála után bekövetkezett visszaesés ékesen ragyogtatják Szele Tibor oktatói, kutatói, tudományos vezetői és emberi nagyságát. Ha valaki, akkor Szele Tibor olyan ember, akit az istenek szerettek.

Köszönetnyilvánítás. A szerzők hálásak Márki Lászlónak és Wiegandt Richárdnak hasznos tanácsaikért.

Irodalom

[1] Tibor Szele (szerkesztőségi cikk), *Publicationes Mathematicae Debrecen* **3** (1954), 193–194.

[2] Noga Alon and Joel H. Spencer, *The probabilistic method*, Wiley, New York, 1992.

[3] Stephen U. Chase, Direct products of modules, *Transactions of the American Mathematical Society* **97** (1960), 457–473.

[4] Fuchs László, Szele Tibor élete és munkássága, *Matematikai Lapok* **6** (1955), 97–129.

[5] Fuchs László, *Infinite Abelian Groups I-II*, Academic Press, 1970–1973.

[6] Fuchs László, Végtelen Abel-csoportok Magyarországon, *Matematikai Lapok, új sorozat* **11** (2002–2003), 16–26.

[7] Gacsályi Sándor, On algebraically closed abelian groups, *Publicationes Mathematicae Debrecen* **2** (1952), 292–296.

[8] Gacsályi Sándor, On pure subgroups and direct summands of abelian groups, *Publicationes Mathematicae Debrecen* **4** (1955), 89–92.

[9] Nathan Jacobson, *Structure of rings*, American Mathematical Society, 1956.

[10] Irving Kaplansky, *Infinite abelian groups*, second edition, University of Michigan Press, 1969.

[11] Kertész Andor, Tibor Szele and his mathematical life-work, *Publicationes Mathematicae Debrecen* **4** (1956), 115–125.

[12] Kertész Andor, In memoriam Tibor Szele, *Matematikai Lapok* **32** (1981/1985), 215–218.

[13] A. G. Kuros, *Csoportelmélet*, Akadémiai Kiadó, 1955 (a 2. orosz kiadás fordítása); 3. orosz kiadás, 1967.

[14] Neil H. McCoy, *Rings and modules*, Mathematical Association of America, 1948.

[15] Pálfy Péter Pál, „Üstökösszerű pályája tudományos életünk egét örökké bevilágítja", Emlékezés Szele Tibor matematikaprofesszorra születésének 100. évfordulóján, *Debreceni Szemle* **26** (2018), 107–126. http://szemle.unideb.hu/wordpress/?page_id=2170

[16] Papp Zoltán, On algebraically closed modules, *Publicationes Mathematicae Debrecen* **6** (1959), 311–327.

[17] B. L. van der Waerden, *Moderne Algebra I-II*, Springer-Verlag, 1930–1931.

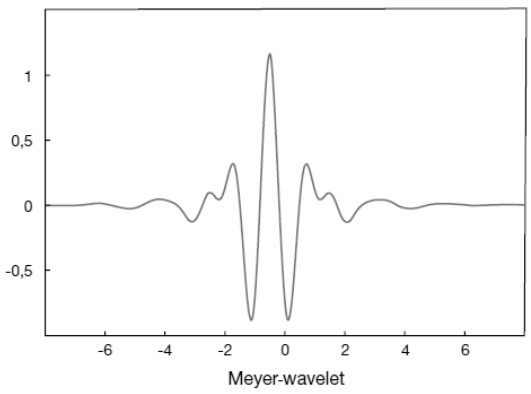
MTA Rényi Alfréd Matematikai Kutatóintézet
1053 Budapest, Reáltanoda utca 13–15.

Schipp Ferenc: Waveletek

A 2017. évi Abel-díjjal kitüntetett Y. Meyer munkásságáról

A 2017. évi Abel-díjat *Yves Meyer* francia matematikus kapta a *waveletek matematikai elméletének kidolgozásában játszott úttörő munkásságért*. Szeizmikus adatok elemzésére és képek tömörítésére használt gyakorlati eljárásokból kiindulva az 1980-as évek közepétől vezetésével a jelfeldolgozás egy új, hatékony módszerének rakták le a matematikai alapjait. A Fourier-analízisben korábban alkalmazott trigonometrikus felbontás helyett rövid tartójú hullám, ún. *wavelet* (franciául: *ondelett*) összetevőket használtak. A szakirodalomban a legtöbb nyelven átvették az angol elnevezést, hazánkban is ez terjedt el. (Egyik tanítványom a *hullámka* elnevezés használatát javasolta.) Meyer nevéhez fűződik az első sima, ortonormált wavelet-bázis konstrukciója, valamint a jelek felbontására használt *multirezolúciós analízis* bevezetése. A waveletek elmélete rövid időn belül igen népszerű lett az adatátvitellel és a jel- és képfeldolgozással foglalkozó szakemberek körében. Az elmúlt három évtizedben a wavelet-analízis számos változatát alkalmazták, többek között a harmonikus analízis, a jeltömörítés, a hibaredukció és a képfeldolgozás problémáinak megoldására. Az eljárást felhasználták a Hubble űrteleszkóp felvételeinek dekonvolúciójára, valamint a napjainkban észlelt gravitációs hullámok detektálásában. Yves Meyernek ezen túlmenően alapvető eredményei vannak a számelmélet, a harmonikus analízis, a parciális differenciálegyenletek, speciálisan a Navier–Stokes-egyenletek, valamint a szinguláris integrálegyenletek elméletében.

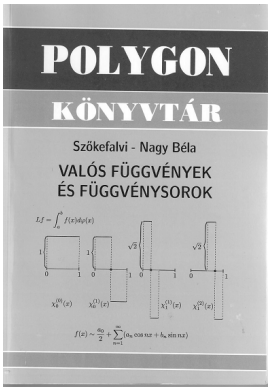
Yves Meyer (Abel-díj 2017)



Meyer-wavelet

Ebben a dolgozatban ismertetjük a témakör előzményeit, vázoljuk matematikai hátterét. Külön figyelmet szentelünk a magyar matematikusok eredményeinek, amelyek jelentősége az irányításelmélet, a jelfeldolgozás és a waveletek területén új megvilágításba kerültek. Például a trigonometrikus Fourier-sorokra vonatkozó *Fejér-féle szummáció* a háromszög ablaknak megfelelő jelszűrési eljárásként interpretálható. Számos, *Riesz Frigyes* által bevezetett fogalom és nevéhez fűződő eredmény alapvető szerepet játszik ezekben az alkalmazásokban. Ezek közül a matematikusok körében jól ismert klasszikus tételein túlmenően itt most csak a Hardy-terek faktorizációjára, a róla elnevezett bázis fogalmára, valamint a nemnegatív trigonometrikus polinomok előállítására vonatkozó *Fejér–Riesz-féle tételre* utalunk, amelyek a wavelet-konstrukciók alapvető eszközeivé váltak. A *Haar Alfrédről* elnevezett mérték, amely az absztrakt harmonikus analízis egyik legfontosabb eszköze, a jelfeldolgozás transzformációinak leírásában is nélkülözhetetlennek bizonyult. A *róla elnevezett rendszer,* amelyet 1909-ben egy elméleti probléma tisztázására vezetett be, napjainkban mint a legegyszerűbb wavelet vált igazán ismertté. Míg az 1960-as években – egyfajta magyar specialitásként – kizárólag csak a hazai egyetemi tankönyvek tesznek említést a Haar-rendszerről [13], addig manapság szinte minden jelfeldolgozással kapcsolatos tankönyv több fejezetet szentel a témának.

Haar Alfréd (1855–1933)



A Haar-függvények grafikonja [13]

A Haar-rendszerből kiinduló wavelet-transzformáció mellett a *Gábor Dénes* által 1945-ben vizsgált (ablakos) Fourier-transzformáció (azóta Gábor-transzformációnak nevezett eljárás) a beszéd és zenei hangok elemzésének hatékony eszköze lett. Ez a transzformáció a waveletek egy másik típusának mintájául szolgál. Az utóbbi két évtizedben a wavelet-transzformációk számos további változatát vezették be és alkalmazták a matematika,

a természet- és műszaki tudományok különböző területein. Ezek a transzformációk, a klasszikus Fourier-transzformációhoz hasonlóan egységes elvek szerint származtathatók, felhasználva az absztrakt harmonikus analízis eszköztárát. Ezen az úton, kiindulva az affin csoport egy reprezentációjából, eljuthatunk az (affin) *wavelet-transzformációhoz,* a Heisenberg-féle csoport egy reprezentációjából a *Gábor-transzformációhoz.* A waveletek 2000 óta az ELTE alkalmazott matematikus és informatikus szakán speciális szakirányok tanterveinek, Ph.D. programok és kutatások részét képezik [11], [16]. Kiindulva a Bolyai–Lobacsevszkij-féle geometria egybevágósági transzformációiból, a fentiek mintájára bevezettük a *hiperbolikus wavelet-transzformációkat* (HWT-t) [12]. A szóban forgó egybevágósági transzformációk a *Blaschke-függvényekkel* írhatók le. Ezek nemcsak a komplex függvénytanban, hanem az irányításelméletben is kitüntetett szerepet játszanak. Ennek alapján azt reméljük, hogy a HWT a jelfeldolgozásnak és a rendszerelméleti alkalmazásoknak adekvát eszközévé válhat. Az MTA SzTAKI és az ELTE Numerikus Analízis Tanszék együttműködésében született eredmények azt mutatják, hogy ezek a transzformációk hatékonyan alkalmazhatók az irányításelméletben [1] és EKG jelek feldolgozására és tömörítésére [4].

Történeti áttekintés

A Fourier-sorok elméletének kialakulása szorosan összefügg fontos gyakorlati problémákkal. Már maga *Fourier* is egy fizikából származó feladat, a hővezetés matematikai leírására dolgozta ki módszerét. A matematika számos fejezetének létrejötte és fejlődése szorosan összefügg azokkal a kérdésekkel, amelyek a Fourier-sorok alkalmazásával kapcsolatban felvetődtek. Ezek tisztázása *Dirichlet* munkássága nyomán a ma is használt függvényfogalom kialakulásához vezetett, *Cantort* a Fourier-sorok konvergencia-halmazaival kapcsolatos vizsgálatai inspirálták a halmazelmélet megalapozására. *Riemann* a Fourier-együtthatók értelmezéséhez kiterjesztette az integrál fogalmát, *Lebesgue* a róla elnevezett integrál bevezetésével a Fourier-sorok elméletét gazdagította egy ma is nélkülözhetetlen eszközzel, amely azután a valószínűségelmélet matematikai megalapozásában is fontos szerepet játszott.

Az első, mai szemmel nézve is korrekt konvergenciatétel *Dirichlet*-től származik, aki 1829-ben bebizonyította, hogy a szakaszonként monoton függvények Fourier-sora konvergens. Már 1876-ban *Du Bois Reymond*

munkássága révén ismert volt, hogy a Fourier-sor 2π szerint periodikus, *folytonos függvény esetén is lehet divergens*. A Fourier-sorok konvergenciájával kapcsolatos problémák tisztázása kapcsán új fogalmakat és módszereket vezettek be, több új fejezettel gazdagítva a matematikát. Többek között a hagyományos, pontonkénti konvergencia helyett az integrálközépben való konvergenciát, a részletösszegek helyett azok számtani közepeinek konvergenciáját véve alapul számos problémára sikerült választ adni. Ezekben *Riesz Frigyes* és *Fejér Lipót* munkássága úttörő jellegű volt [13].

A Haar-rendszer

Már a múlt század elején a trigonometrikus rendszer mellett több, akkor kissé egzotikusnak tűnő függvényrendszert vezettek be, amelyek elméleti és gyakorlati jelentősége jóval később derült ki. Ezek között is a *Haar Alfréd* által definiált ortonormált rendszer játszik kitüntetett szerepet. Haar a róla elnevezett rendszert doktori értekezésében vezette be 1909-ben, választ adva *Hilbert* egy Fourier-sorok divergenciájával kapcsolatos problémájára. A Du Bois Reymond-féle ellenpéldával összefüggésben Hilbert felvetette, hogy létezik-e olyan ortonormált rendszer, amely szerint vett Fourier-sorfejtés minden folytonos függvényre mindenütt konvergens? A kérdésre Haar pozitív választ adott, bebizonyítva, hogy az azóta róla elnevezett $(h_n,\ n \in \mathbb{N})$ *ortonormált rendszer szerinti Fourier-sor minden folytonos függvény esetén egyenletesen konvergens.* Az első pillanatra mesterkéltnek tűnő rendszer lépcsős függvényekből áll, amely a $[0,\infty)$ intervallumon értelmezett h alapfüggvényből egyszerűen származtatható, ahol $h(x) = 1$ $(x \in [0,1/2))$, $h(x) = -1$ $(x \in [1/2,1))$, $h(x) = 0$ $(x \in [1,\infty))$. Nevezetesen *transzlációt és dilatációt* alkalmazva kapjuk az $x \in [0,1)$ intervallumon értelemzett $h_0(x) := 1$, $h_m(x) := 2^{n/2}h(2^n x - k)$ $(m := 2^n + k,\ 0 \le k < 2^n, n \in \mathbb{N})$ *Haar-rendszert*. A h_m függvény tartója a 2^{-n} hosszúságú $I(k,n) := [k/2^n, (k+1)/2^n)$ diadikus intervallum. Ebből következik, hogy az f függvény $\langle f, h_m\rangle := \int_0^1 f(t)h_m(t)\,dt$ Haar–Fourier-együtthatói, ellentétben a trigonometrikus Fourier-együtthatókkal, az f függvénynek csak az $I(k,n)$ intervallumon felvett értékeitől függnek. A Haar-rendszer ortonormált az $L^2 := L^2[0,1)$ Hilbert-tér szokásos skaláris szorzatára nézve, és az $f \in L^1 := L^1[0,1)$ függvény Haar–Fourier-sorának $S_m f := \sum_{k=0}^{m-1}\langle f, h_m\rangle h_m$ részletösszegei előállíthatók az f függvény diadikus intervallumokra vett *integrálközepeivel*, nevezetesen az $x \in I(k,n)$

pontokban $S_{2^n} f(x) = 2^n \int_{I(k,n)} f(t)\, dt$. Innen következik, hogy a Haar-rendszer teljes az L^1 térben, bármely $f \in L^1$ függvény Haar–Fourier-sora L^1-normában és m.m. konvergál az f-hez, továbbá – választ adva Hilbert kérdésére – *folytonos függvény esetén a konvergencia egyenletes*. A Haar-rendszer ezekben a tulajdonságaiban alapvetően különbözik a trigonometrikus rendszertől.

Valószínűségelméleti terminológiát használva S_{2^n} a 2^{-n} hosszúságú diadikus intervallumok által generált σ-algebrára vonatkozó feltételes várható érték, továbbá az $(S_{2^n} f,\ n \in \mathbb{N})$ részletösszegek (reguláris, diadikus) *martingált alkotnak*.

A Haar-rendszernek ezek a tuljdonságai szolgáltak a *bázisokkal összefüggő funkcionálanalízisbeli, a martingálelméleti és a waveletekkel kapcsolatos* vizsgálatok kiinduló pontjául.

Egyszerűen igazolható, hogy a Haar-rendszer nemcsak az L^2 Hilbert-térben, hanem az L^p $(1 \leq p < \infty)$ Banach-terekben is bázist alkot. A Haar-sorok feltétlen (bármely átrendezés melletti) konvergenciájának vizsgálatában fontos szerepet játszik az f függvény *Paley* által bevezetett $Qf := \left(\sum_{k\in\mathbb{N}} |\langle f, h_k\rangle h_k|^2\right)^{1/2}$ kvadratikus variációja. Paley bebizonyította, hogy $1 < p < \infty$ esetén az f és a Qf L^p-normái ekvivalensek. Ennek alapján *Marcinkiewicz* megmutatta, hogy a Haar-rendszer $1 < p < \infty$ esetén *feltétlen* (azaz bármely átrendezés mellett is) *bázis* az L^p térben. Ismeretes, hogy a Parseval-formula alapján az L^2-tér jellemezhető bármely $(\phi_n \in L^2,\ n \in \mathbb{N})$ teljes ortonormált rendszer szerint vett Fourier-együtthatókkal: $f \in L^2$ akkor és csak akkor, ha $\sum_{n\in\mathbb{N}} |\langle f, \phi_n\rangle|^2 < \infty$. Amíg L^p terekre $p \neq 2$ esetén ilyen típusú jellemzés általában nem adható, addig a Haar-együtthatókból a Qf-ből kiindulva szerkeszthetünk az L^p-normával ekvivalens normát. A Haar-rendszernek ezek a tulajdonságai a 60-as években, hosszú szünet után, ismét ráirányították a figyelmet a rendszerre. Orosz matematikusok munkássága révén kiderült, hogy a Haar-rendszer eredményesen alkalmazható a fukcionálanalízis fontos problémáinak megoldásában, és kitüntetett szerepet játszik a bázisok között. Például többek között kiderült, hogy Banach-terek egy tág osztályára igaz a következő állítás: *ha a szóban forgó Banach-térben a Haar-rendszer nem feltétlen bázis, akkor ebben a térben feltétlen bázis nem létezik.* Speciálisan az L^1 térben nincs feltétlen bázis. Ezekről az eredményrekről nyújt részletes áttekintést *Ciesielski* [2] és *Uljanov* [14] 1985-ben a Haar-emlékkonferencián tartott előadása és a [9] monográfia.

A Faber–Schauder-, a Franklin- és a Ciesielski-féle rendszer

Mivel a Haar függvények nem folytonosak, azért ezek nem alkotnak bázist a $C[0,1]$ függvénytérben. *Faber* 1910-ben a Haar-függvények integrálját véve bevezetett egy folytonos függvényekből álló rendszert, amely normáló faktortól eltekintve a h_m-hez hasonló alakban adható meg. Kiindulva a $\varphi(x) := \int_0^x h(t)\,dt$ „háztető" függvényből, a szóban forgó rendszer dilatációval és transzlációval származtatható: $\varphi_m(x) := \varphi(2^n x - k)$ $(m = 2^n + k,\ 0 \le k < 2^n,\ n, k \in \mathbb{N},\ x \in [0,\infty))$. Faber megmutatta, hogy ez a rendszer bázis a $[0,1]$ végpontjaiban eltűnő folytonos függvények $C_0[0,1]$ terén. Ezekhez hozzávéve egy lineáris függvényt a $C[0,1]$ tér egy bázisát kapjuk. Megjegyezzük, hogy ezt a bázist később (1927-ben) *Schauder* újra felfedezte, és azóta ezt a rendszert az irodalomban Faber–Schauder-féle (FS) rendszernek nevezzük. Ez a rendszer nyilván nem ortogonális az L^2-tér skaláris szorzatára nézve. A $[\varphi_n, h_m] := \int_0^1 \varphi_n,\, dh_m = 0$ $(m \ne n,\ m, n \in \mathbb{N})$ reláció úgy interpretálható, hogy a folytonos függvényekből álló FS-rendszer és a korlátos változású függvényekből álló Haar-rendszer biortogonális. Megjegyezzük, hogy az $f \in C_0[0,1]$ függvény FS-rendszer szerinti biortogonális sorfejtésének részletösszegei interpolálnak a diadikusan racionális pontokban: $(S_{2^n}^{FS} f)(x) := \sum_{k=0}^{2^n-1} [f, h_k]\varphi_k(x) = f(x)$ $(x = j2^{-n},\ 0 \le j \le 2^n,\ n \in \mathbb{N})$, továbbá folytonos függvények FS-rendszer szerinti biortogonális sorfejtése egyenletesen tart az f-hez.

Franklin amerikai matematikus 1928-ban az FS-rendszerből kiindulva a Gram–Schmidt-féle ortogonalizációs eljárással bevezetett egy (szakaszonként lineáris, más szóval elsőfokú spline függvényekből álló) ortonormált rendszert, amelyről megmutatta, hogy nemcsak az L^2 térben, hanem $C[0,1]$-ben is bázis.

A Franklin-rendszer nem írható le a Haar-rendszerhez hasonló egyszerű képlettel. Ugyanakkor *Ciesielski* lengyel matematikus 1963-ban jól használható becslést adott a Franklin-rendszer függvényeire és Dirichlet-féle magfüggvényeire. Többek között bebizonyította, hogy az $f_m(x)$ $(m{=}2^n{+}k,$ $0 \le x \le 1,\ 0 \le k < 2^n)$ Franklin-függvények a Haar-függvényhez hasonló függvényekkel becsülhetők: $|f_m(x)| \le 2^{n/2} f(2^n x - k)$, ahol $f(u) = C\exp(-\gamma|u|)$ és C, γ abszolút pozitív konstansok. Ezeket az eredményeket általánosítva az FS-rendszer helyett m-edfokú spline függvényekből kiindulva Ciesielski az 1970-es években jó approximációs tulajdonságokkal rendelkező, *C^r-beli ortogonális bázisoknak egy új osztályát vezette be.* Ezekkel több, Banach 1932-ben megjelent könyvében említett fontos térben si-

került bázist szerkeszteni. Felhasználva ezeket az eredményeket *Bockarjev* orosz matematikus bebizonyította a Paley-féle egyenlőtlenség megfelelőjét a Franklin-rendszerre, következésképpen kiderült, hogy $1 < p < \infty$ esetén a Franklin-rendszer is feltétlen bázist alkot az L^p-terekben. Ugyanitt a Franklin-rendszer analitikus kiterjesztésével *bázist konstruált a diszkalgebrán,* megoldva Banach egy hosszú ideig nyitott problémáját. *Z. Ciesielski, Simon Péter* és *P. Sjölin* megmutatták, hogy azonos együtthatókat véve a Haar- és Franklin-sorok L^p-normában ekvikonvergensek, ha $1 < p < \infty$, más szóval a szóban forgó rendszerek *ekvivalens bázisok* az L^p $(1 < p < \infty)$ terekben. Ez volt az első nem triviális példa ekvivalens bázisokra. Ezekről további információt nyújt a [9] könyv 5. fejezete.

Waveletek

A jel- és képfeldolgozás gyakorlatában a jelek matematikai modellezése, analízise, kódolása, tömörítése, átvitele és tárolása, valamint szintézise és rekonstrukciója kapcsán számos új probléma vetődött fel, amelyek hagyományos eszközökkel nem kezelhetők. A klasszikus Fourier-transzformációt sikerrel alkalmazták stacionárius jelek reprezentálására. Az elmúlt évek tapasztalatai azt mutatják, hogy tranziens jelek esetén a wavelet-transzformációk bizonyultak hatékonyabbnak.

A Ciesielski-féle rendszereket és becsléseket felhasználva számos, bázisokkal kapcsolatos, fontos elméleti problémát sikerült megoldani. Az ezek szerinti sorfejtések jó approximációs tulajdonságaik miatt alkalmasak sztohasztikus folyamatok leírására, jelek reprezentálására és hatékony tömörítésére. Ennek ellenére, talán explicit előállítás hiányában, ezek nem terjedtek el az alkalmazók körében.

Az 1980-as évektől egy másik irányba indultak el a kutatások a Haar-rendszerhez hasonlóan származtatható, *sima függvényekből álló* $\psi_{n,k}(x) = 2^{n/2}\psi(2^n x - k)$ $(x \in \mathbb{R},\, n, k \in \mathbb{Z})$ alakú ortonormált rendszerek konstrukcióját tűzve ki célul az $L^2(\mathbb{R})$ térben. Az ilyen alakú függvényeket *waveletnek,* a rendszert generáló ψ függvényt *anya-waveletnek* nevezzük. Az első, folytonos (szakaszonként lineáris) függvényekből álló ortonormált wavelet-rendszert *Strömberg* konstruálta 1980-ban. Meyer 1985-ben C^∞-beli függvényekből álló ortonormált wavelet-bázisoknak egy osztályát adta meg, *explicit módon előállítva az anya-waveletet* (kompakt tartójú) *Fourier-transzformáltját* [3]. A bevezetőben bemutatott ábra egy Meyer-wavelet grafikonját szemlélteti.

Waveletek szerkesztése, a Haar-rendszert kivéve, nehéz feladatnak bizonyult. A konstrukciókban, a Meyer-féle wavelethez hasonlóan, a ψ anya-wavelet helyett annak $\widehat{\psi}$ Fourier-transzformációjából célszerű kiindulni. A továbbiakban az $L^1(\mathbb{R})$-beli függvény Fourier-transzformáltját, az $\epsilon_x(t) := \exp(2\pi i x t)$ $(x, t \in \mathbb{R})$ függvényeket alapul véve, $\widehat{g}(x) := \int_{\mathbb{R}} g(t)\overline{\epsilon}_x(t)\, dt$ szerint értelmezzük, és terjesztjük ki az $L^2(\mathbb{R})$ térre. Annak ellenére, hogy maga a ψ általában nem adható meg explicit alakban, a wavelet-Fourier-sorok jó konvergencia- és approximációs tulajdonságokkal rendelkeznek, a sorfejtés részletösszegeinek magfüggvényei jól becsülhetők, és a wavelet-Fourier-együtthatók hatékony algoritmussal számíthatók.

Különösen hasznosnak bizonyultak a *sima, kompakt tartójú waveletek*, amelyek *Ingrid Daubechies* úttörő munkásságának köszönhetően nemcsak az elméletben, hanem a gyakorlati alkalmazásokban is központi szerepet játszanak [3]. Az említett két tulajdonság egymás ellen hat: minél rövidebb a wavelet tartója, annál kisebb a simaságát jellemző Hölder-kitevő. A Daubechies által bevezetett, az $N = 2, 3, ...$ paramétertől függő $\psi^N \in C^{\alpha_N}$ wavelet tartójának hossza $2N - 1$, és Hölder-folytonos: $|\psi^N(x_1) - \psi^N(x_2)| \leq M|x_1 - x_2|^{\alpha_N}$ $(\alpha_N \approx 0{,}2075\ N)$. A waveletek konstrukciójában fontos szerepet játszik a ψ anya-wavelettel szoros kapcsolatban álló *skálázási függvény* vagy *apa-wavelet*.

A skálázási függvény értelmezését és szerepét a Haar-rendszer példáján mutatjuk be. Ebben az esetben h az anya-wavelet, és a $[0, 1)$ intervallum $\chi = \chi_{[0,1)}$ karakterisztikus függvénye az apa-wavelet. Legyen $\chi_{n,k}(x) := \chi(2^n x - k)$ $(x \in \mathbb{R}, k \in \mathbb{Z})$ a χ által generált wavelet-sorozat, és jelölje H_n a span$\{\chi_{n,k} : k \in \mathbb{Z}\}$ által generált zárt alteret az $L^2(\mathbb{R})$ térben. Nyilvánvaló, hogy $H_n \subset H_{n+1}$ $(n \in \mathbb{Z})$, és $\cup_{n\in\mathbb{Z}} H_n$ mindenütt sűrű a $H := L^2(\mathbb{R})$ térben. Ebből következik, hogy a $P_n : H \to H_n$ ortogonális projekciókra $P_n f \to f$ $(f \in H, n \to \infty)$ a H-tér normájában, a $K_n := H_{n+1} - H_n$ $(n \in \mathbb{Z})$ alterek egymásra ortogonálisak, továbbá a $h_{n,k} \in H_n$ $(k \in \mathbb{Z})$ Haar-rendszer egy ortonormált bázis ebben a térben, következésképpen a teljes $h_{n,k}$ $(n, k \in \mathbb{Z})$ Haar-rendszer a H tér egy ortonormált bázisa.

Ilyen típusú approximációs eljárást alkalmaztak jelek szűrésére (quadrature mirror filters) és képek tömörítésére (pyramid algorithms). Meyer ezeknek és az ehhez hasonló eljárásoknak tisztázta a matematikai hátterét, bevezetve a *multirezolúciós analízis* fogalmát. Jelölje τ_h az eltolás δ_s a dilatáció operátorát az $\mathbb{R}$-téren értelmezett függvények körében: $(\tau_h f)(x) = f(x + h)$, $(\delta_s f)(x) = f(sx)$ $(x, h \in \mathbb{R},\ s > 0)$. A multirezolúció értelmezéséhez induljunk ki egy $\varphi \in X := L^2(\mathbb{R})$ függvényből, amelynek $\varphi_k := \tau_k \varphi$

$(k \in \mathbb{Z})$ eltoltjai *Riesz-bázist* alkotnak, más szóval létezik két konstans $0 < m \leq M < \infty$, hogy bármely $f = \sum_{k\in\mathbb{Z}} a_k\varphi_k \in \text{span}\{\varphi_k : k \in \mathbb{Z}\}$ elem $L^2(\mathbb{R})$ normájára $m(\sum_{k\in\mathbb{Z}} |a_k|^2)^{1/2} \leq \|f\|_2 \leq M(\sum_{k\in\mathbb{Z}} |a_k|^2)^{1/2}$ teljesül. Megjegyezzük, innen az $m = M = 1$ speciális esetben következik, hogy a $(\tau_k\varphi,\ k \in \mathbb{Z})$ rendszer ortonormált. Az ilyen alakú Riesz-bázisok jellemezhetők a φ Fourier-transzformáltjával, nevezetesen a $(\varphi_k,\ k \in \mathbb{Z})$ rendszer akkor és csak akkor Riesz-bázis, ha $m^2 \leq E(|\widehat{\varphi}|^2) \leq M^2$, ahol E a periodizáló operátort jelöli: $Eg := \sum_{k\in\mathbb{Z}} \tau_k g$ $(g \in L^1(\mathbb{R}))$. Ennek alapján szerkeszthetünk eltolásinvariáns Riesz-bázisokat és ortonormált rendszereket. Mivel B-spline-ok Fourier-transzformáltja explicit alakban adható meg, azért ilyenekre a konstrukció egyszerűen elvégezhető.

Az $X_n \subset X := L^2(\mathbb{R})$ $(n \in \mathbb{Z})$ zárt altereknek egy *monoton növő* sorozatát *multirezolúciónak* nevezzük, ha i) uniójuk mindenütt sűrű X-ben, ii) metszetük a 0 függvényből álló triviális altér, iii) $\delta_2 : X_n \to X_{n+1}$ bijekció, iv) az X_0 alteret egy $(\tau_k\varphi,\ k \in \mathbb{Z})$ alakú Riesz-bázis generálja.

A fenti értelmezéséből következik, hogy az X_0 teret generáló φ függvény meghatározza a multirezolúciót: X_n a $\text{span}\{\varphi_{k,n} : k \in \mathbb{Z}\}$ tér lezárása. Az $X_n \subset X_{n+1}$ $(n \in \mathbb{Z})$ feltétel azzal ekvivalens, hogy $\delta_{1/2}\varphi \in X_0$. Innen következik, hogy kompakt tartójú φ esetén fennáll a

$$\varphi(x/2) = \sum_{j=0}^{2N-1} c_j\varphi(x-j) \qquad (x \in \mathbb{R}),$$

ún. *skálázási egyenlet*. A c_j wavelet konstansok ismeretében az egyenlet alapján iterációs eljárással meghatározhatjuk a φ értékeit a diadikusan racionális pontokban [3].

Az alábbi ábrákon a skálázási függvények értékeit ily módon számítottuk. A skálázási függvény (az apa-wavelet) ismeretében a ψ anya-wavelet

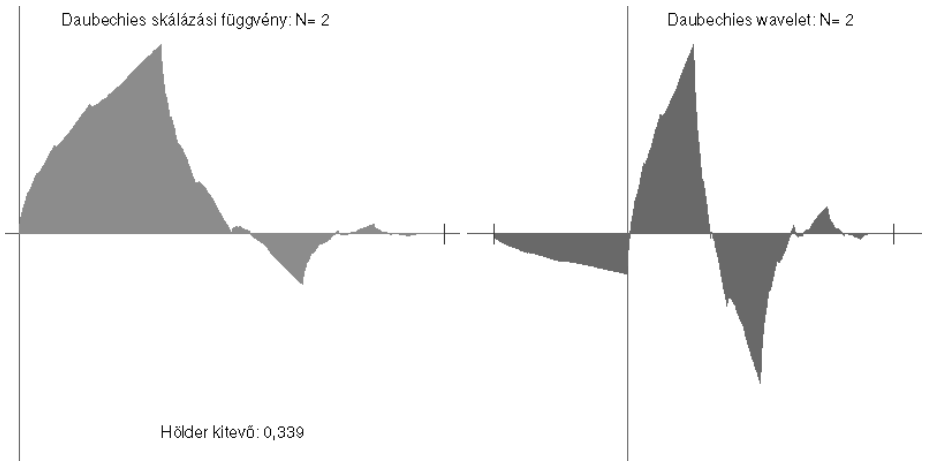
$$\psi(x/2) = \sum_{j=0}^{2N-1} (-1)^{j+1} c_j\varphi(x+2N-j) \qquad (x \in \mathbb{R})$$

alapján már meghatározható [3], [11], [15]. A Haar-rendszer esetén a skálázási egyenlet

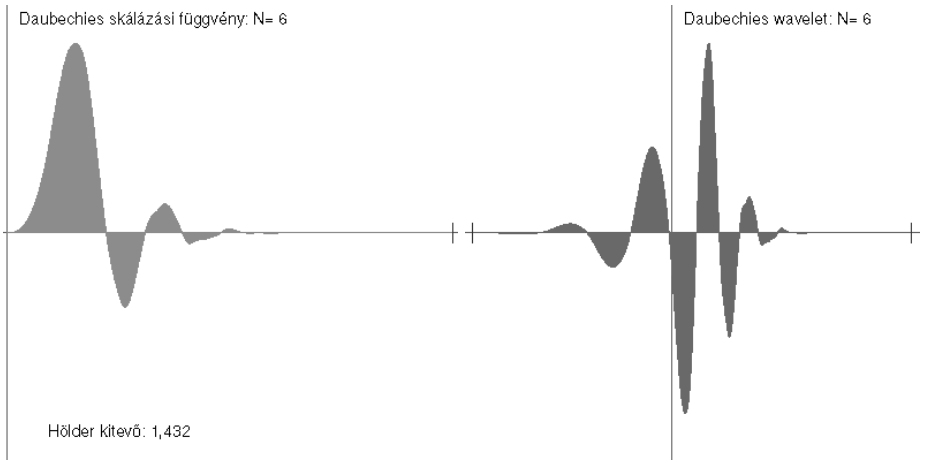
$$\chi(x/2) = \chi(x) + \chi(x-1) \quad \text{és} \quad h(x/2) = \chi(x) - \chi(x-1).$$

Bármely B-spline függvényre fennáll a skálázási egyenlet, és az együtthatók explicit alakban adhatók meg.

Az alábbi ábrákon $N = 2$, $N = 6$ esetén szemléltetjük a Daubechies-féle skálázási függvényt és anya-waveletet.



A Daubechies-féle φ skálázási függvény és ψ wavelet: $N = 2$



A Daubechies-féle skálázási függvény és wavelet: $N = 6$

A skálázási egyenletet célszerű a Fourier-transzformáltakra (a frekvenciatartományban) felírni és megoldani. Kompakt tartójú skálázási függvény esetén $\widehat{\varphi}(2t) = \alpha(t)\widehat{\varphi}(t)$ $(t \in \mathbb{R})$, ahol az $\alpha(t) = \sum_{k=0}^{2N-1} c_k e^{-2\pi ikt}$ trigonometrikus polinomot, a jelfeldolgozásban szokásos terminológiát használva, a *wavelet (alulvágó) szűrőjének nevezik.* Bebizonyítható, hogy ha φ MR-felbontást generál, akkor az 1-szerint periodikus α szűrőre $(*)$ $\alpha(0) = 1$, $|\alpha(x)|^2 + |\alpha(x+1/2)|^2 = 1$ $(x \in \mathbb{R})$ teljesül, továbbá $\widehat{\varphi}$ előállítható végtelen

szorzatként: $\widehat{\varphi} = \prod_{k=1}^{\infty} \delta_{2^{-k}}\alpha$. Megfordítva, kiindulva egy 1-szerint periodikus α trigonometrikus polinomból, amely eleget tesz a $(*)$ feltételnek, a szóban forgó végtelen szorzat (kompakt intervallumokon egyenletesen) konvergál egy folytonos $A \in X$ függvényhez. Amennyiben ezen kívül még $E(|A|^2) = 1$ teljesül, akkor a $\widehat{\varphi} = A$ alapján számított φ MR-felbontást generál. Ez utóbbi feltétel biztosítására több elégséges feltétel ismert. Doubechies a $(*)$ egyenletnek olyan α trigonometrikus polinom megoldásait határozta meg, amelyekből az említett módon származtatott φ skálázási függvény kompakt tartójú, és $\varphi \in C^{\alpha}$ [3]. Megjegyezzük, hogy a konstrukcióban fontos szerepet játszik a következő Fejér–Riesz-féle tétel: Ha az S páros trigonometrikus polinom nemnegatív, akkor van olyan P trigonometrikus polinom, amelyre $S(x) = |P(x)|^2$ $(x \in \mathbb{R})$.

Az utóbbi évtizedekben a waveletek számos változatát vezették be. Elsőként megemlítjük a waveletek egy folytonos paraméterektől függő osztályát, a $\psi_{a,b}(t) := a^{-1/2}\psi((t-b)/a)$ $(\psi \in X, a > 0, b, t \in \mathbb{R})$ waveleteket és az ezekkel képzett $f \to (\mathcal{W}f)(a,b) := W(a,b) := \langle f, \psi_{a,b}\rangle$ $(f \in X)$ transzformációkat, amelyeket *Grossman és Morlet* a kvantummechanika koherens állapotainak leírására vezetett be az 1980-as években. Kiderült, hogy az általuk felfedezett $f(x) = \int_0^{\infty}\int_{\mathbb{R}}(W(a,b)\psi_{a,b}(x)\,db\,da/a$ $(x \in \mathbb{R})$ rekonstrukciós formula *Calderon* egy 20 évvel korábbi azonosságából következik. Ezek az eredmények késztették Meyert az ilyen típusú transzformációk szisztematikus vizsgálatára [5], [6].

A wavelet-transzformációk egy másik fontos osztályát, a *Gábor Dénes* által 1945-ben bevezetett (ablakos) Fourier-tramszformációra utalva, *Gábor-transzformációknak* nevezik. Ebben az esetben az integráltranszformáció magfüggvénye egy $g \in X$ ablakfüggvényből *transzlációval és modulációval* képzett $g_{a,b}(x) := \epsilon_a(x)g(x-b)$ $(x,a,b \in \mathbb{R})$ függvénysereg, maga a transzformáció $f \to (\mathcal{G}f)(a,b) := \langle f, g_{a,b}\rangle$ $(f \in X)$ alakú. A $\psi, g \in X$ függvényre tett megfelelő feltételek mellett mindkét esetben érvényesek a Fourier-transzformációra ismert, az energia-megmaradást kifejező Plancherel-formula és a rekonstrukciót lehetővé tevő inverziós formula megfelelői.

Ezeknek a formuláknak az értelmezése, a Fourier-transzformálthoz hasonlóan, számos kérdést vet fel. *Weisz Ferenc* igen általános feltételek mellett különböző konvergenciatípusokat és szummációs eljárásokat alapul véve meghatározta a szóban forgó formulák érvényességi körét, messzemenően általánosítva a korábbi eredményeket [7], [16].

A Fourier-transzformációt az $\mathbb{R}$ additív csoportjának ϵ_x $(x \in \mathbb{R})$ karak-

terei, az $\mathbb{R}$ egydimenziós reprezentációi segítségével értelmezzük: $\widehat{f}(x) := \langle f, \epsilon_x \rangle$. Az absztrakt harmonikus analízis szemléletét követve ezen az alapon a Fourier-transzformáció fontos tulajdonságai levezethetők. A wavelet- és a Gábor-transzformáció az $\mathbb{R}$ affin csoportjának, ill. a Heisenberg-féle csoport egy-egy reprezentációjából kiindulva hasonló elvek szerint származtatható. Ez a szemlélet elősegíti az említett transzformációk mélyebb megértését, és mintát ad hasonló típusú leképezések szerkesztéséhez. A Bolyai–Lobacsevszkij-féle geometria egybevágósági transzformációiból kiindulva bevezettük a *hiperbolikus waveleteket* és az ezek által generált transzformációkat, valamint bebizonyítottuk a Plancherel- és a rekonstrukciós formulák megfelelőit [12]. *Pap Margit* a hiperbolikus waveletek diszkrét változatából kiindulva a $H^2(\mathbb{T})$ Hardy-térnek egy multirezolúciós felbontását adta meg [8]. Racionális függvényekből álló waveleteket sikerrel alkalmaztunk EKG-görbék matematikai modellezésére és tömörítésére, valamint irányításelméleti problémák megoldására [1], [4].

A wavelet-konstrukciók alapvető eszköze a Fourier-transzformáció. Ez az észrevétel inspirált bennünket arra, hogy alkalmas formában leírva a lokális testek Fourier-transzformációit, lerakjuk a wavelet-konstrukcióhoz szükséges technikai alapokat [10].

Irodalom

[1] Bokor J., Schipp F., Soumelidis, A., Applying hyperbolic wavelet construction in the identification of signals and systems, *15th IFAC Symposium on System Identification, SYSID 2009*, Saint-Malo, France, July 6–8, 2009.

[2] Ciedielski, Z., Haar orthogonal functions in analysis and probability, in: *A. Haar Memorial Conference*, Colloq. Math. Soc. János Bolyai, Eds. J. Szabados, K. Tandori, **49** 1985, 27–56.

[3] Daubechies, I., *Ten Lectures on Wavelets*, SIAM, Philadelphia, Pennsylvania, 1992.

[4] Fridli S., Lócsi L., Schipp F., *Rational Function Systems in ECG Processing*, EUROCAST 2011, Springer LNCS 6927, 88–95.

[5] Meyer, Y., *Ondelettes ét opérateurs. I. Ondelettes, II. Opérateurs de Calderon–Zygmund, III. Opérateurs multilinéaire*, Hermann, Paris, 1990. English translation in Cambridge University Press, 1992.

[6] Meyer, Y., *Wavelets. Algorithms and Applications*, SIAM, Philadelphia, Pennsylvania, 1992.

[7] Feichtinger, H. G., Weisz F., Gabor analysis on Wiener amalgams, *Sampl. Theory Signal Image Process* **6** (2007), 129–150.

[8] Pap M., Hyperbolic Wavelets and Multiresolution in $H^2(\mathbb{T})$, *Journal of Fourier Analysis and Applications*, 2011, DOI: 10.1007/s00041-011-9169-2.

[9] Schipp F., Wade, W. R., Simon P., Pál J., *Walsh series. An introduction to dyadic harmonic analysis*, Akadémia Kiadó, Budapest, Adam Hilger, Bristol and New York, 1990.

[10] Schipp F., Wade, W. R., *Transforms on normed fields. Leaflets in Mathematics*, Pécs, 1995.

[11] Schipp F., *Waveletek. Egyetemi jegyzet alkalmazott- és programtervező matematikusoknak*, ELTE, 2013. (http://numanal.inf.elte.hu/schipp)

[12] Schipp F., Hiperbolikus waveletek, *Alkalmazott Matematikai Lapok* **32** (2015), 1–40.

[13] Szőkefalvi-Nagy B., *Függvények és függvénysorok*, Polygon, Szeged, 2002.

[14] Uljanov, P. L., Haar series and related questions, *A. Haar Memorial Conference*, Coll. Math. Soc. J. Bolyai, Eds. J. Szabados, K. Tandori, **49**, 1985, pp. 57–96.

[15] Weisz F., *Wavelet- és Gábor-transzformált*, ELTE, Budapest, 2013, 317 pp. ISBN 978-963-284-453-4

[16] Weisz F., Multi-dimensional Summability Theory and Applications, *Current Topics in Summability Theory and Application*, Eds. H. Dutta and B. E. Rhoades, Springer Singapore, 2016, 241–311.

ELTE IK, Numerikus Analízis Tanszék
1117 Budapest, Pázmány P. sétány I/C.
schipp@numanal.inf.elte.hu

Soukup Dániel Tamás: Két végtelen számosság és meglepő kapcsolatuk

Már a 17. században Galileo Galilei elgondolkozott azon, hogyan hasonlíthatnánk össze végtelen halmazok méretét. Közel négyszáz évvel később, 2017 nyarán a Budapesten megrendezett hatodik Európai Halmazelmélet Konferencián egy fiatal modellelmélész, Maryanthe Malliaris és a veterán polihisztor, Saharon Shelah vehette át a Hausdorff-medált, melyet az elmúlt öt év legmeghatározóbb halmazelméleti eredményéért ítélnek oda. Malliaris és Shelah jelentős áttörést értek el egy modellelméleti klasszifikációs problémával kapcsolatban, és egyben belátták, hogy két sokat vizsgált és különbözőnek sejtett végtelen számosság, $\mathfrak{p}$ és $\mathfrak{t}$ valójában egyenlőek. Ez utóbbi eredmény jelen ismeretterjesztő cikkünk témája.

S. Shelah és M. Malliaris középen
(Joan Bagaria fotója)

Galilei példájában a természetes számok $\mathbb{N}$ halmazát veszi, és a négyzetszámokat $\{1, 4, 9, 16 \dots\}$. Az első érvelés szerint a két halmaz ugyanakkora: mivel minden négyzetszámhoz pontosan egy pozitív gyök tartozik, és minden természetes szám előfordul valamely négyzetszám gyökeként, ezért ugyanannyi természetes szám kell, hogy legyen, mint négyzetszám. Másrészről, rengeteg természetes szám nem négyzetszám, olyannyira, hogy a négyzetszámok aránya nullához tart a természetes számok között, ahogy nagyobb és nagyobb intervallumokat tekintünk. Galilei ezt egy olyan paradoxonnak könyvelte el, ami megakadályozza, hogy végtelen halmazokat összemérjünk [5].

Georg Cantor a következő, mára általánosan elfogadott, definícióval állt elő az 1870-es években: két tetszőleges halmaz *azonos számosságúak* pontosan akkor, ha elemeik között létezik kölcsönösen egyértelmű megfeleltetés. Tehát Galilei első érvelése pont azt mutatja, hogy $\mathbb{N}$ és a négyzetszámok halmaza azonos számosságúak. Azokat a halmazokat, melyek a természetes számokkal azonos számosságúak, *megszámlálhatóan végtelennek* nevezzük, és méretüket $\aleph_0$-val jelöljük (ejtsd *alef nulla*), utalva arra, hogy ez a legkisebb végtelen számosság.

Cantor egyik nagy hozzájárulása a logika fejlődéséhez, hogy Galilei észrevételét nem feloldhatatlan ellentmondásként kezelte, hanem a fenti definíció alapján nekilátott egy gazdag elmélet kidolgozásához. Első lépésként azt bizonyította, hogy a racionális számok $\mathbb{Q}$ halmaza is megszámlálható, majd a valós számok $\mathbb{R}$ halmazát tekintette: lehetséges, hogy $\mathbb{R}$ is megszámlálható? Cantor szerint, akárhogy is vesszük valós számok egy $x_1, x_2, x_3 \dots$ listáját, mindig találunk olyan y számot, ami nem szerepel a listán. Hiszen ha y az a valós szám, ami az első tizedes helyén eltér x_1 első tizedes jegyétől, a második tizedes helyén eltér x_2 második tizedes jegyétől, és így tovább, akkor y nem szerepelhet a listánkon. Tehát nincs kölcsönösen egyértelmű megfeleltetés $\mathbb{N}$ és $\mathbb{R}$ között, azaz $\mathbb{R}$ számossága, melyre a $2^{\aleph_0}$ jelölés használt, nagyobb mint $\aleph_0$. Tehát beláttuk a következő egyenlőtlenséget végtelen számosságok között:

$$\mathbb{N} \text{ számossága} = \aleph_0 < 2^{\aleph_0} = \mathbb{R} \text{ számossága}.$$

Cantor elmélete alapján bármely két végtelen számosság összemérhető, és számosságok bármely (nem üres) rendszerében van legkisebb. Így van értelme az első nem megszámlálható számosságról beszélni, mely $\aleph_1$-gyel jelölt. A következő szigorúan nagyobb számosság $\aleph_2$-vel jelölt, utána $\aleph_3$, és így tovább.[1]

Van-e legnagyobb végtelen? Cantor definíciója szerint nincs. Bármilyen X halmaznak több részhalmaza van, mint eleme, azaz $\kappa < 2^\kappa$ ha κ számosság.

Tehát kaptunk egy szigorúan növő $\aleph_0 < \aleph_1 < \aleph_2 < \dots$ sorozatot egyre nagyobb és nagyobb végtelen számosságokból. Felmerül a kérdés: hol

[1] Az alefek listája itt nem áll meg: a természetes számokkal indexelt $\aleph_n$ számosságok szuprémuma $\aleph_\omega$, a következő eggyel nagyobb számosság $\aleph_{\omega+1}$, majd $\aleph_{\omega+2}$...

is van $2^{\aleph_0}$ ebben a listában? Érdekes módon, ez *nem eldönthető*, legalábbis a matematikában általánosan elfogadott, úgynevezett ZFC axiómarendszert használva.[2] A matematika bizonyos modelljeiben $2^{\aleph_0} = \aleph_1$, azaz $2^{\aleph_0}$ az első nem megszámlálható számosság: ekkor azt mondjuk, hogy a *kontinuumhipotézis* teljesül. Sok más érdekes modellben ez nem igaz, és vannak közbülső számosságok $\aleph_0$ és $2^{\aleph_0}$ között; sőt megmondhatjuk, hogy $2^{\aleph_0}$ hanyadik végtelen számosság legyen a listánkon: olyan ad hoc egyenlőségekre, mint $2^{\aleph_0} = \aleph_{16}$ is találhatunk egy modellt.

A következő egyszerű példa illusztrálja, hogy mit is jelent egy állítás függetlensége: $\mathbb{R}$ és $\mathbb{Q}$ mint algebrai struktúrák teljesítik az összeadás és szorzás axiómáit,[3] azonban az $x^2 = 2$ egyenletnek $\mathbb{Q}$-ban nincs megoldása, míg $\mathbb{R}$-ben kettő is van. Tehát az összeadás és szorzás axiómái nem döntik el, hogy az „$x^2 = 2$ egyenlet megoldható" állítás igaz vagy hamis-e. Míg a ZFC axiómarendszer azt eldönti, hogy a síkháromszögek belső szögeinek összege 180 fok, azt már nem dönti el, hogy $2^{\aleph_0} = \aleph_1$ vagy $2^{\aleph_0} > \aleph_1$; valamelyik állítás teljesülni fog, de hogy melyik, az a konkrét modelltől függ.[4]

Hogy készülnek új modellek? Az 1960-as években Paul Cohen a semmiből robbant be a halmazelmélet élvonalába: ő bizonyította elsőként, hogy bizonyos modellekben $\aleph_1 < 2^{\aleph_0}$ teljesül, ezzel megválaszolva Hilbert híres első problémáját. Technikájának, a *forszolásnak* az alapötlete meglepően egyszerű: ha M egy halmazelméleti modell, akkor konstruálhatunk egy nagyobb N modellt úgy, hogy hozzáadunk M-hez egy G *generikus objektumot*. A G generikussal megnövelhetjük $2^{\aleph_0}$ értékét ami a kontinuumhipotézis sérüléséhez vezet. Cohent 1966-ban Fields-medállal jutalmazták halmazelméleti eredményeiért.

Az elmúlt ötven évben számos olyan érdekes és érdemben különböző modelljét konstruálták a matematikának amelyben vannak közbülső számosságok $\aleph_0$ és $2^{\aleph_0}$ között, és a modern halmazelmélet szignifikáns részben ilyen modellek vizsgálatával foglalkozik. Két modell, melyekben mondjuk $2^{\aleph_0} = \aleph_{16}$ ugyanúgy teljesül, viselkedhet nagyon különbözően, még csak az algebrát, mértékelméletet vagy topológiát tekintve is. Sokak meglepetésére

[2] Azaz a Zermelo–Fraenkel-axiómarendszer a kiválasztási axiómával (*Axiom of Choice*) kiegészítve.

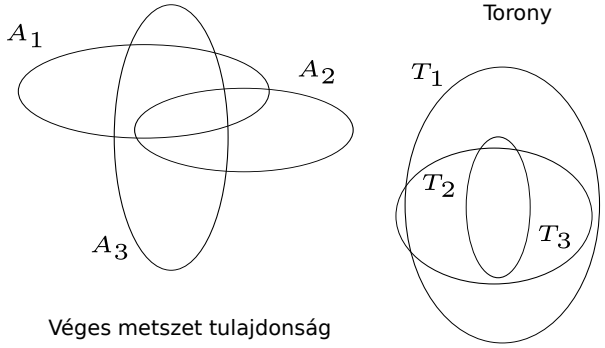
[3] Gondoljunk a felcserélhetőségre, zárójelezésre, vagy általában a *test axiómákra*.

[4] Ez a szituáció ugyancsak párhuzamban áll a modern, nem standard geometriák felfedezésével is a 19. században.

– a szokásos axiómákat használva – például eldönthetetlennek bizonyult a Whitehead-probléma a csoportelméletben, vagy külső automorfizmusok létezése a Calkin-algebrán.[5]

Ez motiválja, hogy egy finomabb kombinatorikus mértéket találjunk annál, minthogy egyedül $2^{\aleph_0}$ értékét, mely egyben $\mathbb{N}$ összes részhalmazainak száma is, vizsgáljuk. Ezzel a kérdéssel, és az $\aleph_0$ és $2^{\aleph_0}$ közötti számosságok vizsgálatával foglalkozik a *kontinuumszámosság-invariánsainak* elmélete.[6]

A terület egyik szépsége, hogy minimális előkészülettel is megérthetünk egy olyan új áttörő eredményt, mint amit Malliaris és Shelah beláttak. Mostantól csak természetes számokból álló halmazokkal foglalkozunk, és a következő, elsőre talán mesterségesnek tűnő kapcsolattal: ha A és B a természetes számok részhalmazai, akkor azt írjuk, hogy $A \subseteq^* B$, szóban A majdnem része B-nek, ha *A-nak véges sok kivétellel minden eleme B-ben is benne van*. Például, az $A = \{1, 2, 3, 4 \dots\}$ halmaz majdnem része a $B = \{3, 4, 5 \dots\}$ halmaznak, hisz az $1, 2$ elemektől eltekintve B minden eleme A-ban is benne van.



Mi az előnye egy ilyen gyenge relációval dolgozni a valódi tartalmazás helyett? Legyen A_n azon pozitív egész számok halmaza, melyek egy fix n számmal oszthatóak: tehát $A_1 = \mathbb{N}$ az összes szám, A_2 a páros számok halmaza, $A_3 = \{3, 6, 9 \dots\}$, és így tovább. Könnyen látszik, hogy ha veszünk véges sok ilyen $A_1, A_2 \dots A_n$ halmazt egy fix n-ig, akkor ezeknek végtelen a metszete.[7]

[5] A jelenleg ismert technikák fényében azonban nagyon valószínűtlen, hogy a híres Riemann-sejtés vagy a Navier–Stokes-egyenletek általános megoldhatósága független lenne a ZFC axiómáktól. Az ezen problémák megoldásáért kiírt Millennium Prize jelenleg egymillió dollárral jár.

[6] Angolul *cardinal characteristics of the continuum*.

[7] Persze, hiszen csak vegyük az $n! = 1 \cdot 2 \cdot \ldots \cdot n$ szorzat többszöröseit.

Ezt úgy is szoktuk mondani, hogy az $\{A_n\}$ halmazrendszer *véges metszet tulajdonságú*.

Persze olyan szám, ami az összes természetes számmal egyszerre osztható, nincsen, azaz egyszerre nincs valódi metszete az összes $A_1, A_2, A_3 \dots$ halmaznak. Ezzel szemben olyan végtelen B halmazokat könnyen találunk, melyre $B \subseteq^* A_n$ minden n-re. Hiszen elég, ha odafigyelünk arra, hogy B-nek az n-dik elemét az $A_1 \cap A_2 \cap \dots \cap A_n$ metszetből vegyük: konkrétan a $B = \{n! : n = 1, 2, 3 \dots\}$ választás például működni fog. Tehát a B halmaz lényegében az $\{A_n\}$ rendszer metszeteként viselkedik, és ezért *az* $\{A_n\}$ *rendszer pszeudometszetének* is nevezzük. Az is könnyen látszik, hogy B-t hozzáadva az $\{A_n\}$ rendszerhez a véges metszet tulajdonság még mindig teljesül.

Ha van egy tetszőleges $\mathcal{A}$ halmazrendszerünk a véges metszet tulajdonsággal, akkor azt ki lehet terjeszteni egy maximális $\mathcal{A}_{\max}$ halmazrendszerré, ami még mindig véges metszet tulajdonságú.[8] Ekkor azonban az $\mathcal{A}_{\max}$ rendszernek már nem lehet pszeudometszete. Ez vezet első fő definíciónkhoz: a $\mathfrak{p}$ invariáns a legkisebb olyan rendszer számossága, ami véges metszet tulajdonságú, de nincs pszeudometszete. A $\mathfrak{p}$ számosságot *pszeudometszet számnak* nevezik.

A fenti példa keretében lényegében láttuk, hogy egy a természetes számokkal indexelt, azaz megszámlálható és véges metszet tulajdonságú rendszernek mindig van pszeudometszete, tehát $\mathfrak{p}$ nem megszámlálható. Azaz:

$$\aleph_0 < \mathfrak{p} \leq 2^{\aleph_0}.$$

Ismerünk számos olyan modellt, amelyben a $\mathfrak{p} = 2^{\aleph_0}$ egyenlőség teljesül (és ez a közös érték lényegében bármely alef lehet); másrészt, az $\aleph_1 = \mathfrak{p} < 2^{\aleph_0} = \aleph_2$ egyenlőtlenség is könnyen előfordulhat különböző modellekben. Tehát a szokásos axiómák nem döntik el, hogy hol van $\mathfrak{p}$ az $\aleph_1, \aleph_2, \dots$ listában, sem azt, hogy $\mathfrak{p} = 2^{\aleph_0}$ vagy $\mathfrak{p} < 2^{\aleph_0}$ teljesül.

Szükségünk van még egy definícióra. Egy tipikus véges metszet tulajdonságú rendszerben semmi oka annak, hogy az elemek rendezve legyenek: az eredeti oszthatósági példánkban, ha csak p prímekre nézzük az A_p halmazokat, semelyik kettő nincs $\subseteq^*$ relációban. Tehát *toronynak* nevezünk egy olyan $\mathcal{T}$ rendszert, amelyben bármely két X, Y elemre vagy $X \subseteq^* Y$ vagy $Y \subseteq^* X$ teljesül. Más szóval, a $\subseteq^*$ reláció lineárisan rendezi $\mathcal{T}$-t. Az

[8] Ez a Zorn-lemma egy klasszikus alkalmazása.

úgynevezett *toronyszám* $\mathfrak{t}$ a legkisebb $\mathcal{T}$ torony mérete, aminek nincs pszeudometszete.

Nagy tornyok. Meglepő módon a megszámlálható $\mathbb{N}$ halmazban is lehet $2^{\aleph_0}$ méretű tornyot találni. Először is, soroljuk fel a racionális számokat mint $q_1, q_2, q_3 \dots$. Ezután minden valós r számra definiáljuk az X_r halmazt, ami azon n természetes számokból áll, hogy $q_n < r$. Tehát X_r pont az r valós számnál kisebb racionális számok indexei. Ha $r < t$ két valós szám, akkor X_r teljesen része X_t-nek, sőt X_t végtelen sok extra elemet is tartalmaz. Tudunk egy pszeudometszetet mondani erre a rendszerre is?

Könnyű látni, hogy minden torony véges metszet tulajdonságú, tehát a $\mathfrak{p}$ invariánsra a tanú legfeljebb akkora, mint $\mathfrak{t}$, és így a következő egyenlőtlenség teljesül:

$$\aleph_0 < \mathfrak{p} \leq \mathfrak{t} \leq 2^{\aleph_0}.$$

A $\mathfrak{t}$ számosság értéke, $\mathfrak{p}$-hez hasonlóan, manipulálható különböző alefekre. Sőt, több mint egy tucat, a $\mathfrak{p}$ és $\mathfrak{t}$-hez hasonló számosságinvariánst vizsgáltak az 1940-es évek óta $\aleph_0$ és $2^{\aleph_0}$ között, és a legtöbbről tudtuk, hogy bizonyos egyszerű összefüggésektől eltekintve, melyek már a 20. század közepén ismertek voltak, más kapcsolat, egyenlőtlenség nem bizonyítható. Azaz különböző forszolási technikák szofisztikált változataival és kombinációival pontosan beállíthatjuk nemcsak $2^{\aleph_0}$, hanem az invariánsok értékeit is olyan előre fixált alefekre, melyek a rég ismert egyenlőtlenségeket nem sértik.[9]

A jelenlegi legerősebb eredények akár öt külön értéket is tudnak egyszerre manipulálni.

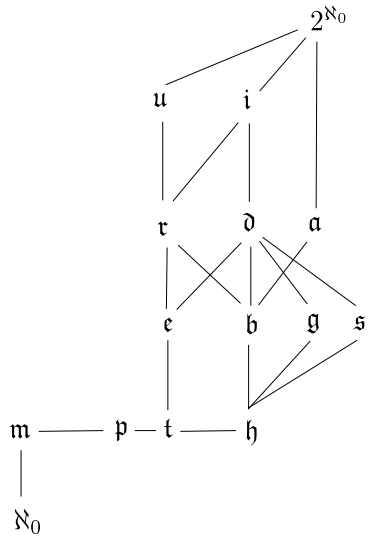
Mindezek ellenére az elmúlt hatvan évben nem sikerült olyan modellt konstruálni, melyben $\mathfrak{p}$ és $\mathfrak{t}$ ne lett volna egyenlő. Ugyanakkor az általánosan elfogadott sejtés szerint $\mathfrak{p} < \mathfrak{t}$ lehetségesnek látszott, bár azt tudtuk, hogy technikailag nem lehet könnyű egy ilyen bizonyítás: régóta ismert, hogy ha $\mathfrak{p} = \aleph_1$, akkor $\mathfrak{t} = \aleph_1$ is teljesül. Tehát $\mathfrak{p} < \mathfrak{t}$ csak úgy lehetséges, ha $2^{\aleph_0}$ nagyobb, mint $\aleph_2$, azonban ilyen modellek finomhangolása sokkal nehezebb feladat, mint amikor $2^{\aleph_0} \leq \aleph_2$.

Malliaris és Shelah új, váratlan tétele azt mondja ki, hogy

$$\mathfrak{p} = \mathfrak{t},$$

[9] További részletekért számosságinvariánsokról, klasszikus eredményekről A. Blass [1] áttekintését javasoljuk.

függetlenül attól, hogy milyen modellben vagyunk. Mit is kellett belátniuk a szerzőknek? Mivel $\mathfrak{p} \leq \mathfrak{t}$ ismert volt, ezért a $\mathfrak{t} \leq \mathfrak{p}$ összefüggésre volt szükség: azaz ha van egy tetszőleges véges metszet tulajdonságú $\mathcal{A}$ rendszerünk, aminek nincs pszeudometszete, akkor akármilyen bonyolult vagy véletlen átfedések is vannak $\mathcal{A}$ elemei között, valamilyen módon konstruálhatunk egy legfeljebb akkora $\mathcal{T}$ tornyot pszeudometszet nélkül, amiben tehát az elemek már rendezve vannak a $\subseteq^*$ relációval. A naiv ötlet, hogy $\mathcal{A}$ elemeiből próbáljunk tornyot építeni, hamar megbukik, hiszen lehet, hogy $\mathcal{A}$ semelyik két eleme nincs $\subseteq^*$ relációban.



Pár számosságinvariáns és bizonyítható kapcsolatuk

Malliaris és Shelah eredménye ahhoz hasonlítható, mintha belátnánk két egyenletről, hogy ugyanaz a megoldásuk, de anélkül, hogy valójában megtalálnánk, hogy mi is ez a közös érték. A ZFC-axiómák nem döntik el, hogy éppen $\mathfrak{p} = \aleph_1$ vagy $\mathfrak{p} = \aleph_2$, vagy $\mathfrak{p} = \aleph_3$, és hasonlóan $\mathfrak{t}$ értéke sem eldönthető. Viszont azt már be lehet látni, hogy bármi is $\mathfrak{p}$ értéke, $\mathfrak{t}$ vele egyenlő lesz.

Meg kell említenünk, hogy a szerzők nemcsak hogy megoldották $\mathfrak{p}$ és $\mathfrak{t}$ hatvan éve nyitott problémáját, de egy teljesen új kapcsolatot fedtek fel egy modellelméleti komplexitáshierarchia, a Keisler-rendezés struktúrája és a számosságinvariánsok elmélete között [6, 7, 8]; ezen eredmények vázolása azonban túlmutat jelen cikkünk keretein. Míg az eredeti bizonyítás a $\mathfrak{p} = \mathfrak{t}$

egyenlőségre komoly halmaz- és modellelméleti eszközöket használ,[10] olyan variánsok már elérhetőek, melyek csak alapvető ismereteket és egy kis kitartást igényelnek [9].

Egy nyitott probléma. Azt mondjuk, hogy egy rendszer $\mathcal{R}$ *szétvághatatlan* ha nincs olyan Y halmaz ami minden X-et $\mathcal{R}$-ből egyszerre szétvág, azaz a metszet $X \cap Y$ és a különbség $X - Y$ mind végtelenek. Legyen $\mathfrak{r}$ a legkisebb szétvághatatlan rendszer mérete. Továbbá legyen $\mathfrak{r}_\sigma$ (ejtsd 'er szigma') a legkisebb olyan rendszer mérete, amit megszámlálható sok $Y_0, Y_1, \dots$ halmazzal sem lehet szétvágni. Könnyen látszik, hogy $\aleph_0 < \mathfrak{r} \leq \mathfrak{r}_\sigma \leq 2^{\aleph_0}$, azonban nem tudjuk, hogy $\mathfrak{r} < \mathfrak{r}_\sigma$ lehetséges-e. A szakértők sejtése, hogy valójában $\mathfrak{r} = \mathfrak{r}_\sigma$, és ez eddig minden általunk ismert modellben teljesülni látszik [3].

Malliaris és Shelah eredménye távolról sem zárja le a számosságinvariánsok elméletét, sőt cikkeik valószínűleg számos új vizsgálat kezdőpontjai. Milyen számosságinvariáns kérdéseken dolgozik eközben egy hétköznapi halmazelmélész? Egyfelől, bizonyos rég ismert invariánsok kapcsolata a mai napig eldöntetlen (egy ilyen kérdést említünk a kiemelésben) [3]. Másrészt napjainkig definiálnak új, érdekes számosságinvariánsokat, melyek elhelyezése a klasszikus invariánsok diagramjában sokszor meglehetősen nehéz feladat [2]. Végül, egy igen gazdag terület van kibontakozóban olyan számosságinvariánsokról, melyek $\mathbb{N}$ részhalmazai helyett, valamely nem megszámlálható számosság részhalmazait tekintik [4].

Zárásként pár szó a főszereplőkről: Maryanthe Malliaris a Berkeley-n szerezte doktoriját 2009-ben, és jelenleg a University of Chicago professzora. A fiatal matematikusnő számos díjat nyert korábbi munkáiért is, és a 2018-as Nemzetközi Matematikai Kongresszus meghívott előadója.

Saharon Shelah neve sokaknak ismerős lehetett: a 72 éves matematikus 1023 publikált cikk szerzője (!), és komoly áttöréseket ért el a véges és végtelen kombinatorika, a modellelmélet, logika, és a csoportelmélet terén. A mai napig heti hat napot dolgozik, a tanévet megosztva a Rutgers, illetve a jeruzsálemi Héber Egyetem között.

[10] A Fields-medállal kitüntetett Timothy Gowers egy blogbejegyzése is foglalkozik ezzel a kérdéssel, l. https://gowers.wordpress.com/2017/09/19/two-infinities-that-are-surprisingly-equal/

A cikk részben az FWF Grant I1921 támogatásával készült. Köszönjük Bottyán Emese, Soukup Lajos, Vidnyánszky Zoltán és Zádorvölgyi Zita javaslatait a cikkel kapcsolatban.

Referenciák

[1] A. Blass, Combinatorial cardinal characteristics of the continuum, *Handbook of set theory*, pages 395–489, 2010.

[2] A. Blass, J. Brendle, W. Brian, J. D. Hamkins, M. Hardy and P. B. Larson, The rearrangement number, *arXiv preprint:1612.07830*, 2016.

[3] J. Brendle, Around splitting and reaping, *Commentationes Mathematicae Universitatis Carolinae*, **39** (1998), (2):269–279.

[4] J. Brendle, A. Brooke-Taylor, S.-D. Friedman and D. Montoya, Cichon's diagram for uncountable cardinals, to appear in *Israel Journal of Mathematics, arXiv:1611.08140*, 2016.

[5] G. Galilei, *Dialogue concerning the two chief world systems, Ptolemaic & Copernican*, Univ of California Press, 1967.

[6] M. Malliaris and S. Shelah, General topology meets model theory, on $\mathfrak{p}$ and $\mathfrak{t}$, *Proceedings of the National Academy of Sciences*, **110** (2013), (33):13300–13305.

[7] M. Malliaris and S. Shelah, Cofinality spectrum theorems in model theory, set theory, and general topology, *Journal of the American Mathematical Society* **29** (2016), (1):237–297.

[8] J. T. Moore, Model theory and the cardinal numbers $\mathfrak{p}$ and $\mathfrak{t}$, *Proceedings of the National Academy of Sciences* **110** (2013), (33):13238–13239.

[9] G. M. Roccasalvo, Ultraproducts of finite partial orders and some of their applications in model theory and set theory, *Master's thesis*, University of Torino, 2014.

Universität Wien
Kurt Gödel Research Center for Mathematical Logic
Austria
e-mail: daniel.soukup@univie.ac.at

Erdélyi Márton: A Lang–Trotter primitív pont sejtésről véges karakterisztikájú függvénytestek felett

1. Bevezetés

A Lang–Trotter primitív pont sejtés az Artin-féle primitív gyök sejtés elliptikus görbés megfelelője. A klasszikus esetben ($\mathbb{Q}$ felett) egyelőre elérhetetlennek tűnik az igazolása, viszont bizonyos más testek fölött könnyebb a helyzet, és vannak részeredmények. A továbbiakban egy ehhez használt bizonyítási módszert vizsgálunk, és egy kriptográfiai szempontból érdekes következményt is látni fogunk.

1.1. Az Artin-féle primitív gyök sejtés

Legyen $a \in \mathbb{Z}$ rögzített egész szám, továbbá X_a a prímszámok $\mathcal{P}$ halmazának azon részhalmaza, ami azokat a p prímeket tartalmazza, amire $a \pmod p$ primitív gyök (tehát $a, a^2, a^3, \ldots, a^{p-1} \equiv 1$ redukált maradékrendszer modulo p). Az Artin-féle primitív gyök sejtés az $X_a \subset \mathcal{P}$ halmaz „sűrűségére” vonatkozik.

Ha a négyzetszám, akkor nyilván $p > 2$-re nézve nem lehet primitív gyök, hiszen $a^{(p-1)/2} \equiv 1$ modulo p. Hasonlóan $a = -1$ sem lehet primitív gyök, mert ekkor $a^2 = 1$. Artin sejtése szerint minden más esetben X_a végtelen halmaz, sőt a Dirichlet-sűrűsége pozitív, és $q_a \cdot c_A$, ahol q_a egy a-tól függő pozitív racionális szám, és c_A az Artin-konstans:

$$c_A = \prod_{\ell \text{ prím}} \left(1 - \frac{1}{\ell(\ell-1)}\right) = \sum_{m \geq 1} \frac{\mu(m)}{m \cdot \varphi(m)} \simeq 0{,}37396.$$

A konstans a következő módon kapható meg. Ahhoz, hogy a primitív gyök legyen, az kell, hogy minden ℓ prímre az alábbi két feltétel legalább egyike ne teljesüljön: (1) $\ell | p-1$, azaz $p \equiv 1 \pmod \ell$, (2) $a^{(p-1)/\ell} \equiv 1 \pmod p$.

Artin észrevette, hogy ebben a bizonyos számtestek algebrai egészeinek számelmélete játszik szerepet: adott ℓ prímre legyen $L_\ell = \mathbb{Q}(\zeta_\ell, a^{1/\ell})|\mathbb{Q}$ testbővítés, ahol ζ_ℓ egy primitív ℓ-edik egységgyök. Ekkor $L_\ell|\mathbb{Q}$ Galois-bővítés. L_ℓ algebrai egészeinek gyűrűje egy Dedekind-gyűrű, és fenti feltételek pontosan akkor teljesülnek ℓ-re, ha p teljesen szétesik az $L_\ell|\mathbb{Q}$

bővítésben. Ha a négyzetmentes, akkor $|L_\ell : \mathbb{Q}| = \ell(\ell-1)$, így a Csebotarev sűrűségi tétel szerint az ilyen ℓ prímek sűrűsége $1/\ell(\ell-1)$.

Tehát a számunkra kérdéses sűrűség várhatóan éppen c_A. A q_a számok azért kellenek, mert az L_ℓ bővítések csak a négyzetmentes esetben épp ekkorák, és általában nem mindig függetlenek, ami viszont befolyásolja a várt sűrűséget.

Az általánosított Riemann-hipotézis mellett Hooley bizonyította az Artin-féle primitív gyök sejtést ([7]). Enélkül azt lehet tudni, hogy a sejtés körülbelül igaz: ha csak olyan a-kra vizsgáljuk, amik prímek (ebből könnyen levezethető az általános állítás), akkor Heath-Brown tétele szerint legfeljebb 2 prímszámra nem igaz a sejtés – de nem tudni melyikre ([6]). Tehát egyelőre egyetlen a számot sem tudunk mondani, amire X_a sűrűsége biztosan pozitív ([5]).

1.2. A Lang–Trotter primitív pont sejtés

A fenti kérdés átfogalmazható elliptikus görbékre, ez a Lang–Trotter primitív pont sejtés ([10]). Az elliptikus görbék olyan görbék, amelyek pontjain természetes módon van egy kommutatív csoportstruktúra.

Legyen most E egy elliptikus görbe és A egy rögzített pont E-n. Az Artin-sejtéshez analóg kérdés, hogy mely p prímszámokra lesz a modulo p vett görbe csoportjában (ez véges sok esettől eltekintve egy elliptikus görbe a véges test felett) generátorelem A képe. Erre akkor lehet esély, amikor a redukált görbe csoportja ciklikus, ami a klasszikus Artin-sejtésben szereplő $(\mathbb{Z}/p\mathbb{Z})^*$-gal ellentétben nem mindig igaz. Ha A torziópont, akkor nyilván nem lehet végtelen sokszor generátor a képe: elég nagy prímekre a redukált görbének több pontja van, mint A rendje, így a többszörösei nem adják ki az egész görbét.

A fenti heurisztika erre az esetre is működik, de a helyzet jóval bonyolultabbnak tűnik az Artin-sejtésnél – még az általánosított Riemann-hipotézis felhasználásával sem jutunk eredményre, mert túl nagy hibatagot kapunk. Jelenleg abban az esetben tudunk valamit mondani, ha E CM görbe (azaz az endomorfizmus-gyűrűje nagy). Illetve az általános esetben, ha a görbe legalább 18 rangú (tehát $\mathbb{Z}^{18}$ részcsoportja E-nek), akkor egy hasonló állítás igaz: ha veszünk 18 lineárisan független pontot, akkor ezek képe generálja a redukált görbék egy pozitív sűrűségű részét ([5]).

1.3. A továbbiak összefoglalása

A következőkben olyan felállásban vizsgáljuk a kérdést, ahol sokkal többet tudunk: a Dedekind-gyűrűk egy másik, jelentős csoportja a véges test feletti algebrai görbék koordinátagyűrűi. A prímek véges testbővítésbeli elágazási tulajdonságai hasonlóan vizsgálhatók, mint a klasszikus esetben. A véges karakterisztikájú függvénytestekre Weil bebizonyította az általánosított Riemann-hipotézist ([13]), és sok klasszikus számelméleti tétel sokkal erősebb változata igaz – a Csebotarev sűrűségi tételé is. Ennek következtében meg tudtak válaszolni néhány olyan kérdést, ami a klasszikus esetben egyelőre elérhetetlennek tűnik.

Legyen K egy véges karakterisztikájú függvénytest (pl. $K = \mathbb{F}_q(T)$ – egy véges test feletti egyváltozós racionális függvények teste), o_K az egészek gyűrűje ($\mathbb{F}_q[T]$), és legyen E/K egy elliptikus görbe. Ekkor ha ν egy prímideál o_K-ban (egy irreducibils polinom $\mathbb{F}_q[T]$-ben), akkor az E-t megadó egyenletet modulo ν tekintve egy véges k_ν test feletti E_ν elliptikus görbét kapunk (ami nem elfajuló, ha ν nem osztja E diszkriminánsát).

A cikkben vizsgált kérdések rögzített E-re a redukált görbék bizonyos tulajdonságait járják körül: milyen „valószínűséggel" lesz E_ν csoportja ciklikus ([2]), vagy az elemszáma négyzetmentes ([3]), illetve az eredeti kérdést: ha rögzítünk egy pontot (rácsot) E-n, akkor ennek a pontnak (rácsnak) a képe mikor generálja a redukált görbét ([8]).

A valószínűség alatt a következőket értjük:

- rögzített n-re a véges sok n fokú értékelési hely (irreducibilis polinom) közül véletlenszerűen választva mekkora valószínűséggel igaz a vizsgált tulajdonság,
- az összes értékelési hely között mekorra a Dirichlet-sűrűsége azoknak, amikre teljesül a vizsgált tulajdonság,
- mikor lesz ez a valószínűség/sűrűség 0.

A megoldások elég hasonló sémával működnek: szitaformulát alkalmazunk, és utána az alapkérdést át tudjuk fogalmazni bizonyos Frobenius-konjugált osztályokra (eddig a klasszikus esetben is megy), amire egy erős, effektív Csebotarev sűrűségi tételt lehet alkalmazni.

A következő fejezetben összeszedjük azokat a tudnivalókat, amik a megoldásokhoz kellenek. Az ezt követő részekben egy-egy kérdést vizsgálunk meg, és a ma ismert eredményeket foglaljuk össze: az elsőnél a megoldási

séma egyszerűen és gyorsan működik, a továbbiakban egyre nehezebb dolgunk lesz. Az utolsó fejezetben az eredményeinknek az elliptikus görbés nyilvános kulcsú kódolásokkal való összefüggéséről lesz szó.

2. Előzetes tudnivalók, jelölések

2.1. Függvénytestek és értékelések

Legyen K egy $p < \infty$ karakterisztikájú függvénytest, melyben az alaptest lezártja $k = \mathbb{F}_q$ valamely $q = p^f$-re. Jelöljük K értékeléseinek halmazát V_K-val, és $\nu \in V_K$-ra ν foka legyen $\deg(\nu) = [k_\nu : \mathbb{F}_q]$.

A legismertebb példa egy véges test feletti racionális törtfüggvények teste: $K = \mathbb{F}_q(T)$, ekkor $k = \mathbb{F}_q$, és a következők az értékelések:

- Ha $\nu \in \mathbb{F}_q[T]$ egy irreducibilis polinom, akkor ez természetes módon megad egy $\mathbb{F}_q(T) \to \mathbb{Z} \cup \{\infty\}$ értékelést, amit szintén ν-vel jelölünk: tetszőleges $f \in \mathbb{F}_q[T] \setminus \{0\}$ polinomra legyen $\nu(f) = \max(n \in \mathbb{N} : \nu^n | f)$, $f/g \in \mathbb{F}_q(T)$-re $\nu(f/g) = \nu(f) - \nu(g)$, és $\nu(0) = \infty$. Ekkor $\deg(\nu)$ a hagyományos fokszám.
- A végtelen értékelés $\nu_\infty : \mathbb{F}_q(T) \to \mathbb{Z} \cup \{\infty\}$, amire $\nu_\infty(f/g) = \deg(g) - \deg(f)$, és $\nu_\infty(0) = \infty$. Ekkor $\deg(\nu_\infty) = 1$.

Egy $n \in \mathbb{N}$-re legyen $V_K(n) = \{\nu \in V_K | \deg(\nu) = n\}$ – ez egy véges halmaz, elemszáma $q^n/n + o(q^{n/2})$, és $S \subset V_K$ részhalmazra legyen $S(n) = S \cap V_K(n)$. Az S részhalmaz sűrűségét a következő módon értelmezhetjük: legyen $\delta(S, n) = |S(n)|/|V_K(n)|$, továbbá

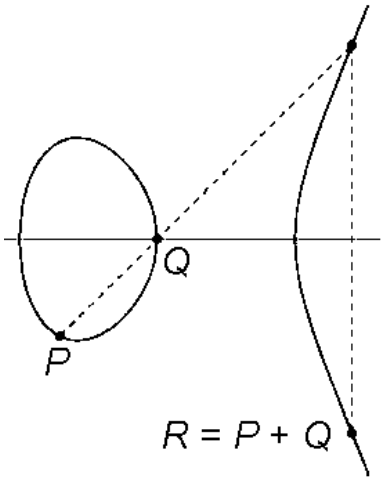
$$\delta(S) = \lim_{s \to 1+0} \frac{\sum_{\nu \in S} q^{-s \deg(\nu)}}{\sum_{\nu \in V_K} q^{-s \deg(\nu)}},$$

a Dirichlet-sűrűség. Ekkor $0 \leq \delta(S) \leq 1$, és ha $|S|$ véges, akkor $\delta(S) = 0$.

2.2. Elliptikus görbék

Legyen $E/K : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ $(a_i \in K)$ projektív algebrai görbe.

A görbe $\Delta(E)$ diszkriminánsa az a_i-k egy polinomja, a görbe pontosan akkor sima, ha $\Delta(E)\neq 0$. A görbe j-invariánsa az a_i-k egy racionális törtfüggvénye – $j(E)\in K$. Ha két görbére $j(E)=j(E')$, akkor E és E' izomorf K egy legfeljebb másodfokú bővítése felett – tehát a j-invariáns többé-kevésbé az elliptikus görbék izomorfizmus osztályait adja meg. Mostantól feltesszük, hogy $j(E)\notin k$, mert a konstans j-invariánsú görbék a mi kérdéseinkben a többitől eltérő, általában egyszerűbb esetet adnak – ami többé-kevésbé a klasszikus CM esetnek felel meg. Az egy génuszú projektív algebrai görbék pontosan a sima elliptikus görbék, és ha az egyetlen végtelen távoli pontjuk az $O[0,1,0]$, akkor olyan alakúak, mint a fenti E.



Ekkor a $\overline{K}$ algebrai lezártban a görbe pontjain természetes módon definiálható a következő művelet ($+$): Ha $P\neq Q\in E$, akkor a két pontot összekötő egyenes metszi E-t egy harmadik pontban (multiplicitással számolva) – ez $-(P+Q)$. Ezt összekötve O-val, a harmadik metszéspont $R=P+Q$. (Ha $P=Q$, akkor a két pontot összekötő egyenes az érintő.) Ez a művelet egy kommutatív csoportstruktúrát ad E pontjain, az egységelem O.

Ha $L|K$ testbővítés, akkor $E(L)$-lel jelöljük a görbe L-pontjait, ekkor $E(L)\leq E(\overline{K})$.

Ismert, hogy $E(K)$ végesen generált, és ha $E[m]=\{P\in E(\overline{K})|m\cdot P=0\}$ az m-torzió, akkor $E[m]=(\mathbb{Z}/m\mathbb{Z})^e$, $(m,p)=1$ esetén $e=2$, és a feltételeink mellett, ha $m=p^k$, akkor $e=1$.

Legyen $K_m=K(E[m])|K$ az a testbővítés, ahol az m-torziópontok koordinátáival ($x=X/Z$ és $y=Y/Z$) bővítjük K-t. Ekkor $K_m|K$ Galois-bővítés, és ha rögzítünk két független torziópontot, akkor a $G_m=\mathrm{Gal}(K_m/K)\leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ természetes módon: hiszen egy $\sigma\in G_m$ automorfizmus $E[m]$-t önmagába képzi, ráadásul a csoportműveletre lineárisan.

Legyen $(m,p)=1$. $K_m|K$ felbontható két részre: Legyen $\mathbb{F}_{q^{c_m}}$ az alaptest bővítése, tehát $\overline{\mathbb{F}}_q^{K_m}$. Ekkor a skalár bővítés $G_m^{(\text{skalár})}=\mathrm{Gal}(K\mathbb{F}_{q^{c_m}}/K)$, a geometriai $G_m^{(\mathrm{geom})}=\mathrm{Gal}(K_m/K\mathbb{F}_{q^{c_m}})$. Így a következő egzakt sorozatot

kapjuk:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_m^{(\mathrm{geom})} & \longrightarrow & G_m & \longrightarrow & G_m^{(\text{skalár})} = \langle q \rangle & \longrightarrow & 1 \\ & & \wedge| & & \wedge| & & \wedge| & & \\ 1 & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) & \xrightarrow{\det} & (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & 1 \end{array}$$

Az algebrai bővítésre mindig igaz, hogy $c_m = \mathrm{ord}_m(q)$, tehát q multiplikatív rendje modulo m. Mivel feltettük, hogy $j(E) \notin k$, a geometriai bővítés majdnem mindig maximális – tehát $G_m^{(\mathrm{geom})} = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.

Ha ν nem osztja $\Delta(E)$-t, akkor az egyenletet modulo ν nézve kapunk egy sima E_ν elliptikus görbét k_ν felett. Legyen az ilyen értékelési helyek halmaza $V_{E/K}$, és $V_{E/K}(n) = V_{E/K} \cap V_K(n)$. Az ilyen ν-kre $E_\nu(k_\nu)$ véges, tehát $E_\nu(k_\nu)$ csoportja izomorf $\mathbb{Z}_{d_\nu} \times \mathbb{Z}_{d_\nu e_\nu}$-vel alkalmas $d_\nu, e_\nu \in \mathbb{N}$-re. Legyen $a_\nu = q^{\deg(\nu)} + 1 - |E_\nu(k_\nu)|$. Ekkor Hasse tétele szerint $|a_\nu| \leq 2q^{\deg(\nu)/2}$. Egy $A \in E(K)$ pont képe a redukciónál legyen $A_\nu \in E_\nu(k_\nu)$.

2.3. Frobenius-konjugált osztályok és Csebotarev sűrűségi tétele

Legyen $L|K$ egy Galois-bővítés, $\nu \lhd o_K$ egy nem elágazó prím (tehát L-ben minden prím, ami osztja ν-t, legfeljebb egy multiplicitással szerepel), $V \lhd O_L$ egy ν feletti prím. A klasszikus esetben a Gauss-egészeknél (az $L = \mathbb{Q}(i)|K = \mathbb{Q}$ testbővítésre, ahol az egészek gyűrűje $O_L = \mathbb{Z}[i] \geq O_K\mathbb{Z}$) egyetlen prím elágazó: $(2) = (1+i)^2$ – tehát elágazik. Ha a ν egy $4k+1$ alakú prímszám által generált ideál, akkor $\nu \cdot O_L$ két különböző $\mathbb{Z}[i]$-beli prímideál szorzatára bomlik, ha pedig $4k+3$ alakú, akkor $\nu \cdot O_L \leq \mathbb{Z}[i]$ prímideál, így ha ν páratlan prím által generált ideál, akkor nem elágazó.

Ekkor $\mathrm{Gal}(L/K) \geq \{\sigma | \sigma V = V\} \simeq \mathrm{Gal}(k_V/k_\nu)$, és az utóbbi véges testek bővítésének Galois-csoportja – tehát ciklikus, és van egy kitüntetett generátoreleme, a Frobenius-automorfizmus, ami minden x elemet $x^{q^{\deg(\nu)}}$-be küld. Ennek az elemnek az előbbi izomorfizmusnál vett ősképét (ami $\mathrm{Gal}(L/K)$ egy eleme) nevezzük ν V-hez tartozó Frobenius-elemének, és $\Phi_{\nu,V}$-vel jelöljük. Ha V helyett egy másik ν feletti prímet választunk, akkor a Frobenius-elem konjugálódik. Az egész konjugált osztály a ν Frobenius-konjugált osztálya, és a jele $\Phi_\nu = \Phi_{\nu,L/K}$.

A Frobenius-konjugált osztály a prím elágazási tulajdonságaitól függ: a klasszikus példánkban a $4k+1$ alakú prímek szétesnek, tehát $k_V \simeq k_\nu$, így $\Phi_\nu = \{\mathrm{id}\}$. A $4k+3$ alakú prímek nem esnek szét, tehát a $k_V|k_\nu$ bővítés

másodfokú, és Φ_ν a $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ generátor elemét tartalmazó konjugált osztály.

Nekünk a $\nu \in V_{E/K}$ prímek K_m-beli elágazási tulajdonságaira lesz szükségünk. Legyen V egy ν feletti prím. Ekkor $g = \Phi_{\nu,V} \in G_m$ természetes módon $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ egy eleme. g hatása az m-torziópontokon a definíció szerint a véges test q-Frobeniusa, tehát pontosan akkor van m-torziópont $E_\nu(k_\nu)$-ben, ha g-nek sajátértéke 1. Másrészt g hat E_ν-n is, és hasonló módon $E_\nu(k_\nu) = \mathrm{Ker}(g-1)$. Egész pontosan le lehet írni, hogy melyik elem $\Phi_{\nu,V}$, nekünk azonban elég lesz a következő két tulajdonsága. A determinánsa kongruens $q^{\deg(\nu)}$-vel modulo m, és a nyoma összefüggésben van a görbe pontjainak számával: $\mathrm{tr}(g) \equiv a_\nu = q^{\deg(\nu)} + 1 - |E_\nu(k_\nu)| \pmod m$.

Legyen most $L|K$ véges Galois-bővítés, amelyik k véges test felett definiált sima projektív görbék Galois-fedéséből jön (nálunk mindig ilyen lesz, legtöbbször $L = K_m$ valamely m-re), és $G = \mathrm{Gal}(L/K)$. Ekkor a prímek véges S halmazán kívül a többi nem elágazó, legyen $|S| = \sum_{\nu\in S} \deg(\nu)$. Legyen c az a szám, hogy az alaptest algebrai lezártja L-ben k c fokú bővítése, és legyen tetszőleges $n \in \mathbb{N}$-re és $C \subset G$ konjugált osztályra $\pi(n, L/K, C) = \#(\nu \in V_K(n) \setminus S | \Phi_\nu = C)$.

A klasszikus esettől eltérően, adott n-re nem feltétlen fordulhat elő minden konjugált osztály Frobenius-osztályként, hiszen ha $c \nmid n$, akkor az $x \mapsto x^n$ nincs is benne $\mathrm{Gal}(k_V/k_\nu)$-ben.

1. Tétel (Csebotarev sűrűségi tétel, [11] Theorem 2)**.** *Ha $c \nmid n$, akkor $\pi(n, L/K, C) = 0$, különben*

$$\left|\pi(n, L/K, C) - \frac{c\cdot|C|}{|[L:K]|}|V_K(n)|\right| \leq 2|C|^{1/2}\left((3g_K + (\rho+1)|S|)\frac{q^{n/2}}{n} + \frac{|S|}{2n}\right) + |S|,$$

ahol g_K a K test (és a megfelelő projektív görbe) génusza – $K = \mathbb{F}_q(T)$ esetén 0 – és ρ bizonyos K-tól függő konstans. (ρ L-től való függetlensége a $p < 5$ esetben a [4] Section 2-ben van bizonyítva.)

Ez pont azt állítja, hogy a lehetséges konjugált osztályok nagyjából a konjugált osztály méreteivel arányos sűrűséggel fordulnak elő. A hibatag sokkal jobb, mint a klasszikus esetben, ott csak $o(q^n)$-t tudunk mondani. A $K_m|K$ bővítésekre $|S|$ becsülhető a nem sima redukciójú $\nu \in V_K \setminus V_{E/K}$ értékelési helyek fokszámösszegével, ekkor a hibatag $O_E(|C|^{1/2}q^{n/2}/n)$.

3. Ciklikusság

Először azt nézzük meg, hogy a redukált görbék pozitív sűrűséggel ciklikusak-e – ez nyilván szükséges feltétele annak, hogy A_ν generátor legyen.

Jelöljük $\delta_{\text{cikl}}(E/K)$-val a $\{\nu \in V_{E/K} | E_\nu(k_\nu) \text{ ciklikus}\} \subset V_{E/K}$ halmaz sűrűségét (meg fogjuk mutatni, hogy ez létezik).

$E_\nu(k_\nu)$ csoportja pontosan akkor ciklikus, ha semelyik $\ell \neq p$ prímre $E_\nu[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ nem részcsoportja. Továbbá $E_\nu[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ pontosan akkor van benne $E_\nu(k_\nu)$-ben, ha a $\Phi_{\nu,K_m/K}$ Frobenius-konjugált osztály az identitás.

Így egy egyszerű szitával a következőt kapjuk:

$$\begin{aligned}&\#(\nu \in V_{E/K}(n) | E_\nu(k_\nu) \text{ ciklikus})\\ &\quad = \sum_{p \nmid m} \mu(m) \# \left(\nu \in V_{E/K}(n) | E_\nu[m] \leq E_\nu(k_\nu)\right).\end{aligned}$$

A szitának nagyon kevés tagja nem 0, mert Hasse tétele szerint $m^2 \leq q^n + 2q^{n/2} + 1$ kell legyen, azaz $m \leq q^{n/2} + 1$, és ráadásul a Csebotarev-tételben csak akkor nem 0 a kapott sűrűség, ha $c = c_m | n$, azaz ha $m | q^n - 1$ (ez lényegében a Weil-párosítás). A maradék tagok pedig

$$\begin{aligned}&\#(\nu \in V(E/K, n) | E_\nu(k_\nu) \text{ ciklikus})\\ &\quad = \sum_{\substack{m \leq q^{n/2}+1 \\ m | q^n - 1}} \mu(m) \# \left(\nu \in V(E/K, n) | E_\nu[m] \leq E_\nu(k_\nu)\right)\\ &\quad = \sum_{\substack{m \leq q^{n/2}+1 \\ m | q^n - 1}} \left(\frac{\mu(m) c_m q^n}{|G_m| \cdot n} + O_E\left(\frac{q^{n/2}}{n}\right)\right)\\ &\quad = \sum_{\substack{m \leq q^{n/2}+1 \\ m | q^n - 1}} \frac{\mu(m) \text{ord}_m(q) q^n}{|G_m| \cdot n} + O_{E,\varepsilon}\left(\frac{q^{(1/2+\varepsilon)n}}{n}\right).\end{aligned}$$

Például ha $q = 2$ és $2^n - 1$ Mersenne prím, akkor csak az $m = 1$-nek megfelelő tag marad, tehát az összes redukált görbe ciklikus. Ezek alapján

2. Tétel ([2] Theorem 1, $p < 5$-re [4] Theorem 1)**.**

$$\left| \#(\nu \in V_{E/K}(n) | E_\nu(k_\nu) \text{ ciklikus}) - \delta_{\text{cikl}}(E/K, n) \frac{q^n}{n} \right| < O_{E,\varepsilon}\left(\frac{q^{(1/2+\varepsilon)n}}{n}\right),$$

ahol $\delta_{\text{cikl}}(E/K,n) = \sum_{m|q^n-1} \frac{\mu(m)\text{ord}_m(q)}{|G_m|}$. *Ezek segítségével standard módon kiszámolható a Dirichlet-sűrűség:*

$$\delta_{\text{cikl}}(E/K) = \sum_{(m,p)=1} \frac{\mu(m)}{|G_m|}.$$

Itt nem kapunk szorzatalakot, mert a G_m-ek rendje nem multiplikatív: véges sok ℓ-től eltekintve ugyan $G_\ell \simeq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, de a skalárbővítések a véges test $\text{ord}_\ell(q)$ rendű bővítései, amik nem függetlenek. (A geometriai bővítések véges sok prímtől eltekintve viszont függetlenek.)

Ha az E görbe csoportja nem ciklikus – tehát ha tartalmaz torziópontot, akkor a redukció csak akkor lehet ciklikus, ha a pont képe az új görbe egységeleme, ami viszont csak véges sokszor fordulhat elő. Tehát ilyenkor $\delta_{\text{cikl}}(E/K) = 0$. Meglepő módon máskor is lehet a Dirichlet-sűrűség 0:

3. Állítás ([4] Theorem 2)**.** $\delta_{\text{cikl}}(E/K) = 0 \iff \delta_{\text{cikl}}(E/K,1) = 0$. *Legyen K rögzített, ebben az esetben pontosan akkor létezik olyan E elliptikus görbe, aminek a csoportja ciklikus és $\delta_{\text{cikl}}(E/K) = 0$, ha $q-1$-nek legalább 3 prímosztója van.*

4. Négyzetmentes elemszám

Ebben a részben azt vizsgáljuk meg, hogy mikor lesz $|E_\nu(k_\nu)|$ négyzetmentes – pontosabban $|E_\nu(k_\nu)|$ p-hez relatív prím része (amit $|E_\nu(k_\nu)|'$-vel jelölünk) négyzetmentes. Jelöljük a megfelelő Dirichlet-sűrűséget $\delta_{\text{nm}}(E/K)$-val.

Ha azt akarjuk leírni, hogy p^2 mikor osztja $|E_\nu(k_\nu)|$-t, akkor egy másik (nem $K_m|K$ alakú) testbővítést kell vizsgálnunk. Ettől az egyszerűség kedvéért most eltekintünk, $(\mathbb{Z}/p\mathbb{Z})^2$ úgysem lehet részcsoportja a redukált görbének – tehát az előbbinél erősebb feltételünk van, amit szintén le lehet írni bizonyos Frobenius-konjugált osztályokkal:

Ha $(m,p)=1$ és $g = \Phi_{\nu,K_{m^2}/K}$, akkor $m^2||E_\nu(k_\nu)| \iff m^2|\det(g) - \text{tr}(g)+1 \equiv 0 \pmod{m^2}$. Az ilyen konjugált osztályokat könnyű megtalálni: legyen

$$C_{m^2}^{(n)} = \Big\{ g \in \text{GL}_2(\mathbb{Z}/m^2\mathbb{Z}) | \det(g) \equiv q^n \pmod{m^2}, \det(g) - \text{tr}(g) + 1 \equiv 0 \pmod{m^2} \Big\}.$$

Ekkor $\ell \neq p$ prímre

$$\left|C_{\ell^2}^{(n)}\right| = \begin{cases} \ell^4 + \ell^3, & \text{ha } q^n \not\equiv 1 \pmod{\ell}, \\ \ell^4 + \ell^3 - \ell^2, & \text{ha } q^n \equiv 1 \pmod{\ell}. \end{cases}$$

Összességében $\left|C_{m^2}^{(n)}\right| \leq m^4 \prod_{\ell|m}(1 + 1/\ell) = O(m^4 \log\log m)$ és $\left|C_{m^2}^{(n)}\right| / \left|G_{m^2}^{(n)}\right| = O(m^{-2} \log\log m)$, ahol

$$G_{m^2}^{(n)} = \{g \in G_{m^2} | \det(g) \equiv q^n \pmod{m^2}\}.$$

Fontos különbség a ciklikus esethez képest, hogy itt nincs oszthatósági feltétel m-re, tehát a szitában jóval több tagot kapunk, ezért a nagy m-ekre más becslést kell alkalmazni. Ezért osszuk ketté a szita tagjait egy később, optimálisan megválasztott y-nál:

$$\begin{aligned} &\#\left(\nu \in V_{E/K}(n) || E_\nu(k_\nu)|' \text{ négyzetmentes}\right) \\ &\quad = \sum_{\substack{m \leq q^{n/2}+1 \\ (m,p)=1}} \mu(m) \cdot \#\left(\nu \in V_{E/K}(n) | m^2 || E_\nu(k_\nu)|\right) \\ &\quad = \sum_{\substack{m \leq y \\ (m,p)=1}} \mu(m) \cdot \#\left(\nu \in V_{E/K}(n) | m^2 || E_\nu(k_\nu)|\right) \\ &\qquad + O\left(\sum_{\substack{y < m \leq q^{n/2}+1 \\ (m,p)=1}} \#\left(\nu \in V_{E/K}(n) | m^2 || E_\nu(k_\nu)|\right)\right) \\ &\quad =: S_{\text{fo}} + S_{\text{hiba}}. \end{aligned}$$

Az első részre a Csebotarev-tételt alkalmazva:

$$\begin{aligned} S_{\text{fo}} &= \sum_{\substack{m \leq y \\ (m,p)=1}} \mu(m) \cdot \#\left(\nu \in V_{E/K}(n) | \Phi_{\nu, K_{m^2}/K} \subset C_{m^2}^{(n)}\right) \\ &= \left(\sum_{\substack{m \leq y \\ (m,p)=1}} \mu(m) \frac{\operatorname{ord}_{m^2}(q) \left|C_{m^2}^{(n)}\right|}{|G_{m^2}|}\right) \frac{q^n}{n} \\ &\quad + O\left(\sum_{\substack{m \leq y \\ x \equiv 1 \pmod{\operatorname{ord}_{m^2}(q)}}} \left|C_{m^2}^{(n)}\right|^{1/2} \frac{q^{n/2}}{n}\right) \end{aligned}$$

$$= \left(\sum_{\substack{m \geq 1 \\ (m,p)=1}} \mu(m) \frac{\left| \mathrm{ord}_{m^2}(q) \cdot C_{m^2}^{(n)} \right|}{|G_{m^2}|} + O_E\left(\frac{\log\log y}{y} \right) \right) \frac{q^n}{n}$$
$$+ O_E\left(\frac{q^{n/2} y^3 (\log\log y)^{1/2}}{n} \right).$$

A nagy m-ekhez tartozó tagok becsléséhez azt használjuk, hogy a redukált görbék elemszáma nemcsak véges sok féle lehet (a Hasse-tétel szerint $q^n - 2q^{n/2} + 1 \leq |E_\nu(k_\nu)| \leq q^n + 2q^{n/2} + 1$)), hanem ez a véges sok lehetőség többé-kevésbé egyenletesen oszlik el (az igazság az, hogy van néhány érték, ami nagyon kevésszer szerepel, és a $q+1$-hez közeliek gyakrabban fordulnak elő az átlagosnál), és van egy használható becslésünk az adott elemszámú görbék számára:

4. Tétel ([12] Theorem 2.8, [3])**.**

$$\#(\nu \in V_{E/K}(n) | a_\nu = a) = O_E(q^{n/2} n^2).$$

Itt a konstans igazából csak $j(E)$ fokszámától függ.

Így ν-ket az $a = a_\nu$ szerint szétválasztva

$$S_{\text{hiba}} = O\left(\sum_{|a| < 2q^{n/2}} \sum_{\substack{y < m \leq q^{n/2}+1 \\ m^2 | q^n - a + 1}} \#\left(\nu \in V_{E/K}(n) | a_\nu = a \right) \right)$$
$$= O_E\left(\sum_{|a| < 2q^{n/2}} \sum_{\substack{y < m \leq q^{n/2}+1 \\ m^2 | q^n - a + 1}} q^{n/2} n^2 \right)$$
$$= O_E\left(q^{n/2} n^2 \sum_{y < m} \frac{q^{n/2}}{m^2} \right) = O_E\left(\frac{q^n n^2}{y} \right).$$

Ezek alapján az $y \simeq q^{n/8} \cdot n^{3/4}$ választással azt kapjuk, hogy

5. Tétel ([3])**.**

$$\#\left(\nu \in V_{E/K}(n) || E_\nu(k_\nu)|' \text{ négyzetmentes} \right)$$

$$= \delta_{\mathrm{nm}}(E/K,n)\frac{q^n}{n} + O_E\left(q^{\frac{7}{8}n}\cdot n^{\frac{5}{4}}\right),$$

ahol $\delta_{\mathrm{nm}}(E/K,n) = \left(\sum_{\substack{m\geq 1\\(m,p)=1}} \mu(m)\frac{\mathrm{ord}_{m^2}(q)\cdot\left|C_{m^2}^{(n)}\right|}{|G_{m^2}|}\right)$. *Továbbá ha* $\overline{C}_{m^2} = \sum_{1\leq n\leq \mathrm{ord}_{m^2}(q)} \left|C_{m^2}^{(n)}\right|$, *akkor*

$$\delta_{\mathrm{nm}}(E/K) = \sum_{\substack{m\geq 1\\(m,p)=1}} \mu(m)\frac{\overline{C}_{m^2}}{|G_{m^2}|}.$$

5. A Lang–Trotter-sejtés

Most már az eredeti kérdést vizsgáljuk: hogy milyen sűrűséggel lesz egy pont képe generátor.

Legyen $A\in E(K)$ rögzített, $m\in\mathbb{N}$-re $E[m^{-1}A] = \{B\in E | m\cdot B = A\}\subset E$ és $A_m\in E[m^{-1}A]$ egy kiválasztott pont. Tekintsük az alábbi testbővítést: $L_{A,m} = K(E[m], E[m^{-1}A])|K$, ahol megint a megfelelő pontok koordinátáival bővítjük K-t.

Ha A nem torziópont, akkor majdnem minden ℓ prímre

$$H_{A,\ell} = \mathrm{Gal}(L_{A,\ell}/K)\leq \mathrm{Aff}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

ami $E[\ell^{-1}]\simeq(\mathbb{Z}/\ell\mathbb{Z})^2$ eltolásainak $T_{A,\ell}$ csoportjának bővítése G_ℓ-lel. $H_{A,\ell}$ természetes módon hat $E[\ell^{-1}A]$-n az affin csoport részcsoportjaként: minden eleme reprezentálható egy (γ,τ) párral valamely $\gamma\in G_\ell$-re és $\tau\in T_{A,\ell}$-re, ekkor egy $B\in E[\ell^{-1}]$ pontra $(\gamma,\tau)B = B_0+\gamma(B-B_0)+\tau$.

Ha ℓ olyan, mint az előbbi bekezdésben, akkor $\nu\in V_{E/K}(n)$-ra pontosan akkor lesz $\langle A_\nu\rangle\leq E_\nu(k_\nu)$ indexe osztható az ℓ-lel, ha $(\gamma,\tau)\in\Phi_{\nu,L_{A,\ell}/K}\subseteq H_{A,\ell}$-ra γ féligegyszerű, sajátértéke 1, és ha $\gamma\neq\mathrm{id}$, akkor $\tau\in\mathrm{Im}(\gamma-1)$. Jelöljük ezen elemek halmazát $D_{A,\ell}$-lel, továbbá $D_{A,\ell}^{(n)} = \{(\gamma,\tau)\in D_{A,\ell} | \det(\gamma)\equiv q^n \pmod\ell\}$. Ekkor

$$\left|D_{A,\ell}^{(n)}\right| = \begin{cases} \ell^3+\ell^2, & \text{ha } q^n\not\equiv 1 \pmod\ell,\\ \ell^3+\ell^2-\ell, & \text{ha } q^n\equiv 1\pmod\ell.\end{cases}$$

Az előbbihez hasonlóan $\left|D_{A,m}^{(n)}\right| = O(m^3\log\log m)$ és $|D_{A,m}^{(n)}|/|H_{A,m}^{(n)}| = O(m^{-2}\log\log m)$, ha $H_{A,m}^{(n)} = \{(\gamma,\tau)\in H_{A,m} | \det(\gamma)\equiv q^n \pmod m\}$.

A gond az, hogy itt még sokkal több tag van a szitában, mint az előbb, hiszen most m elvileg akár $q^n+2q^{n/2}+1$ is lehet. Viszont ha m nagy, akkor A_ν rendje (amit most k-val jelöljünk) kicsi, hiszen legfeljebb $|E_\nu(k_\nu)|/m$, ami nem sokszor fordulhat elő: az kell, hogy $\nu(x(k\cdot A))<0$ legyen, ez pedig egy nyilvánvaló becsléssel $O(k^2)$ esetben fordulhat elő, tehát $O(x^3)$ esetben lesz A_ν rendje legfeljebb x. Így tehát az $m \gg q^{2/3\cdot n}$ tagok elintézhetők. Sajnos egy pontra nincs jobb becslés, és a maradék tagok is túl sokan vannak, mert a Csebotarev-tételben a hiba $\Omega(q^{n/2})$ nagyságrendű, tehát így nem juthatunk eredményre.

Amit lehet csinálni, hogy A helyett több, független pontot veszünk, mondjuk r darabot, és az általuk generált Σ rácsot nézzük. Ekkor a Néron–Tate-párosítás szerint Σ-ban nem lehet túl sok kis magasságú pont és ennek következményeként

6. Állítás ([5] Lemma 14)**.**

$$\sum_{\substack{\nu\in V_{E/K}\\ |\Sigma_\nu|\le x}} \deg(\nu) = O_\Sigma\left(x^{(r+2)/r}\right).$$

Itt a jobb oldal Σ regulátorától függ.

Tehát minél nagyobb Σ rácsunk van $E(K)$-n, a képéről annál erősebbet tudunk mondani: ha r rangú, akkor az $m \gg q^{2n/(r+2)}$-nél nagyobb tagokból legfeljebb $o(q^n/n)$ van.

Legyen S azon prímek (véges) halmaza, ahol valamelyik $A\in\Sigma$ generátorra $\mathrm{Gal}(K(E[\ell],E[\ell^{-1}A])$ nem olyan, mint a fenti, általános esetben (igazából ezek közül néhányra nem is feltétlenül van szükség). És keressük azokat a $\nu \in V_{E/K}(n)$ prímeket, amikre Σ_ν már tartalmazza az $E_\nu(k_\nu)$ S-beliekhez relatív prím részét, és az ilyenek halmazát jelöljük $V_{LT}(E/K,\Sigma,n)$-nel.

Ha m-nek nincs S-beli prímosztója, akkor

$$H_{\Sigma,m} = \mathrm{Gal}(K(E[m],E[m^{-1}\Sigma]/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2r} \rtimes G_m.$$

Az előbbiekhez hasonlóan a megfelelő konjugált osztályok azok, amik minden generátor elemre megfelelők. Az értelemszerű jelöléssel $|D^{(n)}_{\Sigma,\ell}| = \ell^{r+2}+\ell^{r+1}-\ell^r$, ha $q^n\equiv 1 \pmod\ell$, és $\ell^{r+2}+\ell^{r+1}$ különben.

Ahhoz, hogy a módszerünk működjön, tovább kell finomítani a becsléseket:

- Ha m kicsi, akkor a szokásos érvelést használjuk. Mivel itt a testbővítés nem $K_m|K$ alakú, a Csebotarev-tételben sokkal rosszabb hibát kapunk, úgyhogy ez csak az $m \leq Cn$ esetre használható.
- Ha m közepes ($Cn < m < Dq^{n/5}/n$), akkor egy olyan becslést használunk, ami $r+1$ különböző teljesen szétesési feltételre bontja szét az eredeti konjugált osztályos feltételt, és erre használjuk a Csebotarev-tételt – a kis m-ekre ez elrontaná a főtagot.
- Az $Dq^{n/5}/n < m < Dq^{n/5} \cdot \log n$ eset kezelhető a prímszámtétel megfelelő alkalmazásával.

Így, ha $r \geq 10$, akkor az eddigi bizonyítási séma működik.

Az érvelést még lehet erősíteni: ehhez azt az L testet érdemes nézni, ami egy egyenes stabilizátorának felel meg G_m-ben, továbbá az $L_{\Sigma,m} = L(E[m], E[m^{-1}\Sigma])|L$ bővítést. Ez nem normális bővítés, úgyhogy ebben sokkal bonyolultabbak a prímek elágazási tulajdonságai. De ha $\nu \in V_{E/K}$ és $\Phi_{\nu,L_{\Sigma,m}/K} \in C_{\Sigma,m}$, akkor ν felett van egy megkülönböztetett $\overline{\nu} \leq L$ prím, ami segítségével hasonló módon $q^{n/4}\log n$-ig fel lehet vinni a becslést, így az $r \geq 6$ eset kezelhető. Egyelőre ez a legtöbb, amit tudunk:

7. Tétel ([8] Theorem 1)**.** *Ha E/K elliptikus görbe, $j(E) \notin k$, és $\Sigma \leq E(K)$ rács, aminek a rangja legalább 6, akkor létezik a prímszámok egy véges S halmaza, amire a $\nu \in V_{E/K}(n)$ prímek pozitív részére Σ_ν tartalmazza $E_\nu(k_\nu)$ S-beli prímekhez relatív prím részét. A fenti jelölésekkel*

$$|V_{LT}(E/K,\Sigma,n)| = \delta_{LT}(E/K,n)\frac{q^n}{n} + o\left(\frac{q^n}{n}\right),$$

ahol $\delta_{LT}(E/K,n) = \sum_{m\geq 1}\mu(m)\frac{\left|D^{(n)}_{\sigma,m}\right|}{\left|H^{(n)}_{\sigma,m}\right|}$. *És* $\inf_n\left(\delta_{LT}(E/K,\Sigma,n)\right) > 0$.

6. Egy kriptográfiai alkalmazás

Véges test feletti elliptikus görbéket használnak bizonyos nyilvános kulcsú titkosítási eljárásokban (pl. ECDH, ECIES, [1] Section 3.3 és 5.1). Ez az elliptikus görbés diszkrét logaritmus problémán alapszik: Ha $E_0/\mathbb{F}_{q^n}$ egy elliptikus görbe, akkor egy pont m-szeresét gyorsan és hatékonyan lehet számolni (még ha n és m nagyok is), viszont egy pont m-ed részét úgy tűnik, hogy

általában elég nehéz. Ez meglehetősen hasonlít a klasszikus diszkrét logaritmus problémára, amin az RSA alapszik. Az elliptikus görbés kódolások előnye az RSA-val szemben, hogy ha nyilvános kulcsú kódot csinálunk, ugyanakkora biztonsághoz elég jóval kisebb kulcsokat használni.

Röviden mutatunk egy példát egy kódolási sémára:

Ha Alíz szeretne Bobtól titkos üzeneteket kapni, meg kell adnia egy véges test feletti E_0 elliptikus görbét (vigyázni kell, mert nem minden görbe „biztonságos"), és azon egy A_0 pontot, aminek a rendje n. Alíz titkos kulcsa egy $1 \leq d \leq n$ természetes szám, a nyilvános kulcs $Q = d \cdot A_0$.

Bob üzenete egy $M \in E_0$ pont (vannak olyan algoritmusok, amelyek természes számokhoz a görbe pontjait rendelik hozzá), aminek továbbításához választ egy $1 \leq k \leq n$ véletlen számot, és az $(M_1 = M + k \cdot Q$, $M_2 = k \cdot A_0)$ pontpárt küldi tovább Alíznak.

Ekkor az $S = d \cdot M_2 = d \cdot (k \cdot A_0) = k \cdot (d \cdot A_0) = k \cdot Q$ pontot csak Alíz és Bob ismeri, ennek segítségével Alíz könnyen megfejtheti az üzenetet: $M = M_1 - S = M_1 - d \cdot M_2$.

Látható, hogy olyan A_0 pontot érdemes választani, ahol az $\langle A_0 \rangle \leq E_0$ részcsoport indexe kicsi (a gyakorlatban legfeljebb 4). Viszont ahogy láttuk, az RSA-val ellentétben, adott E_0-ra nem biztos, hogy van ilyen pont – mivel E_0 csoportja nem feltétlen ciklikus (mint a modulo p redukált maradékosztályoké). De az eddigi eredményeink alapján

8. Állítás. *Ha n elég nagy, akkor az $\mathbb{F}_q$ feletti elliptikus görbék legalább negyedének a csoportja ciklikus.*

Bizonyítás. Tekintsünk most egy olyan $K = \mathbb{F}_q(T)$ felett egy olyan E elliptikus görbét, amire $j(E) = T$. Ilyen például az

$$E/K : y^2 + xy = x^3 + \frac{36}{1728 - T}x + \frac{1}{1728 - T}$$

affin egyenlet által definiált elliptikus görbe. Ekkor az E_ν redukált görbék $\nu \in V_{E/K}(n)$-re azok a görbék, ahol T helyére $\mathbb{F}_{q^n}$ elemeit helyettesítjük be, és ahogy láttuk, ez lényegében az $\mathbb{F}_{q^n}$ feletti elliptikus görbéket (illetve azok felét) adják meg.

Tehát ha $\delta_{\text{cikl}}(E/K, n)$ pozitív, akkor az $\mathbb{F}_{q^n}$ feletti elliptikus görbék egy pozitív hányadára a görbe csoport ciklikus. Igusa tétele szerint erre görbére a geometriai bővítés mindig maximális ([9], Theorem 4), így a 2. tétel szerint

$$\delta_{\text{cikl}}(E/K, n) = \sum_{m|q^n-1} \mu(m)\frac{\text{ord}_m(q)}{|G_m|} = \sum_{m|q^n-1} \mu(m)\frac{1}{|G_m^{(\text{geom})}|}$$

$$= \prod_{\ell \mid q^n - 1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right)$$
$$\geq \prod_{\ell \neq p} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \simeq 0{,}788 \cdot \frac{p^3 - p}{p^3 - p - 1} > 0{,}5.$$

Ez elég az állításunkhoz. □

Ha a Lang–Trotter-sejtés igaz lenne, akkor arról is tudnánk valamit mondani, hogy egy adott $A \in E$ pont képe mekkora valószínűséggel lenne jó Alíz A_0 pontjának.

Hivatkozások

[1] Brown, D., *Standards for Efficient Cryptography, Elliptic Curve Cryptography*, vol. SEC 1, version 2.0. 2009.

[2] Cojocaru, A. C., Tóth Á., The distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field, *Journal of Number Theory* **132** (2012), 953–965.

[3] Cojocaru, A. C., Tóth Á., Voloch, J. F., Squarefree orders for the reductions of an elliptic curve over a function field, Preprint.

[4] Erdélyi M., The distribution and density of cyclic groups of the reductions of an elliptic curve over a function field, *J. Number Theory* **175** (2017), 87–99.

[5] Gupta, R., Murty, M. R., Cyclicity and generation of points mod p on elliptic curves, *Invent. Math.* **101** (1) (1990), 225–235.

[6] Heath-Brown, D. R., Artin's conjecture for primitive roots, *Quart. J. Math. Oxford* **37** (1987), 27–38.

[7] Hooley, C., Artin's conjecture for primitive roots, *J. Reine Angew. Math.* **225** (1967), 209–220.

[8] Hall, C., Voloch, J. F., Towards Lang–Trotter for elliptic curves over function fields (part 1), *Pure Appl. Math. Q.* **2** (1) (2006), 163–178.

[9] Igusa, J.-I., Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves, *Amer. J. Math.* **81** (1959), 453–476.

[10] Lang, S., Trotter, H., Primitive points on elliptic curves, *Bull. Amer. Math. Soc.* **83** (2) (1977), 289–292.

[11] Murty, V. K., Scherk, J., Effective versions of the Chebotarev density theorem for function fields, *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), 523–528.

[12] Pacheco, A., Distribution of the traces of Frobenius on elliptic curves over function fields, *Acta Arithmetica* **106** (3) (2003), 255–263.

[13] Weil, A., On the Riemann hypothesis in function-fields, *Proc. Nat. Acad. Sci. U.S.A.* **27** (1941), 345–347.

Rényi Alfréd Matematikai Kutatóintézet,
1053 Budapest, Reáltanoda utca 13-15. merdelyi@renyi.hu

Társulati élet – 2017

A Bolyai János Matematikai Társulat Szele Tibor-emlékérem bizottsága a 2016. évi érmet **Simon Károlynak** ítélte oda.

Indoklás:

Simon Károly a Budapesti Műszaki és Gazdaságtudományi Egyetem Matematika Intézetének egyetemi tanára, a fraktálok elméletének vezető kutatója.

Szegeden szerezte matematikusi oklevelét. Valós függvénytani kutatásait Totik Vilmos vezetésével kezdte, majd Laczkovich Miklós irányításával a folytonos függvények iterációival foglalkozott. Kandidátusi dolgozatát Major Péter – és részben M. Jakobson – vezetésével a dinamikai rendszerek és fraktálok elméletének határterületén folytatott kutatásaiból írta. 2007 óta az MTA doktora.

Legtöbbet idézett dolgozatában 1995-ben Mark Pollicottal kidolgozták a transzverzalitási módszert a fraktálok elméletében, amely azóta az elmélet egyik klasszikus eszközévé vált. Többek között ezt a módszert használta Boris Solomyak egy 60 évig nyitott Erdős-probléma, a nevezetes Bernoulli-konvolúció-sejtés megoldására. Fő érdeklődési területe a kaotikus rendszerek attraktoraiként előálló fraktálok tört dimenziójának meghatározása. Michał Ramsszal közös munkáiban a fraktálperkolációk geometriájának elméletében ért el jelentős eredményeket. Az utóbbi években bekapcsolódott a komplex hálózatok és az internet forgalmának matematikai eszközökkel történő vizsgálatába.

Jellemzően számos külföldi társszerzővel dolgozik, és – mint a fraktálok elméletének vezető kutatóját – sokat hívják meg vezető külföldi egyetemekre, kutatóintézetekbe. Munkáira, előadásaira jellemző az energikusság. A matematikai problémákat elhivatottan és gondos precizitással kezeli. Tanított gimnáziumban, a Miskolci Egyetemen. 1999 óta oktat a BME-n. 2012 óta a Sztochasztika Tanszék vezetője, 2017-től egy MTA kutatócsoportot is vezet. Több évet töltött két igen rangos külföldi egyetemen (University of Washington, University of Warwick).

Simon Károly egyetemi oktatóként is példaértékű és igen eredményes. Komoly figyelmet fordít tanítványaira, akik mind szakmailag, mind emberileg sokat kapnak tőle. Hallgatóit arra sarkallja, hogy egyszerre foglalkoz-

zanak magas színvonalú elméleti kutatásokkal és ezzel párhuzamosan alkalmazott matematikával. Szívügye, hogy diákjai – az igényes és magas színvonalú kutatómunka mellett – jól megtanuljanak tanítani is, valamint konferenciákon előadni. Ennek eredményeként tanítványai igen sikeresek, kiemelkedően rangos állásokat, posztdoktori ösztöndíjakat szereznek, mint azt az alábbi példák is mutatják.

A témavezetésével doktori fokozatot szerzett Bárány Balázs egy évig a Lengyel Tudományos Akadémia Matematikai Intézetében, majd másfél évig a dinamikai rendszerek elméletében különösen erős University of Warwickon volt vendégkutató. Posztdoktorként két évet a Banach Centerben, nyolc hónapot a Hebrew Universityn töltött. Nemzetközileg igen jól ismert, magasan jegyzett kutató. Komjáthy Júlia doktori fokozata megszerzése után az Eindhoveni Műszaki Egyetemen kapott állást. Móra Péter végzése után a Morgen Stanley Researchnél helyezkedett el. Kolossváry István, akinek doktori eljárása folyamatban van, több értékes fiatal kutatói díjat nyert. További két doktorjelölt és egy harmadéves doktoranduszhallgató munkáját irányítja.

Beke Manó-emlékdíj

A 2017. évi Beke Manó-emlékdíj Bizottság körültekintő mérlegelés után az alábbi határozatot hozta: a Beke Manó-emlékdíj első fokozatát **Katz Sándor**, a második fokozatát **Árvainé Libor Ildikó, Bere Lászlóné, Fenyvesi Mária, Jakucs Erika, Stallenberger Józsefné, Szomódi Zsuzsanna** és **Tóthné Berzsán Gabriella** kapták.

Indoklások:

Katz Sándor a szegedi József Attila Tudományegyetem matematika-fizika szakán szerzett középiskolai tanári oklevelet 1973-ban. Azóta a Bonyhádi Petőfi Sándor Evangélikus Gimnázium és Kollégium tanára. Első publikációi a függvények tanításának módszertanával foglalkoztak. Ebből a témából írta doktori disszertációját 1985-ben, és ezzel a kérdéskörrel foglalkozik a Tankönyvkiadónál 1988-ban megjelent első könyve is.

Jelentős eredményeket ért el a tehetséggondozásban, több mint 70 tanítványa lett díjazott országos és nemzetközi versenyeken. A tehetséggondozás és a matematika módszertan kérdéseiről 100-nál több előadást tartott országos szakmai rendezvényeken. Az Erdős Pál Matematikai Tehetséggon-

dozó Iskola alapító tanára, 2014-től a Pannon Egyetem címzetes egyetemi docense.

Hat szakkönyve és feladatgyűjteménye, illetve 27 szakmai cikke jelent meg. Szakirodalmi CD-t készített, amely több ezer szakkönyv és cikk adatait és 200 olvasható cikket tartalmaz. Legutóbb 2016-ban jelent meg *Játékos matematika* című könyve. Az Arany János Tehetséggondozó Program keretében a hátrányos helyzetű tanulók tehetségfejlesztéséhez tantervet és feladatgyűjteményt állított össze. Részt vett a kerettanterv kidolgozásban.

1988-tól 2012-ig Tolna megyei matematika szaktanácsadó, 1995-től 2015-ig a magyarországi evangélikus iskolák matematikai szaktanácsadója. 2000-től az Arany János Tehetséggondozó Program matematika tantárgyfelelőse.

Több mint 30 éve szervezi a megyei és regionális versenyeket, szakköröket, ill. 16 éve az AJTP matematikaversenyét. Iskolájában először a 4 évfolyamos, majd a 6 osztályos emelt szintű (heti 5 órás) helyi tantervet és ezekhez szakmai anyagokat dolgozott ki. Károlyi Károly általános iskolai szaktanácsadóval együtt a megye és a régió tanulói és tanárai számára mintaértékű tehetséggondozó rendszert alakítottak ki versenyekkel, szakmai programokkal, és ezek működtetéséhez alapítványt hoztak létre. Iskolájában is a matematikai tehetséggondozás segítésére létrehozott alapítványt vezeti. Az elmúlt tíz évben több mint 20 millió forintot sikerült különböző szponzoroktól bevonnia a helyi és regionális matematikai tehetségfejlesztés támogatásába. Meghatározó szerepe van abban, hogy a Bonyhádi Petőfi Sándor Evangélikus Gimnázium matematikából az ország egyik legeredményesebb, leginnovatívabb iskolája. 2011-ben megszervezte a XX. Nemzetközi Magyar Matematikaversenyt.

2005-től a Bolyai János Matematikai Társulat Oktatási Szakosztályának alelnöke, az elmúlt tanévben tagja volt az MTA Matematika Közoktatási Munkabizottságának. Aktívan részt vesz a matematikatanítás és tehetséggondozás eredményességének növelését célul tűző tevékenységekben. Fontosabb elismerései: Beke Manó-díj II. fokozat, Ericsson-díj, Graphisoft Díj, Rácz Tanár Úr Életműdíj.

Katz Sándor hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj I. fokozatában részesül.

Árvainé Libor Ildikó a Szegedi Tudományegyetem Juhász Gyula Gyakorló Általános Iskolája, Alapfokú Művészetoktatási Intézményének szakvezető tanítója, szakvezető tanára.

Általános iskolai tanítói diplomáját Baján, az Eötvös József Tanítóképző Főiskolán szerezte 1989-ben. Főiskolai tanulmányai során két területre fordított kiemelt figyelmet: a matematikatanításra és a gyermek- és ifjúságvédelemre. 1991 augusztusától a Juhász Gyula Tanárképző Főiskola Gyakorló Iskolájában kis felmenő rendszerben 3. és 4. osztályban tanít. Vállalta a nem szakrendszerű oktatás keretében az 5. és 6. osztályban is a matematika tanítását azért, hogy személyesen megtapasztalhassa, mi okoz nehézséget a tanulóknak az alsó és felső tagozat közötti átmenetben. 2001-től szakvezető tanítóként és tanárként dolgozik az intézményben. Hittel vallja, hogy szakvezetőként személyes példaadással lehet és kell hitelesen segíteni a hallgatók pedagógussá válását.

Kezdettől fogva nagy gondot fordít az önképzésre, folyamatosan törekszik a legújabb szakmai, módszertani ismeretek megszerzésére. 2008 és 2010 között elvégezte a Szegedi Tudományegyetem Bölcsészettudományi Karán a Pedagógiai értékelés és mérés tanára mesterszakot. Az így megszerzett ismereteit több szinten is hasznosítja, hiszen az iskolájában a diagnosztikus mérések és a kompetenciamérések eredményeinek elemzése az ő feladata, illetve a pedagógiai értékelési szakértő hallgatók is nála töltik gyakorlatukat. Az SZTE Neveléstudományi Intézet felkérésére a matematika diagnosztikus teszt online feladatait lektorálta 2011-től 2015-ig.

2001-től kezdődően a Mozaik Kiadó felkérésére környezetismeret és matematika tankönyvcsalád kidolgozásában vett részt, amelyhez módszertani segítségként kézikönyvet írt, és egy applikációs eszközöket tartalmazó doboz kidolgozásában is részt vett. Ezen feladatok kapcsán az elmúlt évtizedben nagyon sok iskolába jutott el, ahol módszertani előadások keretében adhatta át mások számára is hasznosítható saját tapasztalatait.

Az elmúlt 15 évben a fővárosban és az ország legkülönbözőbb részein számtalan előadást tartott az alsó tagozatos matematikatanítás különböző területeiről és lehetőségeiről, a változatos munkaformáktól a mozaBook használatán, a tevékenykedtetésen alapuló matematikai fogalomalkotáson át a kompetenciák fejlesztéséig.

Árvainé Libor Ildikó hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Bere Lászlóné a Ceglédi Szakképzési Centrum Közgazdasági és Informatikai Szakgimnáziumának matematikatanára, aki feladatokat vállaló, jól teljesítő és elhivatott pedagógus. Kedves, közvetlen, segítőkész személyiség, aki törődik munkatársaival és tanítványaival is. Szabadidejét is szívesen áldozza tanítványaira, egy-egy versenyre való felkészülés (szombati napon is), vagy éppen felzárkóztatás érdekében.

Tehetséges, matematika iránt érdeklődő tanulókkal szakköri és egyéni felkészítéseken foglalkozik, igen eredményesen. A Pest megyei Matematikaversenyen tanulói évek óta az első három helyezett között végeznek. 2007–2011 között a szárnyai alá vett hátrányos és halmozottan hátrányos helyzetű tanulókkal – szülői motivációk hiányának ellenére is – kitűnő eredményeket ért el. A tavalyi tanévben két tehetséges diákot kapott a tizenegyedikes emelt szintű matematikacsoportjába. Sikeres felkészítésének eredményeként mindkét fiú részt vett az OKTV döntőjében is, kiemelkedő eredménnyel. Tizenkettedikesként is ott voltak a döntőben.

Nyaranta folyamatosan részt vesz a Rátz László Vándorgyűlésen, az itt megismerteket kollégáinak továbbadja, munkájába beépíti. Folyamatos megújulásra képes, 2009–2010 óta gyarapítja iskolája kompetencia alapon oktató matematikatanárainak sorát. A mentorképzésen megszerzett ismereteit más iskolák tanárainak is át tudja adni. Munkaközössége aktív tagjaként segíti a beiskolázást a nyolcadikosok matematikai felkészítésével.

A 2015-ös kétszintű érettségi indulása óta javít és vizsgáztat emelt szinten matematikából, és mindezt vissza is forgatja az emelt szintű felkészítéseibe, igen nagy sikerrel.

2014 nyarán matematikából szaktanácsadói képzést végzett, amelyen keresztül újabb lehetőséget kapott a fiatalabb kollégák segítésére, a szakmai-módszertani tapasztalatok továbbadására.

Kiemelkedő szakmai tudását bizonyítja az is, hogy éveken át tanított matematikát a Gábor Dénes Főiskola ceglédi kihelyezett tagozatán. Életét hivatásának és iskolájának szentelő, pluszfeladatokat is szívesen vállaló, oktató és nevelő munkáját kimagasló színvonalon végző pedagógus.

Bere Lászóné hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Fenyvesi Mária 25 éve a Kastélydombi Általános Iskola matematika-kémia szakos tanára. Munkáját mindennap kihívásnak tekinti, alkotó-nevelő munkáját elhivatottsággal végzi. Elkötelezett továbbadója a természettudo-

mányos gondolkodásnak, annak az elme pallérozására gyakorolt hatását elsőrendűnek tekinti. A pedagógiai programban megfogalmazott céloknak kiválóan megfelel, innovatív, mindig előremutató indítványai vannak. A tantárgyát tekintve vallja: erős, biztos alapismeret, szorgalmas, precíz munka szükséges ahhoz, hogy a matematikai, természettudományos kompetencia kialakuljon. A tanítás tartalmában mindig ügyel arra, hogy az ismeretek készséggé válhassanak, óráira jellemző a sokoldalú, kreatív feladatokra épülő, feszes, de jó hangulatú munka. Nyitott személyiség, a gyerekek tisztelik a matematika és kémia tantárgyhoz való viszonyát.

Szakmájának magas szintű művelésével, lelkesedésével és nagy gyermekszeretetével mind a szülők, mind a kollégái körében egyaránt elismerést vívott ki. Elterjedt nézet szerint kivételesen szerencsésnek érezheti magát, akinek gyermeke Marika néni „szárnyai alá kerül" az iskola felső tagozatán. Tehetségüket kibontakoztatva hozzászoktatja őket a versenyzéshez, a precíz, kitartó munkához. Lelkesedése átragad a gyerekekre, ami nélkülözhetetlen az áldozathozatalhoz, amivel a fárasztó felkészülés jár, ami nélkül viszont nincs eredményes versenyzés. A versenyeken részt vevő gyerekek óriási előnye a tudáson túl az a versenyrutin, amire szert tesznek.

Hosszú évekre visszamenőleg – figyelembe véve tanítványai országos, megyei, területi vagy budapesti helyezéseit – nem lehet kétséges, hogy erőn felül teljesít, és rendkívüli szakértelemmel áll a versenyzői mellett, hogy a bennük rejlő tehetséget felszínre hozhassa.

10 éve már szakmai sikerei csúcsán van. A Tanárnő mindig lépést tart a szakmai újdonságokkal, rendszeresen jár mind matematikai, mind kémiai továbbképzésekre, és a hallottakat, látottakat – legyen az új tanítási módszer, feladat – igyekszik a tanításba beépíteni. Innovatív tanár, aki nemcsak új utakat keres, hanem rendkívül széles körű, óriási feladatgyűjteményt alakított, alakít ki hosszú szakmai életútja során, amely segíti a differenciált oktatásban is.

Az iskolában, szakkörön, tudományos táborban, otthonában is a matematikatanítás népszerűsítését végzi. Külön feladatok alapján tesztel kollégákat, diákokat. Kísérletező elme, jól motiválja tehetséggondozó csapatát.

Fenyvesi Mária hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Jakucs Erika pályáját képesítés nélküli nevelőként kezdte. Felsőfokú

tanulmányait munka mellett végezte, 1989-ben a Budapesti Tanítóképző Főiskolán, 1992-ben az ELTE Tanárképző Főiskolai Karán, majd 1996-ban az ELTE Természettudományi Karán kapott tanári diplomát. Hét évig dolgozott napközis nevelőként, majd ezután az ELTE Tanárképző Főiskolai Karán tanított. 2002-től a Dob utcai Kéttannyelvű Általános Iskolában és a Fazekas Mihály Fővárosi Gyakorló Általános Iskolában is óraadó volt. 2004-től a Budapesti Fazekas Mihály Gyakorló Általános Iskola tanára, 2008-tól pedig a mai napig az iskola vezetőtanára. Szakmai fejlődése érdekében jelenleg végzi az egri Eszterházy Károly Egyetem gyakorlatvezető mentortanár pedagógus szakvizsgát adó képzését.

Jakucs Erika a kísérletező, felfedeztető matematikatanítás lelkes híve. Óráin sokszor épít a tanulók önálló munkájára. Célja, hogy a gyerekek ne csak tanulják, hanem értsék és szeressék is a matematikát. A tanulók érdeklődésének felkeltése érdekében különböző változatos eszközöket, módszereket használ. Tervezett fóliasorozatot, készített szemléltető eszközöket, a tanítási folyamatba beépíti a számítógépet is. Tehetséggondozó munkája sokrétű: vezet fővárosi szakkört, tart évközi tehetséggondozó tábort, nyári matematikatábort, csoportvezető a MaMuT-ban, részt vesz a Kalmár László Matematikaverseny feladatíró teamjében. A Bolyai Csapatverseny területi fordulójának szervezője.

Jakucs Erika pedagógusi, tanári tevékenysége sokoldalú. A tanulókkal való foglalkozáson kívül fontosnak tartja a pedagógusok képzését, továbbképzését, illetve a szakma megújulását is. Rendszeresen tartott különböző iskolákban módszertani továbbképzéseket, ehhez kapcsolódva gyakran tartott bemutató órákat. A Fazekasban tartott órái közül többet videóra vett a Sulinova. Többször tartott előadást a Varga Tamás Módszertani napokon és a Tanárklubban. Jelenleg részt vesz az MTA módszertani kutatási projektjében.

Munkájának elismeréseképpen 2012-ben a Graphisoft Alapítvány *A Magyar Matematika Oktatásért Díj*-át, 2013-ban kiváló tehetséggondozó kategóriában *Bonis Bona* díjat kapott.

Jakucs Erika hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Statlenberger Józsefné, a Nagymányoki II. Rákóczi Ferenc Általános Iskola tanítónője több évtizede kiemelkedő szakmai munkát végez iskolájában és a régióban. A friss érettségivel rendelkező Katalin a nagymányoki diákotthonban kezdte meg pá1yafutását képesítés nélküli nevelőként. Je-

lentkezett a Kaposvári Tanítóképző Főiskolára, melyet a munka mellett párhuzamosan végzett el. A diákotthon megszűnésével az általános iskolában folytatja munkáját. A kezdetektől fogva matematikát oktatott alsó tagozaton. Feladatait 34 év óta elhivatottan és lelkiismeretesen végzi, abban a meggyőződésben, hogy a gyermeki logika és kreativitás fejlesztésének kulcsfontosságú területe a matematika.

Stallenberger Józsefné kezdeményezésére iskolájában bevezették az 1.–6. évfolyamokon a matematika tehetséggondozó szakkört, melynek keretén belül versenyelőkészítés folyik. Nemcsak az alsó tagozatos diákokkal, hanem az egész iskola matematikából tehetséges tanítványaival foglalkozik. Szakkörein, versenyfelkészítőin való részvétel élmény a tanulók számára.

Tehetséges diákjainak jelentős része a Bonyhádi Petőfi Sándor Evangélikus Gimnáziumban tanul tovább, ezért Stallenberger Józsefnét a gimnázium 2013-ban Lehr András-díjban részesítette.

Mivel évfolyamonként a heti egy óra szakkör kevésnek bizonyult a tényleges felkészítéshez, a kolléganő szabadideje terhére, délutánonként további alkalmakat kerített a gyerekekkel való fog1alkozásra. 2006-ban az ELTE Tanító- és Óvóképző Karán pedagógus szakvizsgával bővített tanító, fejlesztési (differenciáló) szakot végzett, majd 2007-ben a „Sindelar–Zsoldos"-programmal ismerkedett meg a hatékonyabb képességfejlesztés érdekében.

Növendékei sok szép sikerrel büszkélkedhetnek. Nem véletlen, hogy ebben a kisvárosi iskolában a tanulók több eredményt értek el, mint sok helyen egy egész megyében.

Munkáját megbízhatóság, pontosság és alaposság jellemzi. Munkatársaival szemben mindig nyitott és segítőkész. Szaktanácsadóként és szakértőként kérés nélkül is segít a kollégáknak az őket érintő pedagógusminősítések és tanfelügyeletek lehető legjobb előkészítésében.

Tevékenysége messze túlmutat iskolája keretein. Részt vesz versenyek szervezésében, szakmai előadások tartásában. Tapasztalatait, módszereit szívesen továbbadja az érdeklődő kollégáknak. Több publikációja is ezt a célt szolgálja. Igazi példamutató személyiség.

Stallenberger Józsefné hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Szomódi Zsuzsanna a Bem József Óvóképzőben szerzett kitűnő érettségi után a Tanítóképző Főiskolán folytatta tanulmányait. Nem volt kérdés számára, hogy a diploma megszerzése után 1988-tól mint tanítónő kezdje meg élete új szakaszát. Az Áldás Utcai Általános Iskolába került, ahol nagyon jó kapcsolatot alakított ki a diákjaival és a kollégákkal. Az első osztálya matematika tagozatos volt. A matematika iráni szeretete átragadt a tanítványaira is, akik szép sikereket értek el az alsós országos matematikaversenyeken. Az alsó tagozat munkaközösség-vezetője lett. Kiváló oktató és nevelőmunkájára, kiemelkedő emberi tulajdonságaira felfigyelt az ELTE Tanítóképző Matematika Tanszéke is, ahonnan számtalan tanítójelölt főiskolás járt hozzá tanulni/tanítani. Vezetőtanítói tevékenységét elismerés kísérte.

Fontosnak tartja az önképzést, továbbképzésekre jár, műhelyeket látogat.

A matematikát úgy tanítja, hogy feltétlen megszerettesse a gyerekekkel. Szeretné, hogy a diákok azt „higgyék”, hogy ez egy jó játék. Sokat játszanak, tevékenykednek, felfedeznek az órákon, rengeteg vizuális élmény éri őket. Közös munkájukra jellemző Varga Tamás filozófiája: cselekvésből, tevékenységből kiinduló gondolkodásra nevelés.

2.–4. osztályban már verseny-előkészítő foglalkozásokat is tart az érdeklődőknek, ahol nagyon sok érdekes, gondolkodtató feladatot oldanak meg. Szomódi Zsuzsanna határozottan élvezi, ahogy a kis okos diákok eljutnak sajátos gondolkodásukkal a felismerésig, a megoldás élményéig. Több versenyen értek el már kerületi, területi, budapesti és országos sikereket is.

Külön dicséretes, hogy osztályaival színházba jár, sportol a gyerekekkel együtt, többnapos tavaszi, nyári osztálykirándulásokat szervez, melyek előkészítése és kivitelezése mintaszerűen gyerekbarát.

A Tanítónő nemcsak a tehetséggondozás, hanem a felzárkóztatás területén is kimagasló munkát végez. Sok szülő keresi meg iskoláját azzal a szándékkal, hogy gyermeke Szomódi Zsuzsanna tanítónő osztályába kerüljön.

Így vallott a munkájáról egy alkalommal: *„Azért szép ez a hivatás, mert nincs két egyforma nap, hét, év. Nem lehet ugyanazt, ugyanúgy tanítani, hiszen minden gyerekcsoport más és más. De lehet mindennap lelkesíteni a kicsiket, s megszerettetni velük valamit.”*

Szomódi Zsuzsanna hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Tóthné Berzsán Gabriella jelenlegi munkahelyén, a Kaposvári Táncsics Mihály Gimnázium speciális matematika tagozatán érettségizett, majd tanulmányait a budapesti Eötvös Lóránd Tudományegyetem matematika-fizika szakán folytatta.

1996-tól 2007-ig a Rippl-Rónai József Közlekedési Szakközépiskola tanáraként dolgozott, majd 2007-től a Kaposvári Táncsics Mihály gimnázium tanára lett, ahol 2013-tól igazgatóhelyettesként dolgozik.

Munkáját kezdettől fogva lelkiismeretesen végezte, szakmai felkészültségét az igényesség jellemzi. Részt vett a „Felkészítés 11.–12. évfolyamok iskolai (helyi) matematikai tehetséggondozására" tanfolyamon, rendszeresen hospitált az Erdős Pál Matematikai Tehetséggondozó Iskola foglalkozásain, s élénk szakmai közéletet élve önmaga is képezte saját magát.

2006-tól tagként, elnökként lát el feladatokat az emelt szintű érettségin. Bekapcsolódott a ZALAMAT Alapítvány által szervezett nyári matematikai táborok munkájába is, s előadott Révkomáromban a Nagy Károly Matematikai Diáktalálkozón is. Gyakori résztvevője a Rátz László Vándorgyűlésnek.

2015-től pedagógusminősítési és tanfelügyeleti szakértő.

Szívesen segít kollégáinak mindenben, szakmai felkészültségének köszönhetően ezt egyre többen és egyre gyakrabban igénybe is veszik.

Az iskolában folyó Arany János Tehetséggondozó Program programfelelőseként fokozott szociális érzékenységet tanúsítva egyengette tanítványai matematikai előremenetelét, de ugyanilyen igényességgel tanít az emelt szintű matematikai csoportokban is. Tág teret biztosít a diákok versenyeztetésének. Munkájának sikerességét jól bizonyítják tanítványai országos és nemzetközi versenyeredményei.

Munkája elismeréseként 2014-ben Graphisoft-Díjat, ugyanezen esztendőben Polgármesteri Dicséretet, 2016-ban Miniszteri Dicséretet kapott.

Nemcsak a kollégái előtt van nyitva mindig irodájának ajtaja, de tanítványai is gyakran fordulnak meg ott. Aktívan dolgozik a Táncsics Mihály Gimnázium Matematikai Tehetségeiért Alapítvány kurátoraként is.

Tóthné Berzsán Gabriella hosszabb időn át végzett kiváló és eredményes matematikai nevelő-oktató munkájáért a Beke Manó-emlékdíj II. fokozatában részesül.

Grünwald Géza-emlékérem

2017-ben a Grünwald Géza-emlékéremre hét felterjesztés érkezett, melyek kivétel nélkül magas színvonalat képviseltek. A Bizottság öt díj odaítéléséről döntött. A díjazottak tudományos munkássága hűen tükrözi a matematika sokszínűségét. Külön örömünkre szolgál, hogy lehetőségünkben állt különböző egyetemek, illetve kutatóintézetek munkatársait kitüntetni. A Bizottság szavazatai alapján az idei díjazottak a következők: **Bertók Csanád, Kiss Viktor, Nagy Dániel, Soukup Dániel** és **Szikszai Márton**.

Indoklások:

Bertók Csanád 1988-ban született. Biológus tanulmányai után 2012-ben szerzett matematika B.Sc. diplomát, majd 2014-ben matematikus mesteri fokozatot a Debreceni Tudományegyetemen, ahol jelenleg matematikus doktoranduszhallgató.

Bertók Csanád eddig nyolc matematikai témájú dolgozatot publikált. Kutatásai a számelmélet területére összpontosulnak. Fontos eredményeket ért el az exponenciális diofantikus egyenletek szerteágazó területén. Ilyen típusú egyenletek állnak fontos számelméleti problémák hátterében. Effektív eredmények azonban csupán a kéttagú egyenletekre ismertek; három vagy több tagszám esetén csupán a megoldások száma korlátozható. Bertók Csanád – társszerzőkkel – egy olyan újszerű eljárást dolgozott ki, amely az általános esetben is jól alkalmazható konkrét exponenciális egyenletek összes megoldásának meghatározására. Ezt a módszert kiterjesztette a sokkal általánosabb algebrai esetre is. Érdekes és fontos eredményeket ért el az algebrai számok többdimenziós diofantikus approximációjával kapcsolatban is, lényegében a lánctört-algoritmus kiterjesztését adta algebrai számtestekre. Legfrissebb munkájában pedig korlátos együtthatójú polinomok eloszlásával kapcsolatban bizonyított fontos elméleti és numerikus eredményeket. Munkáiban alapos elméleti háttértudása mellett kiváló algoritmikus érzékét is sikerrel alkalmazza.

Kiemelkedő eredményeire tekintettel Bertók Csanád a Grünwald Géza-emlékéremben részesül.

Kiss Viktor 1990-ben született. 2011-ben diplomázott az ELTE Matematika B.Sc. szakán, majd 2013-ban szerzett ugyanitt M.Sc. fokozatot. Az ELTE Doktori Iskolájában 2017-ben védte meg doktori disszertációját,

témavezetője Elekes Márton volt. Jelenleg az MTA Rényi Alfréd Matematikai Kutatóintézet fiatal kutatója, illetve posztdoktori állást kapott a Cornell Universityn. 2016-ban az MTA Turán Pál-díjának kitüntetettje.

Kiss Viktornak öt dolgozata jelent meg rangos nemzetközi folyóiratokban, és további négy munkája van előkészületben. Érdeklődése széles körű, de alapvetően a valós analízis különféle ágaival foglalkozik. Remek problémamegoldó, amit IMO és IMC eredményei mellett az is mutat, hogy fő témájától különböző területeken is számos problémát megoldott, amiből egy geometriai mértékelméleti és három kombinatorikai témájú cikke is született. Legjelentősebb eredményeit a leíró halmazelmélet területén érte el. Társszerzőivel sikerült általánosítania a rangfüggvények elméletét a Baire 1 esetről a Baire ξ esetre. Ennek alkalmazásaként megválaszolt egy függvényegyenlet-rendszerek megoldhatóságáról szóló kérdést is, melyet a paradox geometriai átdarabolások motiváltak. Két további halmazelméleti témájú, társszerzős cikkében pedig a modern leíró halmazelméletben centrális kérdéskörrel, lengyel csoportokkal foglalkozott. Különféle automorfizmus- és homeomorfizmus-csoportokban vizsgálta meg a konjugált osztályok nullmértékűségét, és a problémát számos nyitott esetben teljesen megoldotta.

Kiemelkedő eredményeire tekintettel Kiss Viktor a Grünwald Géza-emlékéremben részesül.

Nagy Dániel 1990-ben született. 2012-ben diplomázott az ELTE-n matematika B.Sc. szakon, majd 2014-ben szerzett matematikus mesteri fokozatot ugyanitt. Jelenleg az ELTE Doktori Iskolájának hallgatója Katona Gyula témavezetésével, illetve az MTA Rényi Alfréd Matematikai Kutatóintézetben fiatal kutató. 2014-ben Rényi Kató-díjat kapott.

Nagy Dánielnek négy megjelent publikációja van, és további három dolgozata van előkészületben. Főleg az extremális halmazelmélet területén dolgozik. Több eredménye kapcsolódik a kizárt részben rendezett halmazok, azaz posetek kérdésköréhez. Társszerzőivel együtt meghatározta, hogy aszimptotikusan maximum hány példányát lehet elhelyezni egy adott kis posetnek a Boole-hálóban úgy, hogy két elemnek megfelelő halmazok akkor és csak akkor állnak tartalmazási relációban, ha a posetben összehasonlíthatóak. Új kutatási irányt indított el: felső becslést adni egy halmazrendszer méretére egy kizárt poset valamilyen paramétereinek függvényében. Több eredményt bizonyított olyan kizárt posetekre, amelyekre bizonyos számosságmegkötési feltételek teljesülnek. Különböző dimen-

ziófogalmakkal jellemzett olyan síkbeli alakzatokat, melyek tartalmaznak egy négyzetvonalat az egységnégyzet minden pontja mint középpont körül. Legkomolyabb munkájában pedig jelentős korábbi eredményeket felülmúlva aszimptotikusan meghatározta, hogy adott pont- és élszámú gráfban maximálisan hány 4 élű út lehet.

Kiemelkedő eredményeire tekintettel Nagy Dániel a Grünwald Géza-emlékéremben részesül.

Soukup Dániel 1987-ben született. 2009-ben B.Sc., majd 2011-ben matematikus M.Sc. fokozatot szerzett az ELTE-n. Doktori tanulmányait a University of Toronton végezte William Weiss témavezetése mellett, disszertációját 2015-ben védte meg. 2015-ben az MTA Rényi Alfréd Matematikai Kutatóintézet, 2016-ban a University of Calgary posztdoktor kutatója, jelenleg pedig az Univesität Wien alá tartozó Kurt Gödel Research Center for Mathematical Logic posztdoktor munkatársa. 2011-ben Rényi Kató-díjat kapott.

Soukup Dánielnek tíz megjelent, egy elfogadott és hat benyújtott cikke van. Főbb eredményeit a halmazelméleti topológia és a végtelen kombinatorika területén érte el. Első cikkeiben D-terekkel kapcsolatos problémákkal foglalkozott. Megmutatta, hogy a reguláris aD-terek nem feltétlenül D-terek. A D-terek elméletének fő kérdése, hogy minden reguláris Lindelöf-tér D-tér-e? A legerősebb eredményt Soukup Dániel érte el társszerzőjével: konstruáltak olyan öröklődően Lindelöf Hausdorff-teret, amely nem D-tér, valamint megmutatták annak konzisztenciáját, hogy két D-tér uniója nem feltétlenül D-tér. A végtelen kombinatorika területén is számos szép eredménye van. Megmutatta, hogy akárhogyan is színezzük egy tetszőleges végtelen teljes gráf éleit véges sok színnel, a gráf pontjait véges sok monokromatikus útra lehet particionálni, méghozzá minden színt legfeljebb egyszer használva. Megoldotta Erdős és Hajnal egy régi sejtését: belátta, hogy létezik olyan nem megszámlálható kromatikus számú gráf, amelyben nincs nem megszámlálható, végtelenszer összefüggő részgráf. Több tételt bizonyított nem megszámlálható dikromatikus számú irányított gráfokról, illetve nem megszámlálható kromatikus számú gráfok irányításairól. Egyik legújabb eredményében pedig társszerzőjével bebizonyították, hogy bizonyos halmazelméleti feltevések mellett akárhogyan is színezzük a valós számokat véges sok színnel, mindig van olyan végtelen X halmaz, hogy az $X + X$ halmaz monokromatikus.

Kiemelkedő eredményeire tekintettel Soukup Dániel a Grünwald Géza-emlékéremben részesül.

Szikszai Márton 1989-ben született. Tanulmányait a Debreceni Egyetemen folytatta: 2011-ben Matematika B.Sc., majd 2013-ban Alkalmazott Matematika M.Sc. fokozatot szerzett. 2013 óta a Debreceni Egyetem doktorandusza, 2016-tól egyetemi tanársegéd ugyanitt. Rényi Kató-díjas.

Szikszai Mártonnak kilenc megjelent publikációja van. Főként a diofantoszi egyenletek területén ért el jelentős eredményeket. Társszerzőivel igazolta, hogy végtelen sok racionális diofantikus hatos létezik, azaz nem nulla racionális számok olyan hatelemű részhalmaza, amelyben bármely két különböző elem szorzatát eggyel megnövelve racionális négyzetszám adódik. Eredményük fontosságát mutatja, hogy korábban kizárólag sporadikus példákat mutattak diofantikus hatosokra. Konstruktív bizonyításuk módszert ad végtelen sok olyan racionális diofantikus hármas explicit konstrukciójára, melyek végtelen módon egészíthetők ki racionális hatossá. További munkáiban igazolta, hogy néhány explicit módon megadható sorozattól eltekintve egy nem degenerált elsőfajú Lucas-sorozatban kizárólag véges sok háromtagú számtani sorozat található, és ezek számossága effektív módon korlátozható a sorozat függvényében. Társszerzőjével együtt megmutatta, hogy tetszőleges harmadfokú sorozathoz létezik olyan G szám, amelyre bármely $k > G$ esetén a sorozatnak van k egymást követő tagja, melyek közül egyik sem relatív prím az összes többihez. Fontos eredményeket ért el rekurzív sorozatokra vonatkozó diofantikus problémák vizsgálatában, valamint a sztochasztikus analízis terén is.

Kiemelkedő eredményeire tekintettel Szikszai Márton a Grünwald Géza-emlékéremben részesül.

Farkas Gyula-emlékdíj

A Bizottság a beérkezett javaslatok alapján 2017-ben négy Farkas Gyula-emlékdíjat adományozott. A díjazottak: **Görbe Tamás Ferenc, Kerepesi Csaba, Kovács Balázs** és **Kyeongah Nah**.

Indoklások:

Görbe Tamás Ferenc doktori tanulmányait a Szegedi Tudományegyetem Fizika Doktori Iskolájában végezte. Integrálható rendszerek témában írt dok-

tori értekezését 2017 májusában védte meg. Tudományos eredményeiről számos hazai és külföldi konferencián számolt be, előadásokat tartott Angliában, Ausztriában, Csehországban, Hollandiában, Lengyelországban és Svájcban.

2013-ban elnyerte az Eötvös Loránd Ösztöndíjat. A XXXI. Országos Tudományos Diákköri Konferencián kiemelt különdíjas lett, 2016 óta Junior Templeton Fellow. 2017 áprilisában a La Femme magazin beválasztotta az 50 tehetséges magyar fiatal programba.

Görbe Tamás Ferenc 10 referált, matematikai, illetve fizikai folyóiratban megjelent cikket publikált. Munkái a teljesen integrálható hamiltoni rendszerek egy speciális osztályával, egyenesen, ill. körön mozgó, kölcsönható tömegpontokat modellező rendszerekkel foglakoznak. Az alkalmazott matematika és a matematikai fizika határterületére eső kutatásaiban szimplektikus geometriai és Lie-csoportokon alapuló technikákat kombinál egyszerűbb analitikus eszközökkel.

Egy Pusztai Béla Gáborral közös dolgozatában az ún. hiperbolikus van Diejen-rendszerek területén értek el egy áttörést jelentő eredményt. Kiemelendő egy, a témavezetőjével, Fehér Lászlóval közös dolgozata is, amelyben az ún. Ruijsenaars–Schneider-rendszer fázisterének új kompaktifikálását adják meg. Végül említésre méltó egy, az ún. Calogero–Moser-rendszerrel kapcsolatos, 2009-ben nyilvánosságot kapott nevezetes sejtés igazolása is.

A fenti érdemei alapján a Görbe Tamás Ferenc Farkas Gyula-emlékdíjban részesül.

Kerepesi Csaba 1983-ban született Kecskeméten, 2008-ban végzett matematikus szakon a Szegedi Tudományegyetemen. 2012-től az ELTE PIT Bioinformatikai Csoportjában dolgozott, majd 2016-ban az MTA SZTAKI Informatikai Kutatólaboratóriumába nyert felvételt.

Első kutatási területe a metagenomika, amelynek célja a természetes környezetből vett mintákban található örökítő anyag vizsgálata és a mikroorganizmusok eddig ismeretlen világának feltárása.

Ebben a témakörben kiemelkedő az AMPHORA metagenomikai analizáló szoftver webszerverként történő implementálása, valamint a nehezen értelmezhető eredmények egyszerű szemléltetésének és vizuális analízisének megoldása. Nevéhez fűződik a *Giant Virus Finder* nevű nyílt elérésű program megalkotása, amelynek alkalmazásával elsőként igazolta óriásvírusok jelenlétét sivatagi mintákban.

Másik jelentős kutatási területe az emberi agygráf vizsgálata, amelynek célja az agyi kapcsolatok szerkezetének és kifejlődésének a vizsgálata. Az amerikai Human Connectome Project diffúziós MRI adataira támaszkodva meghatározó szerepe volt a Budapest Referencia Konnektóm szerver létrehozásában. Erre az eszközre támaszkodva érte el eddigi talán legjelentősebb eredményét, a Konszenzus Konnektóm Dinamika felfedezését, amely a feltevéseink szerint az agyi kapcsolatok kifejlődését vizualizálja. Ez az eredmény alkalmasnak tűnik az agyi kapcsolatok irányának a meghatározására is.

Eredményes publikációs tevékenységét 11 impakt faktoros folyóiratcikk jelzi, ebből 8 dolgozatban ő az első szerző. Kumulatív impakt faktora: 27.

A fenti érdemei alapján Kerepesi Csaba Farkas Gyula-emlékdíjban részesül.

Kovács Balázs 2011-ben szerzett kitüntetéses diplomát az Eötvös Loránd Tudományegyetem Alkalmazott Matematika szakán. Ezt követően doktori hallgatóként folytatta tanulmányait az Eötvös Loránd Tudományegyetem Matematika Doktori Iskolájában. Doktori értekezését 2016-ban summa cum laude minősítéssel védte meg.

Doktori tanulmányai során öt hónapos Erasmus mobilitási ösztöndíjjal, majd tíz hónapos német akadémiai csereprogram keretében kapott DAAD kutatói ösztöndíjjal a Tübingeni Egyetemen folyó alkalmazott matematikai kutatásokban vett részt. 2016 óta pedig ugyanott posztdoktori kutatóként egy, a német kutatási alap (DFG) által támogatott, hullámjelenségeket vizsgáló matematikai kutatócsoport tagja.

Kutatásai keretében elsősorban mozgó felületeken adott parciális differenciálegyenletek numerikus megoldási módszereivel foglalkozik. Legfontosabb eredményeit a magasabb rendű idődiszkretizációk és a teljes, idő-, ill. térbeli diszkretizációk konvergenciasebességével kapcsolatos munkássága során érte el.

Az elmúlt 5 évben 14 tudományos dolgozata jelent meg a szakterület élvonalbeli, döntően Q1-es folyóirataiban. Az elmúlt két évben 4 alkalommal tartott meghívott előadást neves konferenciákon.

A fenti érdemei alapján Kovács Balázs Farkas Gyula-emlékdíjban részesül.

Kyeongah Nah matematikus diplomáját Dél-Koreában, a Kyungpook National Universityn szerezte, ezt követően 2011 augusztusától 2015 szeptemberéig Szegeden a Bolyai Intézet doktorandusza volt Röst Gergely témavezetése mellett. Doktori értékezését 2015-ben védte meg.

Kyeongah Nah első kutatási területe a malária terjedésével volt kapcsolatos, ami Koreában egy újra visszatérő népegészségügyi probléma. Tagja volt annak a csapatnak, akik meghatározták az inkubációs periódus empirikus eloszlását. Doktori disszertációjának fő motívuma ennek az eloszlásnak a beépítése dinamikus modellekbe, amelyeket funkcionál-differenciálegyenletek rendszerei határoznak meg.

Két alkalommal elnyerte az IIASA (International Institute for Applied Systems Analysis) fiatal kutatói ösztöndíját. 2015-ben Japánban kapott kétéves posztdoktori ösztöndíjat Hiroshi Nishiura csoportjában a Hokkaido Egyetemen, majd a torontói York University, Centre for Disease Modelling kutatója lett Jianhong Wu csoportjában, ahol jelenleg is dolgozik. Több első szerzős publikációja van rangos élettudományi folyóiratban az AIDS, a MERS és a Zika járványok modellezéséről. 10 tudományos publikációjára mintegy 100 független hivatkozást kapott.

Kyeongah Nah aktív résztvevője volt a szegedi matematikai életnek, könyvismertetőt írt a szegedi Actába, népszerűsítő előadást tartott a szegedi Science Cafében, és előadást tartott középiskolás diákok számára is. Sokat tett a magyar-koreai tudományos kapcsolatok fejlesztéséért, jelenleg pedig egy kanadai-kínai-magyar közös kutatási projektet koordinál a kullancsencephalitis modellezésére. Munkásságának sajátos magyar vonatkozása, hogy a Ph.D. fokozathoz előírt második idegen nyelv ismerete az ő esetében a magyar volt, amiből szakmai vizsgát tett.

A fenti érdemei alapján Kyeongah Nah Farkas Gyula-emlékdíjban részesül.

Rényi Kató-emlékdíj

A Rényi Kató-emlékdíj I. fokozatát kapta **Maga Balázs**, az ELTE matematikus M.Sc. szakos hallgatója, II. fokozatát kapta **Konkoly Ágnes**, a Debreceni Egyetem alkalmazott matematikus M.Sc. szakos hallgatója.

Maga Balázs [1] dolgozatában azt vizsgálja, hogy a sík egy részhalmaza mikor áll elő alkalmasan választott Baire-1 vagy Baire-2 függvény grafikonja

torlódási pontjainak halmazaként. A [2] cikk ezt az eredményt általánosítja egyrészt magasabb Baire-osztályokra, másrészt a valósoknál bonyolultabb értelmezési tartománnyal, illetve értékkészlettel rendelkező függvények esetére. Bátyjával írt, közlésre benyújtott [3] cikke véletlen együtthatós hatványsorok konvergenciaintervallum határán vett viselkedésével foglalkozik.

Maga Balázs publikációi

[1] B. Maga: Accumulation points of graphs of Baire-1 and Baire-2 functions, *Real Analysis Exchange* **41** (2) (2016), 315–330.

[2] B. Maga: Characterizations and properties of graphs of Baire functions, *Mathematica Slovaca*, megjelenés alatt.

[3] B. Maga, P. Maga: Random power series near the endpoints of the convergence intervals, kézirat.

Konkoly Ágnes [1] dolgozatában a szerzők olyan egyváltozós, lineáris függvényegyenletet vizsgálnak, amely helyettesítések véges csoportját tartalmazza. Klasszikus és lineáris algebrai módszerekkel teljesen leírják a megoldásokat. A [2] cikkben a szerzők a Radon-, Helly- és Carathéodory-tétel síkbeli változatait, illetve konvex függvényekre vonatkozó tételeket terjesztenek ki az úgynevezett Beckenbach-családokra.

Konkoly Ágnes publikációi

[1] M. Bessenyei, Á. Konkoly, G. Szabó: Linear functional equations and finite groups of substitutions, *Acta Sci. Math. (Szeged)* **83** (2017), 71–81.

[2] M. Bessenyei, Á. Konkoly, B. Popovics: Convexity with respect to Beckenbach families, *Journal of Convex Analysis* **24** (2017), 75–92.

A Patai László Alapítvány díja

A Bolyai János Matematikai Társulat elnöksége által kiküldött bizottság a Patai Alapítvány 2017. évi díját Csányi Petrának és Varga Adriennek ítélte oda.

Csányi Petra 2017-ben végzett az ELTE matematika-informatika szakán. Harmadéves korában a szakdolgozata témája kapcsán elkezdett kutatásokat

folytatni Szabó Csaba és Vásárhelyi Éva témavezetésével. A 2015-ös és a 2017-es OTDK-n is társszerzőivel 2-2 TDK dolgozattal indult a Tanulás- és Tanításmódszertani – Tudástechnológiai szekcióban. Összesen egy országos 1. helyezést és két országos 2. helyezést ért el. A kari konferenciákon rendszeresen első és második díjat kapott. Ez a teljesítmény példátlan a szekció történetében. Eredményeiről rendszeresen beszámolt hazai és nemzetközi szakmódszertani konferenciákon magyar és angol nyelven is. Kétszer vett részt a MIDK konferenciasorozaton, amelyik a tudományterület legrangosabb Kárpát-medencei tudományos eseménye. Előadását elfogadták az igen rangos 2016-os PME (Psychology of Mathematical Education) konferenciára. Munkái társszerzőivel két nemzetközi idegen nyelvű referált dolgozatban is megjelentek. Az INFOÉRA konferencián informatikai tárgyú előadással szerepelt.

Oktatási és társadalmi tevékenysége sem elhanyagolható. Gyakorlatokat tartott a TTK-n és az IK-n is, valamint fél évig ő tartotta a Pázmány Péter Katolikus Egyetem BTK tanítóképzésén a matematika szakmódszertan tárgyat. Tanítási gyakorlata alatt robotika szakkört szervezett iskolájában. 2016 nyarán részt vett az ELTE oktatóinak informatikai képzésében, 2017 nyarán pedig informatikatábort szervezett középiskolásoknak. Jelenleg a Szent László Gimnáziumban tanár.

Mindezek alapján Csányi Petra a Patai-alapítvány díjában részesül.

Varga Adrienn 2005-ben matematikaszakos tanári diplomát, 2012-ben pedig doktori fokozatot a szerzett a Debreceni Egyetemen.

Varga Adriennek 13 cikke jelent meg matematikai folyóiratokban elsősorban függvényegyenletek témakörében. Tudományos munkásságának másik meghatározó területe a matematikai didaktika. Aktivitását számos konferencia-részvétel, előadás és az ezekhez kapcsolódó oktatási segédanyagok, tudomány-népszerűsítő előadások jelzik. Ezek többsége a mérnökképzés során felmerülő módszertani kérdések köré szerveződik.

Részt vett elektronikus tananyagfejlesztésben, ahol is elsősorban szabad felhasználású szoftverek alkalmazását mutatta be a mérnökképzésben és a mérnöki munkában.

Tudomány-népszerűsítő előadásokat tartott középiskolások számára. Oktatóként részt vett az Debreceni Egyetemen folyó angol nyelvű képzésben.

Mindezek alapján Varga Adrienn a Patai-alapítvány díjában részesül.

Jelentés a 2017. évi Schweitzer Miklós Matematikai Emlékversenyről

A Bolyai János Matematikai Társulat 2017. október 20. és október 30. között rendezte meg a 2017. évi Schweitzer Miklós Matematikai Emlékversenyt. A versenyen középiskolai tanulók, egyetemi és főiskolai hallgatók, valamint 2017-ben egyetemet vagy főiskolát végzettek vehettek részt.

A Bolyai János Matematikai Társulat a verseny megrendezésére a következő bizottságot kérte fel: Páles Zsolt (elnök), Nagy Ábris és Varga Nóra (titkárok), Baran Sándor, Bérczes Attila, Bessenyei Mihály, Boros Zoltán, Daróczy Zoltán, Fazekas István, Figula Ágota, Gaál István, Gát György, Gselmann Eszter, Győry Kálmán, Hajdu Lajos, Kozma László, Losonczi László, Lovas Rezső, Maksa Gyula, Muzsnay Zoltán, Nagy Gergő, Pethő Attila, Pink István, Pongrácz András, Pintér Ákos, Sztrik János, Tamássy Lajos, Tengely Szabolcs, Terdik György, Tran Quoc Binh és Vincze Csaba.

A versenybizottság 10 feladatot tűzött ki. A feladatokat sorrendben Pach János, Tardos Gábor és Andrej Kupavszkij; Pongrácz András; Tengely Szabolcs és Pongrácz András; Győry Kálmán és Hajdu Lajos; Totik Vilmos; Páles Zsolt; Csirmaz László; Gát György; Totik Vilmos valamint Pap Gyula bocsátotta a bizottság rendelkezésére.

A versenyre 12 versenyző 67 megoldást nyújtott be, amelyek közül 34 volt hibátlan. Az alábbi táblázatban pontok jelzik, hogy a versenyzők mely feladatokra nyújtottak be megoldásokat.

	1	2	3	4	5	6	7	8	9	10
Ágoston Péter			•			•	•	•	•	
Ágoston Tamás	•	•	•	•	•	•	•	•	•	•
Csépai András	•						•			
Csernák Tamás	•	•					•	•	•	•
Fehér Zsombor	•	•	•		•		•	•	•	•
Forman Balázs Attila	•									
Grünwald Richárd						•				
Hevesi Bence					•					
Kúsz Ágnes Tímea	•	•	•	•	•	•		•	•	•
Maga Balázs	•	•	•	•	•	•	•	•	•	•
Markó Ádám					•	•	•	•	•	•
Szőke Tamás		•	•	•	•		•	•	•	•

A megoldások értékelése után a versenybizottság a következő döntést hozta:

*I. díj*ban részesül **Maga Balázs**, az ELTE-TTK elsőéves matematikus M.Sc. hallgatója.

*II. díj*ban részesül **Ágoston Tamás**, az ELTE-TTK elsőéves Ph.D. hallgatója.

*III. díj*ban részesül **Csernák Tamás**, az ELTE-TTK elsőéves matematikus M.Sc. hallgatója; **Fehér Zsombor**, az ELTE-TTK harmadéves matematikus B.Sc. hallgatója és **Szőke Tamás**, az ELTE-TTK harmadéves matematikus B.Sc. hallgatója

*Dicséret*ben részesül **Kúsz Ágnes Tímea**, a University of Bonn elsőéves matematikus M.Sc. hallgatója.

Indoklás

Maga Balázs 10 feladatra nyújtott be megoldást; a 2. feladatra adott megoldása kiemelkedő, az 1., 3., 6., 7., 8., 9. és 10. feladatokra adott megoldása hibátlan és teljes; a 4. és 5. feladatokra adott megoldása hiányos, de javítható.

Ágoston Tamás 10 feladatra nyújtott be megoldást; a 2. és 5. feladatokra adott megoldása kiemelkedő, a 3., 8., 9. és 10. feladatokra adott megoldása hibátlan és teljes; a 4. és 7. feladatokra benyújtott megoldása lényegében helyes, az 1. és 6. feladatok esetében részeredményeket ért el.

Csernák Tamás 6 feladatra nyújtott be megoldást; a 8. feladatra adott megoldása kiemelkedő, a 2., 7., 9. és 10. feladatokra érkezett megoldása hibátlan és teljes, az 1. feladatra adott megoldás lényegében helyes.

Fehér Zsombor 8 feladatra nyújtott be megoldást; az 1. feladatra adott megoldása kiemelkedő, a 3., 5., 8., 9. és 10. feladatokra adott megoldása hibátlan és teljes, a 7. feladatra adott megoldása lényegében helyes, és a 2. feladatban részeredményeket ért el.

Szőke Tamás 8 feladatra nyújtott be megoldást; a 3., 5., 7. és 9. feladatokra adott megoldása hibátlan és teljes, a 4., 8. és 10. feladatok megoldása lényegében helyes, a 2. feladatra adott megoldása erősen hiányos, de javítható.

Kúsz Ágnes Tímea 9 feladatra nyújtott be megoldást; a 3., 8. és 9. feladatokra érkezett megoldás hibátlan és teljes, az 1. feladatra adott megoldása

lényegében helyes, a 2. feladatra adott megoldása erősen hiányos, de javítható, és részmegoldásokat ért el a 4. és 6. feladatokban.

A feladatok és megoldásaik

1. feladat (Pach János, Tardos Gábor és Andrej Kupavszkij). Fel lehet-e bontani egy négyzetet véges sok háromszögre úgy, hogy semelyik kettőnek ne legyen közös oldala? (A háromszögeknek nincs közös belső pontjuk, és uniójuk a négyzet.)

Megoldás (Fehér Zsombor). Tegyük fel, hogy van ilyen háromszögelés. Vegyük a felbontáshoz tartozó síkgráfot, azaz melynek csúcsai a háromszögek csúcsai, élei pedig a háromszögek oldalainak azon darabjai, melyek közvetlenül szomszédos csúcsokat kötnek össze. Legyen a háromszögek száma l, a gráf csúcsainak és éleinek száma c és e. Ekkor Euler tétele szerint

$$c - e + l = 1.$$

Számoljuk most össze a szögeket: az l darab háromszög belső szögeinek összege $l\pi$. Másrészt, minden csúcsnál legalább π ezen szögek összege, és a négyzet 4 csúcsánál csak $\pi/2$, ezért

$$\begin{aligned} l\pi &\geq (c-4)\cdot\pi + 4\cdot\frac{\pi}{2}, \\ l + 2 &\geq c. \end{aligned}$$

Számoljuk össze az oldalakat, ehhez írjunk a gráf éleire számokat a következőképpen: ha egy háromszögoldal a gráfban n részre van osztva, akkor mindegyik darabra írjunk $1/n$-et, és ezt tegyük meg mindegyik háromszögre. Ekkor összesen $3l$-et írtunk az élekre. Másrészt, mivel a háromszögeknek nincsen közös oldaluk, egyik élre sem írhattunk összesen 2-t. Így mindegyik élen a ráírt számok összege legfeljebb $3/2$, és a négyzet oldalain legalább 4 élre csak 1-et írtunk, így

$$\begin{aligned} 3l &\leq (e-4)\cdot\frac{3}{2} + 4, \\ 2l + \frac{4}{3} &\leq e. \end{aligned}$$

Mindezeket összevetve:

$$2l + \frac{7}{3} \leq 1 + e = c + l \leq 2l + 2,$$

ami ellentmondás.

2. feladat (Pongrácz András). Bizonyítsuk be, hogy egy K test pontosan akkor rendezhető, ha minden $A \in M_n(K)$ szimmetrikus mátrix diagonalizálható K algebrai lezártja felett. (Azaz minden $n \in \mathbb{N}$-re és $A \in M_n(K)$ szimmetrikus mátrixra létezik olyan $S \in GL_n(\overline{K})$, amire $S^{-1}AS$ diagonális.)

Első megoldás (Ágoston Tamás). Először is belátjuk, hogy egy ilyen K test esetén K rendezhető. Jól ismert tény, hogy egy test pontosan akkor nem rendezhető, ha a 0 előáll mint nem 0 négyzetek összege, azaz valamilyen $n > 0$ egészre

$$0 = a_1^2 + \cdots + a_n^2,$$

ahol $a_1, \ldots, a_n \neq 0$ a K-ban vannak. (Speciálisan ha $\mathrm{char}\, K = p > 0$, akkor $n = p, a_1 = \cdots = a_p = 1$ választással kapunk ilyen alakot.)

Megjegyzés. Leosztva a_n^2-tel és átrendezve az egyenletet azt az alternatív megfogalmazást kapjuk, hogy K pontosan akkor nem rendezhető, ha

$$-1 = b_1^2 + \cdots + b_k^2$$

valamilyen $b_1, \ldots, b_k \in K$ elemekre. Ezen állítás bizonyítása megtalálható például az A. R. Rajwade: *Squares* könyv 212. oldalán, 15.1. Tételként.

Legyen tehát most K nem rendezhető, és a fönti a_i-khez tekintsük az alábbi mátrixot:

$$A = \begin{pmatrix} 0 & a_1 & a_2 & \cdots & a_n \\ a_1 & 0 & 0 & \cdots & 0 \\ a_2 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

E mátrix karakterisztikus polinomja

$$\chi_A(\lambda) = \det(\lambda I_{n+1} - A) = \begin{vmatrix} \lambda & -a_1 & -a_2 & \cdots & -a_n \\ -a_1 & \lambda & 0 & \cdots & 0 \\ -a_2 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_n & 0 & 0 & \cdots & \lambda \end{vmatrix}.$$

Kérdés, hogy itt hogyan kaphatunk nem 0 kifejtési tagokat. Ha az első sorból a λ elemet választjuk, akkor a hozzá tartozó részmátrix a λI_n skalármátrix, azaz így egyedül a λ^{n+1} nem 0 taghoz jutunk.

Ha viszont $i \geq 1$-re az első sor $(i+1)$-edik elemét, a $-a_i$-t választjuk, akkor az $(i+1)$-edik sorból csak az első elemet, a $-a_i$-t tudjuk kiválasztani mint nem 0 elemet. Ezután pedig már minden $j \neq 1, i+1$-re a j-edik oszlopból csakis a j-edik elemet, a λ-t választhatjuk. Az ezen kifejtési taghoz tartozó permutáció az $1.$ és $(i+1).$ elem transzpozíciója, vagyis előjele -1.

Tehát

$$\chi_A(\lambda) = \lambda^{n+1} - \sum_{i=1}^{n} a_i^2 \lambda^{n-1} = \lambda^{n+1}.$$

Mármost eszerint A egyedüli sajátértéke (a K bármilyen bővítésében) a 0 lehet, azaz ha diagonális alakja a 0 mátrix kéne, hogy legyen, ami nyilván nem lehet, mert $A \neq 0$. Így A nem diagonalizálható, bár szimmetrikus.

Most lássuk be a másik irányú állítást. Legyen K rendezhető test, rögzítsünk egy rendezést. Ismeretes, hogy létezik egyértelműen ennek egy legbővebb algebrai, rendezett bővítése, melynek rendezése kiterjeszti a K-n lévőt. Ez az L egy úgynevezett valós zárt test. Egy valós zárt test teljesíti, hogy minden pozitív elemnek létezik négyzetgyöke, és minden páratlan fokú polinomnak van benne gyöke. Sőt, ez a két tulajdonság ekvivalens azzal, hogy egy rendezett test valós zárt. (Ezen állítások úgyszintén megtalálhatók az A. R. Rajwade: *Squares* c. könyv $15.$ fejezetében.)

Végezetül Tarski egy tétele (lásd A. Tarski: *A decision method for elementary algebra and geometry*) szerint a rendezett test axiómáihoz hozzávéve az előbbi két tulajdonságot:

$$\forall a \left(a > 0 \implies \exists x (x^2 = a) \right),$$

és minden n páratlan számra a

$$\forall a_0 \forall a_1 \cdots \forall a_n \left(a_n \neq 0 \implies \exists x (a_n x^n + \cdots + a_1 x + a_0 = 0) \right)$$

formulákat, a valós zárt testek így kapott elmélete teljes. Speciálisan bármely két modellje elemien ekvivalens, azaz L elemien ekvivalens $\mathbb{R}$-rel.

Mármost minden n esetén az az állítás, hogy minden L fölötti $n \times n$-es szimmetrikus mátrix diagonalizálható L fölött, elsőrendű formulával kifejezhető. Következésképpen ha $L = \mathbb{R}$-re igaz (márpedig ezt valóban tud-

juk), akkor tetszőleges L valós zárt testre is. Így viszont speciálisan minden $M_n(K)$-beli szimmetrikus mátrix diagonalizálható L fölött, így persze $\overline{K} \geq L$ fölött is. Ezzel a másik irányt is beláttuk.

Második megoldás (Maga Balázs). Először tegyük fel, hogy minden K feletti szimmetrikus mátrix diagonalizálható $\overline{K}$ felett. Állítom, hogy ekkor a -1 nem áll elő négyzetek összegeként. Ez elegendő: az Artin–Schreier-elmélet eredményei alapján egy test pontosan akkor rendezhető, ha a -1 nem áll elő benne négyzetek összegeként. Indirekt tegyük fel, hogy mégis. Ekkor $a_1 = 1$-re és valamely $a_2, a_3..., a_n \in K$ elemekre $\sum_{i=1}^{n} a_i^2 = 0$. Tekintsük a következő mátrixot:

$$A = \begin{bmatrix} a_1^2 & a_1a_2 & \dots & a_1a_n \\ a_2a_1 & a_2^2 & \dots & a_2a_n \\ \dots & \dots & \dots & \dots \\ a_na_1 & a_na_2 & \dots & a_n^2 \end{bmatrix}.$$

Azaz az (i, j) helyre az a_ia_j kerül. Ekkor az A^2 mátrix (s, t) helyre kerülő eleme definíció alapján:

$$\sum_{i=1}^{n} a_s a_i^2 a_t = a_s a_t \sum_{i=1}^{n} a_i^2 = 0.$$

Azaz A^2 nullmátrix. De ekkor ha $S^{-1}AS$ diagonális lenne, az ő négyzete is $0 = S^{-1}A^2S$, azaz $S^{-1}AS$ nullmátrix. Így A is, ami ellentmond $a_1 = 1$-nek. Ezzel az egyik irány bizonyítását befejeztük.

Most tegyük fel, hogy K rendezhető. Ekkor K formálisan valós, azaz a -1 nem négyzetek összege benne. Ebben a bekezdésben az alábbi címen fellelhető eredmények 40–42. oldalára hivatkozunk:
http://homepages.math.uic.edu/ marker/orsay/orsay3.pdf
Vegyük a K test F valós lezártját, azaz K olyan algebrai bővítését, mely formálisan valós, nincs valódi formálisan valós bővítése, s amelyre K rendezése egyértelműen kiterjed. (Corollary 7.12). F tehát egy valós zárt test.

Mivel F valós zárt, nyilván valós zárt testek metszete. Így David Mornhinweg, Daniel B. Shapiro, és K. G. Valente: *The Principal Axis Theorem over Arbitrary Fields* cikkének Theorem 4-e alapján (*The American Mathematical Monthly* Vol. 100, No. 8 (Oct., 1993), 749–754) tetszőleges F feletti szimmetrikus mátrix diagonalizálható F felett. Speciálisan $K \subseteq F \subseteq \overline{K}$ miatt tetszőleges K feletti szimmetrikus mátrix diagonalizálható $\overline{K}$ felett. Ezt akartuk megmutatni.

3. feladat (Tengely Szabolcs és Pongrácz András). Egy α algebrai egészre definiáljuk α pozitív fokát: $\deg^+(\alpha)$ legyen az a minimális $k \in \mathbb{N}$, amelyre van olyan nemnegatív egészekből álló $k \times k$-as mátrix, melynek α sajátértéke. Mutassuk meg, hogy tetszőleges $n \in \mathbb{N}$ esetén minden n-edfokú α algebrai egészre $\deg^+(\alpha) \leq 2n$.

Megoldás (Tengely Szabolcs és Pongrácz András). Ha α n-edfokú algebrai egész, akkor legyen A az a blokkmátrix, mely két $n \times n$-es blokkból áll, és mindkettő α kísérőmátrixa. (A kísérőmátrix az az $n \times n$-es mátrix, melynek a főátlója alatt minden elem 1-es, a jobb szélső oszlopában fentről lefelé α minimálpolinomjának az együtthatói szerepelnek ellentétetes előjellel, index szerint növekvő sorrendben, és minden más eleme 0.) Ha $\underline{u}$ a kísérőmátrix egy sajátvektora α sajátértékkel, akkor legyen $\underline{v}$ az a $2n$-hosszú vektor, melynek első fele $\underline{u}$, második fele $-\underline{u}$. Ekkor a $\underline{v}$ vektor sajátvektora $A+m\cdot E$-nek α sajátértékkel, ahol E a csupa -1 mátrix. Elég nagy m-et választva $A+m\cdot E$ nemnegatív; ezzel $\deg^+(\alpha) \leq 2n$ bizonyítása kész.

4. feladat (Győry Kálmán és Hajdu Lajos). Legyen K egy, a racionális számtesttől és a másodfokú imaginárius számtestektől különböző algebrai számtest. Jelölje $\mathcal{L}(K)$ azon pozitív $n \geq 3$ egészek halmazát, melyekre találhatók olyan K-beli $\varepsilon_1, \ldots, \varepsilon_n$ egységek, hogy

$$\varepsilon_1 + \cdots + \varepsilon_n = 0,$$

de $\sum_{i \in I} \varepsilon_i \neq 0$ az $\{1, \ldots, n\}$ bármely nemüres, valódi I részhalmaza esetén. Igazoljuk, hogy $\mathcal{L}(K)$ végtelen sok elemet tartalmaz, és legkisebb eleme K fokszáma és diszkriminánsa segítségével felülről korlátozható! Mutassuk meg továbbá, hogy végtelen sok K esetén $\mathcal{L}(K)$ végtelen sok páros és végtelen sok páratlan elemet tartalmaz!

Megoldás (Győry Kálmán és Hajdu Lajos). Legyen ε egy tetszőleges K-beli egység, amely nem egységgyök (Dirichlet tétele alapján ilyen létezik), és legyen $f_\varepsilon(x) = x^k + a_1 x^{k-1} + \cdots + a_{k-1}x + a_k$ az ε definiáló főpolinomja. (Nyilván $a_k = \pm 1$.) Vegyük észre, hogy ekkor

$$L(\varepsilon) = 1 + |a_1| + \cdots + |a_{k-1}| + |a_k|$$

jelöléssel egyrészt $L(\varepsilon) > 2$, másrészt $L(\varepsilon) \in \mathcal{L}(K)$. Mivel bármely C konstans esetén $C > L(\varepsilon)$ csak véges sok ε esetén teljesülhet, viszont K

végtelen sok egységet tartalmaz, így $|\mathcal{L}(K)| = \infty$. Másrészt régóta ismert (lásd pl. T. N. Shorey, R. Tijdeman: *Exponential Diophantine Equations* bevezető A fejezetét, amely történeti utalásokat is tartalmaz), hogy bármely (adott típusú) K test tartalmaz olyan ε (egységgyököktől különböző) egységet, amelyre $L(\varepsilon)$ a K fokszáma és diszkriminánsa segítségével felülről korlátozható. Így ugyanez igaz $\mathcal{L}(K)$ legkisebb elemére is.

A második rész bizonyításához legyen p egy páratlan prím, és legyen $K_p = \mathbb{Q}(\varepsilon_p)$, ahol ε_p a $g_p(x) = x^2 + (p+2)x + 1$ polinom egy gyöke. Világos, hogy $g_p(x)$ irreducibilis, K_p egy valós kvadratikus számtest, és $K_p = \mathbb{Q}(\sqrt{p(p+4)})$ miatt a K_p számtestek páronként különbözőek. (Az utóbbi összefüggés abból adódik, hogy ha $q > p$ prím, akkor $p(p+4)$ és $q(q+4)$ négyzetmentes része nyilván különböző.) Legyen most η egy tetszőleges K_p-beli egység, $x^2 + bx + 1$ definiáló főpolinommal. Könnyen ellenőrizhető, hogy ekkor η^2 definiáló főpolinomja $x^2 + (2 - b^2)x + 1$, η^3 definiáló főpolinomja pedig $x^2 + (b^3 - 3b)x + 1$. (Ez rögtön adódik az

$$x^4 + (2 - b^2)x^2 + 1 = (x^2 + bx + 1)(x^2 - bx + 1),$$

$$x^6 + (b^3 - 3b)x^3 + 1 = (x^2 + bx + 1)(x^4 - bx^3 + (b^2 - 1)x^2 - bx + 1)$$

összefüggésekből.) Így indukcióval könnyen adódik, hogy bármely $k \geq 0$ esetén $L(\varepsilon_p^{2^k})$ páratlan, míg $L(\varepsilon_p^{3\cdot 2^k})$ páros. (Ehhez csak azt kell észrevenni, hogy egyrészt $L(\varepsilon_p)$ páratlan, másrészt a fentiek alapján ha $L(\eta)$ páratlan, akkor $L(\eta^2)$ is páratlan, $L(\eta^3)$ viszont páros.) Ez pedig (a korábbiakat is figyelembe véve) állításunkat igazolja.

5. feladat (Totik Vilmos). Egy legalább elsőfokú p polinomra legyen $H_p = \{z \mid |p(z)| = 1\}$. Igazoljuk, hogy ha $H_p = H_q$ valamely p, q polinomokra, akkor van olyan r polinom, hogy $p = r^m$ és $q = \xi \cdot r^n$ valamely m, n pozitív, egész számokkal és $|\xi| = 1$ konstanssal.

Megoldás (Ágoston Tamás). Legyen $H = H_p = H_q$, és $\deg p = m$, $\deg q = n$. Nyilván $H \neq \emptyset$ zárt, hiszen p, q legalább elsőfokúak, vagyis minden komplex értéket fölvesznek. Továbbá mivel p és q polinomok, így ∞-ben ∞-be tartanak, tehát H korlátos. Továbbá speciálisan H szeparálja ∞-t mind p, mind q gyökeitől. Legyen most $m' = \dfrac{m}{(m,n)}$ és $n' = \dfrac{n}{(m,n)}$, és tekintsük az $f(z) = \dfrac{p(z)^{n'}}{q(z)^{m'}}$ racionális törtfüggvényt. Ek-

kor $f \in \mathcal{M}(\mathbb{C})$, azaz f meromorf $\mathbb{C}$-n (sőt $f \in \mathcal{M}(\hat{\mathbb{C}})$, ahol $\hat{\mathbb{C}}$ a Riemann-gömb), és $\deg f = m\frac{n}{(m,n)} - n\frac{m}{(m,n)} = [m,n] - [m,n] = 0$, tehát ∞-ben nem 0 értékkel megszüntethető szingularitása van. Azaz f-et mint a $\hat{\mathbb{C}}$-on értelmezett meromorf függvényt tekintve az összes gyöke és pólusa a p és q gyökei.

Ugyanakkor $|f\|_H = \frac{\left(|p\|_H\right)^{n'}}{\left(|q\|_H\right)^{m'}} \equiv 1$, és H szeparálja ∞-t ezen gyököktől, így $\hat{\mathbb{C}}\setminus H$-nak a ∞-t tartalmazó G összefüggőségi komponensén (G nemüres, összefüggő nyílt) f holomorf, határán pedig $|f|$ azonosan 1. Így a maximumelv miatt $|f\|_{\overline{G}} \leq 1$, azaz $|f|$-nek van lokális minimuma G-ben. A minimumelv szerint ez vagy gyöke f-nek, vagy f konstans. Mivel tudjuk, hogy G-ben nincs gyöke se p-nek, se q-nak, ezért $f|_G \equiv \zeta \in \mathbb{C}$. A G határán pedig $|f| = 1$, így $|\zeta| = 1$.

(A szokásos, $\mathbb{C}$-n értelmezett függvényekre érvényes minimum- és maximumelv itt közvetlenül a $g(z) = f\left(\frac{1}{z}\right)$ függvényre alkalmazható, mely G-nek a $\hat{\mathbb{C}} \to \hat{\mathbb{C}}, z \mapsto \frac{1}{z}$ diffeomorfizmus általi képén holomorf.)

Továbbá $G \subset \hat{\mathbb{C}}$ nemüres nyílt, így persze az egész $\hat{\mathbb{C}}$-n konstans az f, vagyis

$$p^{n'} = \zeta q^{m'}. \tag{1}$$

Így speciálisan $p^{n'}$-ben minden gyök multiplicitása osztható m'-vel, míg $q^{m'}$-ban n'-vel. Viszont az m', n' értékek választása miatt $(m', n') = 1$, így valójában p-ben oszthatók a multiplicitások m'-vel, és q-ban n'-vel. Azaz

$$p(z) = r_1(z)^{m'}, \quad q(z) = r_2(z)^{n'}.$$

Mármost (1) miatt

$$r_1^{m'n'} = \zeta r_2^{m'n'},$$

vagyis $r_2 = \eta r_1$, ahol $\eta^{m'n'} = \zeta$, speciálisan $|\eta| = 1$. Tehát $r = r_1$ és $\xi = \eta^{n'}$ választással (ekkor persze $|\xi| = 1$)

$$p = r_1^{m'} = r^{m'}, \quad q = r_2^{n'} = (\eta r_1)^{n'} = \xi r^{n'}.$$

Márpedig éppen ezt akartuk belátni.

6. feladat (Páles Zsolt). Legyenek I és J intervallumok, $\varphi, \psi : I \to \mathbb{R}$ szigorúan monoton növő és folytonos függvények, továbbá $\Phi, \Psi : J \to \mathbb{R}$ folytonos függvények. Tegyük fel, hogy $\varphi(x)+\psi(x) = x$ és $\Phi(u)+\Psi(u) = u$ teljesül minden $x \in I$, illetve $u \in J$ esetén. Legyen $f : I \to J$ folytonos megoldása az

$$f\Big(\varphi(x) + \psi(y)\Big) \le \Phi(f(x)) + \Psi(f(y)) \qquad (x, y \in I)$$

függvényegyenlőtlenségnek. Mutassuk meg, hogy ekkor $\Phi \circ f \circ \varphi^{-1}$ és $\Psi \circ f \circ \psi^{-1}$ konvex függvények.

Megoldás (Páles Zsolt). A megoldásbeli sorozatok konstrukciójához szükségünk lesz az alábbi lemmára.

Lemma. *A feladat jelölései és feltételei mellett bármely $a, b \in I$, $a < b$ esetén létezik olyan $a < u < v < b$, hogy*

$$u = \varphi(a) + \psi(v), \qquad v = \varphi(b) + \psi(u).$$

A Lemma bizonyítása. Értelmezzük a $g : [a, b] \to \mathbb{R}$ függvényt a

$$g(u) = \varphi(a) + \psi(\varphi(b) + \psi(u))$$

képlettel. Ekkor $u \in [a, b]$ esetén a φ és ψ függvények szigorú monotonitása miatt

$$\begin{aligned} a = \varphi(a) + \psi(\varphi(a) + \psi(a)) &< \varphi(a) + \psi(\varphi(b) + \psi(u)) \\ &< \varphi(b) + \psi(\varphi(b) + \psi(b)) = b, \end{aligned}$$

tehát g az $[a, b]$ intervallumot (a, b)-be képezi. Így g folytonossága miatt g-nek létezik (a, b)-ben egy u fixpontja. Legyen $v := \varphi(b) + \psi(u)$. Ekkor $u = g(u) = \varphi(a) + \psi(v)$ is teljesül, továbbá

$$u = \varphi(u) + \psi(u) < \varphi(b) + \psi(u) = v = \varphi(b) + \psi(u) < \varphi(b) + \psi(b) = b,$$

tehát $u < v < b$ is fennáll.

A feladat megoldásához kimutatjuk, hogy $\Phi \circ f \circ \varphi^{-1}$ Jensen-konvex a $\varphi(I)$ intervallumon.

Legyen $x, y \in I$, $x < y$ rögzített. Ekkor a Lemma alkalmazásával megkonstruálható egy olyan (x_n) szigorúan monoton növő és (y_n) szigorúan monoton csökkenő sorozatok, melyekre $x_1 := x$ és $y_1 := y$, továbbá $n \in \mathbb{N}$

$$x_{n+1} = \varphi(x_n) + \psi(y_{n+1}), \qquad y_{n+1} = \varphi(y_n) + \psi(x_{n+1}).$$

Mivel $x_n < y_n$ is teljesül, így (x_n) felülről, (y_n) pedig alulról korlátos sorozat. Ezért léteznek a $\lim x_n =: u$ és $\lim y_n =: v$ határértékek. A fenti egyenletekben végrehajtva az $n \to \infty$ határátmenetet kapjuk, hogy

$$u = \varphi(u) + \psi(v), \qquad v = \varphi(v) + \psi(u),$$

ahonnan φ és ψ szigorú monotonitása miatt $u = v$ következik. Most megmutatjuk, hogy

$$u = \varphi^{-1}\Big(\frac{\varphi(x) + \varphi(y)}{2}\Big).$$

A rekurziós definíció szerint:

$$\varphi(x_{n+1}) + \psi(x_{n+1}) = \varphi(x_n) + \psi(y_{n+1}),$$
$$\varphi(y_{n+1}) + \psi(y_{n+1}) = \varphi(y_n) + \psi(x_{n+1}).$$

Ezeket összeadva nyerjük, hogy

$$\varphi(x_{n+1}) + \varphi(y_{n+1}) = \varphi(x_n) + \varphi(y_n).$$

Ezt az egyenlőséget iterálva kapjuk, hogy $n \in \mathbb{N}$-re

$$\varphi(x_n) + \varphi(y_n) = \varphi(x) + \varphi(y),$$

amiből az $n \to \infty$ határátmenet elvégzése után

$$2\varphi(u) = \varphi(x) + \varphi(y)$$

adódik, tehát valóban $u = \varphi^{-1}\big(\frac{\varphi(x)+\varphi(y)}{2}\big)$.

Térjünk most rá a tétel állításának igazolására. A függvényegyenlőtlenség teljesülése miatt

$$f(x_{n+1}) = f\Big(M_{\varphi,\psi}(x_n, y_{n+1})\Big) \le \Phi\Big(f(x_n)\Big) + \Phi\Big(f(y_{n+1})\Big)$$

és

$$f(y_{n+1}) = f\Big(M_{\varphi,\psi}(y_n, x_{n+1})\Big) \le \Phi\Big(f(y_n)\Big) + \Psi\Big(f(x_{n+1})\Big),$$

azaz

$$\Phi\Big(f(x_{n+1})\Big) + \Psi\Big(f(x_{n+1})\Big) \le \Phi\Big(f(x_n)\Big) + \Psi\Big(f(y_{n+1})\Big)$$

és

$$\Phi\Big(f(y_{n+1})\Big) + \Psi\Big(f(y_{n+1})\Big) \le \Phi\Big(f(y_n)\Big) + \Psi\Big(f(x_{n+1})\Big).$$

Ezeket összeadva:

$$\Phi\Big(f(x_{n+1})\Big) + \Phi\Big(f(y_{n+1})\Big) \le \Phi\Big(f(x_n)\Big) + \Phi\Big(f(y_n)\Big).$$

Ezt az egyenlőtlenséget iterálva nyerjük, hogy $n \in \mathbb{N}$ esetén

$$\Phi\Big(f(x_n)\Big) + \Phi\Big(f(y_n)\Big) \le \Phi\Big(f(x)\Big) + \Phi\Big(f(y)\Big).$$

Véve az $n \to \infty$ határátmenetet:

$$2\Phi\Big(f(u)\Big) \le \Phi\Big(f(x)\Big) + \Phi\Big(f(y)\Big),$$

amiből $u = \varphi^{-1}\Big(\frac{\varphi(x)+\varphi(y)}{2}\Big)$ figyelembevételével adódik, hogy

$$\Phi \circ f\left(\varphi^{-1}\left(\frac{\varphi(x)+\varphi(y)}{2}\right)\right) \le \frac{\Phi\circ f(x) + \Phi\circ f(y)}{2} \qquad (x, y \in I).$$

Innen $\varphi(x) := s$ és $\varphi(y) := t$ helyettesítésekkel kapjuk, hogy $\Phi \circ f \circ \varphi^{-1}$ Jensen-konvex a $\varphi(I)$ intervallumon. Ebből a folytonosság miatt ennek a függvénynek a konvexitása is következik.

A $\Psi \circ f \circ \psi^{-1}$ függvény konvexitása hasonló módon igazolható.

7. feladat (Csirmaz László). Jellemezzük azokat a pozitív számokból álló növekvő (s_n) sorozatokat, amelyekhez létezik a valós számoknak olyan pozitív mértékű A részhalmaza, hogy minden $\frac{1}{n}$ hosszúságú I intervallum esetén $\lambda(A \cap I) < \frac{s_n}{n}$, ahol λ a Lebesgue-mértéket jelöli.

Megoldás (Elekes Márton). Lebesgue sűrűségi tétele miatt $\lim s_n \ge 1$, megmutatjuk hogy ez elég is. Feltehető, hogy $s_1 \ge 1 - 1/4$, egyébként vesszük a konstrukciót a $[0, 1/2t]$ intervallumon, ahol t az az index, ahonnan $s_n > 1 - 1/4$. Legyen i_k olyan növő, hogy $n > 2^{i_k}$ esetén már $s_n > 1 - 2^{-k}$. Az egységszakasz diadikus 2^{-i_k} hosszú szakaszából kihagyjuk az utolsó 2^{-k}-ad részt. Ami megmarad, az pozitív mértékű, mert $\prod(1 - 2^{-i})$ nem nulla. A

halmaz a diadikus intervallumokra jó, tetszőleges $1/n$ hosszú intervallum lefedhető két, $1/2n$-nél hosszabb diadikus intervallummal. Ami azt jelenti, hogy a konstrukciót a [0,1/2]-re elkészítve készen vagyunk.

Megjegyzés. Persze nem kell, hogy s_n növekvő legyen, ekkor $\liminf s_n \geq 1$ a feltétel.

8. feladat (Gát György). Legyen az $x \in [0,1)$ valós szám 2-es számrendszerbeli alakja: $x = \sum_{i=0}^{\infty} \frac{x_i}{2^{i+1}}$. (Ha x diadikusan racionális, azaz $x \in \left\{\frac{k}{2^n} : k, n \in \mathbb{Z}\right\}$, akkor a véges felírást válasszuk.) Legyen az $f_n : [0,1) \to \mathbb{Z}$ függvény a következő módon megadva:

$$f_n(x) = \sum_{j=0}^{n-1} (-1)^{\sum_{i=0}^{j} x_i}.$$

Van-e olyan $\varphi : [0,\infty) \to [0,\infty)$ függvény, amelyre $\lim_{x\to+\infty} \varphi(x) = \infty$ és

$$\sup_{n\in\mathbb{N}} \int_0^1 \varphi(|f_n(x)|)dx < \infty?$$

Megoldás (Csernák Tamás). Fogalmazzuk át a feladatot a valószínűségszámítás nyelvére: Legyen X a $[0,1)$ intervallumon vett egyenletes eloszlású valószínűségi változó. A kérdés ekkor az, hogy van-e olyan $\varphi : [0,\infty) \to [0,\infty)$, melyre $\lim_{x\to\infty} \varphi(x) = \infty$ és $\sup_{n\in\mathbb{N}} E\left(\varphi(f_n(X))\right) < \infty$ (a várható értékek supremuma).

Legyen X_i az X valószínűségi változó értékének 2-es számrendszerbeli i-edik jegye a feladatban definiált módon. Könnyen ellenőrizhető, hogy $X_0, X_1, \ldots$ független valószínűségi változók és $i \in \mathbb{N}$-re $P(X_i = 0) = P(X_i = 1) = 1/2$. Legyen $T_n = X_0 + X_1 + \ldots + X_n$ (mod 2). Rögzítsük le $T_0 = t_0, \ldots, T_{n-1} = t_{n-1}$ értékeket. A mod 2 összegből persze vissza tudjuk számolni ebben az esetben $X_0, \ldots, X_{n-1}$ értékét, legyen $X_0 = x_0, \ldots, X_{n-1} = x_{n-1}$. Ilyen feltételek mellett persze X_n pontosan egyik lehetséges értékére lesz $T_n = 0$, a másikra $T_n = 1$, tehát $t \in \{0,1\}$-re

$$P(T_n = t | T_0 = t_0, ..., T_{n-1} = t_{n-1}) = P(T_n = t | X_0 = x_0, ..., X_{n-1} = x_{n-1}) = 1/2.$$

Mivel T_n-nek a $T_0, \ldots, T_{n-1}$-re vonatkozó feltételes eloszlása nem függ $T_0, \ldots, T_{n-1}$ értékétől, ezért a T_n valószínűségi változók függetlenek, és $P(T_n = 0) = P(T_n = 1) = 1/2$.

Legyen

$$Y_n = (-1)^{T_n} = (-1)^{\sum_{i=0}^{n} X_i}.$$

Ezek a valószínűségi változók is függetlenek lesznek, mert függetlenek függvényei, és $P(Y_n = 1) = P(Y_n = -1) = 1/2$. A definíció szerint $f_n(X) = \sum_{j=1}^{n-1} Y_j$.

Az Y_n valószínűségi változók várható értéke 0, szórása 1, nézzük a normált összegüket: $Z_n = \frac{\sum_{j=1}^{n-1} Y_j}{\sqrt{n}}$. A centrális határeloszlás-tétel alapján a Z_n valószínűségi változók eloszlásban tartanak az $N(0,1)$ standard normális eloszláshoz.

Jelölje $\Phi(x)$ a standard normális eloszlás eloszlásfüggvényét, $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$. Az eloszlásbeli konvergencia miatt $\lim_{n\to\infty} P(Z_n > 1) = 1 - \Phi(1)$, ezért $\exists n_0, \forall n > n_0$, $P(Z_n > 1) > \frac{1-\Phi(1)}{2}$. Legyen $K \in R$, mivel $\lim_{x\to\infty} \varphi(x) = \infty$, $\exists a, \forall x > a$-ra $\varphi(x) > K$. Legyen $n \in N$ olyan, hogy $n > n_0$ és $\sqrt{n} > a$. Mivel $f_n(X) = Z_n \cdot \sqrt{n}$, ha $Z_n > 1$, akkor $f_n(X) > a$, ekkor persze $|f_n(X)| > a$, $\varphi(|f_n(X)|) > K$, így

$$P(\varphi(|f_n(X)|) > K) \geq P(Z_n > 1) > \frac{1 - \Phi(1)}{2}.$$

Mivel $\varphi(|f_n(X)|)$ nemnegatív, ezért

$$E(\varphi(|f_n(X)|)) \geq K \cdot P(\varphi(|f_n(X)|) > K) > K \cdot \frac{1 - \Phi(1)}{2},$$

ezért $\sup_{n\in N} E\left(\varphi(f_n(X))\right) > K \cdot \frac{1-\Phi(1)}{2}$, de mivel K tetszőlegesen nagyra választható, és amivel meg van szorozva egy fix pozitív konstans, ezért $\sup_{n\in N} E\left(\varphi(f_n(X))\right) = \infty$. Mivel φ is tetszőlegesen választott függvény volt, a feladat feltételeinek megfelelő függvény nincs.

9. feladat (Totik Vilmos). Legyen N lineáris normált tér és M az N egy sűrű lineáris altere. Igazoljuk, hogy ha $L_1, \ldots, L_m$ véges sok lineáris funkcionál N-en, akkor minden $x \in N$-re van olyan x-hez konvergáló M-beli (y_n) sorozat, amelyre $L_j(y_n) = L_j(x)$ teljesül minden $j = 1, \ldots, m$ és $n \in \mathbb{N}$ esetén.

Megoldás (Totik Vilmos). Az

$$U = \Big\{ (L_1(x), \ldots, L_m(x)) \,\Big|\, x \in N \Big\}$$

az $\mathbb{R}^m$ (vagy a $\mathbb{C}$, ha a tér komplex normált tér) egy altere, amelyben

$$U^* = \Big\{(L_1(x), \dots, L_m(x)) \,\Big|\, x \in M\Big\}$$

egy sűrű altér, ezért $U^* = U$. Legyen $k \in \mathbb{N}$ az U dimenziója, és legyenek $x_1, \dots, x_k \in M$ olyan elemek, amelyekre $(L_1(x_j), \dots, L_m(x_j))$ $j = 1, \dots, k$ az U egy bázisa. Mivel véges dimenzióban bármely két norma ekvivalens (így az x_j-k által kifeszített altérben $\max_{j=1}^m |L_j(x)| \sim \|x\|$), azt kapjuk, hogy van olyan C, hogy ha $(v_1, \dots, v_m) \in U$ tetszőleges, akkor van olyan z az $x_1, \dots, x_k$ által kifeszített altérben, amelyre $L_1(z), \dots, L_m(z) = (v_1, \dots, v_m)$ és $\|z\| \le C \max_{j=1}^m |v_j|$. Mármost ha $X_n \to x$, $X_n \in M$ tetszőleges, akkor a $v_{n,j} = L_j(x) - L_j(X_n)$ választással kapunk olyan $z_n \in M$ fenti típusú elemeket, amelyekre $\|z_n\| \le C \max_{j=1}^m |L_j(x) - L_j(X_n)|$, és így $y_n = X_n + z_n$ megfelel minden feltételnek.

10. feladat (Pap Gyula). Legyenek $X_1, X_2, \dots$ független, azonos eloszlású véletlen változók $\mathbb{P}(X_1 = 0) = \mathbb{P}(X_1 = 1) = \frac{1}{2}$ eloszlással. Legyenek Y_1, Y_2, Y_3 és Y_4 független, azonos eloszlású véletlen változók, ahol $Y_1 := \sum_{k=1}^\infty \frac{X_k}{16^k}$. Abszolút folytonos eloszlású-e az $Y_1 + 2Y_2 + 4Y_3 + 8Y_4$, valamint az $Y_1 + 4Y_3$ véletlen változó?

Első megoldás (Pap Gyula). Az X_1 véletlen változó karakterisztikus függvénye

$$\mathbb{E}(\mathrm{e}^{\mathrm{i}tX_1}) = \frac{1}{2} + \frac{1}{2}\mathrm{e}^{\mathrm{i}t} = \frac{1}{2}\mathrm{e}^{\frac{\mathrm{i}t}{2}}\Big(\mathrm{e}^{-\frac{\mathrm{i}t}{2}} + \mathrm{e}^{\frac{\mathrm{i}t}{2}}\Big) = \mathrm{e}^{\frac{\mathrm{i}t}{2}}\cos\Big(\frac{t}{2}\Big), \qquad t \in \mathbb{R}.$$

Nyilván a $\sum_{k=1}^\infty \frac{X_k}{16^k}$ sor 1 valószínűséggel konvergens (hiszen a részletösszegek sorozata monoton növekvő, és nem nagyobb, mint $\sum_{k=1}^\infty \frac{1}{16^k} = \frac{1}{15}$), ezért eloszlásban is konvergens, így Lévy folytonossági tétele alapján Y_1 karakterisztikus függvénye

$$\begin{aligned}\mathbb{E}\Big(\mathrm{e}^{\mathrm{i}tY_1}\Big) &= \lim_{n\to\infty} \mathbb{E}\left(\exp\left\{\mathrm{i}t\sum_{k=1}^n \frac{X_k}{16^k}\right\}\right) = \lim_{n\to\infty}\prod_{k=1}^n \mathbb{E}\Big(\mathrm{e}^{\frac{\mathrm{i}tX_k}{16^k}}\Big) \\ &= \prod_{k=1}^\infty \Big(\mathrm{e}^{\frac{\mathrm{i}t}{2\cdot 16^k}}\cos\Big(\frac{t}{2\cdot 16^k}\Big)\Big) = \mathrm{e}^{\frac{\mathrm{i}t}{30}}\prod_{k=1}^\infty \cos\Big(\frac{t}{2\cdot 16^k}\Big), \qquad t \in \mathbb{R}.\end{aligned}$$

Így $Y_1 + 2Y_2 + 4Y_3 + 8Y_4$ karakterisztikus függvénye

$$
\begin{aligned}
&\mathbb{E}\big(\mathrm{e}^{\mathrm{i}t(Y_1+2Y_2+4Y_3+8Y_4)}\big)\\
&=\mathrm{e}^{\frac{(1+2+4+8)\mathrm{i}t}{30}}\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 16^k}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{2t}{2\cdot 16^k}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{4t}{2\cdot 16^k}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{8t}{2\cdot 16^k}\Big)\\
&=\mathrm{e}^{\frac{\mathrm{i}t}{2}}\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 2^{4k}}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 2^{4k-1}}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 2^{4k-2}}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 2^{4k-3}}\Big)\\
&=\mathrm{e}^{\frac{\mathrm{i}t}{2}}\prod_{\ell=1}^{\infty}\cos\Big(\frac{t}{2\cdot 2^{\ell}}\Big)=\prod_{\ell=1}^{\infty}\Big(\mathrm{e}^{\frac{\mathrm{i}t}{2\cdot 2^{\ell}}}\cos\Big(\frac{t}{2\cdot 2^{\ell}}\Big)\Big)=\lim_{n\to\infty}\prod_{\ell=1}^{n}\mathbb{E}\Big(\mathrm{e}^{\frac{\mathrm{i}tX_\ell}{2^\ell}}\Big)\\
&=\lim_{n\to\infty}\mathbb{E}\left(\exp\left\{\mathrm{i}t\sum_{\ell=1}^{n}\frac{X_\ell}{2^\ell}\right\}\right),\qquad t\in\mathbb{R}.
\end{aligned}
$$

Tetszőleges pozitív egész n esetén $\sum_{\ell=1}^{n}\frac{X_\ell}{2^\ell}$ egyenletes eloszlású a $\{0,\frac{1}{2^n},\dots,\frac{2^n-1}{2^n}\}$ halmazon, így eloszlásfüggvénye legfeljebb $\frac{1}{2^n}$-nel tér el a $(0,1)$ intervallumon egyenletes eloszlás eloszlásfüggvényétől, ezért $\sum_{\ell=1}^{n}\frac{X_\ell}{2^\ell}$ eloszlásban konvergál a $(0,1)$ intervallumon egyenletes eloszláshoz, tehát Lévy folytonossági tétele alapján $Y_1+2Y_2+4Y_3+8Y_4$ egyenletes eloszlású a $(0,1)$ intervallumon, ami abszolút folytonos eloszlás.

Hasonlóan számolva Y_1+4Y_3 karakterisztikus függvénye

$$
\begin{aligned}
\mathbb{E}\big(\mathrm{e}^{\mathrm{i}t(Y_1+4Y_3)}\big)&=\mathrm{e}^{\frac{(1+4)\mathrm{i}t}{30}}\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 16^k}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{4t}{2\cdot 16^k}\Big)\\
&=\mathrm{e}^{\frac{\mathrm{i}t}{6}}\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 4^{2k}}\Big)\prod_{k=1}^{\infty}\cos\Big(\frac{t}{2\cdot 4^{2k-1}}\Big)\\
&=\mathrm{e}^{\frac{\mathrm{i}t}{6}}\prod_{\ell=1}^{\infty}\cos\Big(\frac{t}{2\cdot 4^{\ell}}\Big)=\prod_{\ell=1}^{\infty}\Big(\mathrm{e}^{\frac{\mathrm{i}t}{2\cdot 4^k}}\cos\Big(\frac{t}{2\cdot 4^{\ell}}\Big)\Big)\\
&=\mathbb{E}\left(\exp\left\{\mathrm{i}t\sum_{\ell=1}^{\infty}\frac{X_\ell}{4^\ell}\right\}\right),\qquad t\in\mathbb{R},
\end{aligned}
$$

ezért Y_1+4Y_3 eloszlása megegyezik a $\sum_{\ell=1}^{\infty}\frac{X_\ell}{4^\ell}$ véletlen változó eloszlásával, ahol a $\sum_{\ell=1}^{\infty}\frac{X_\ell}{4^\ell}$ sor is nyilván 1 valószínűséggel konvergens. A $\sum_{\ell=1}^{\infty}\frac{X_\ell}{4^\ell}$ véletlen változó lehetséges értékei azok a $[0,\frac{1}{2}]$ intervallumba eső számok, melyek felírhatók a 4-es számrendszerben a 0 és 1 számjegyek segítségével, tehát nem eshetnek a $H:=\cup_{\ell=1}^{\infty}\Big[\Big(\frac{1}{2^{\ell+2}},\frac{2}{2^{\ell+2}}\Big)\cup\Big(\frac{2^\ell+1}{2^{\ell+2}},\frac{2^\ell+2}{2^{\ell+2}}\Big)\Big]$ halmazba, aminek a Lebesgue-mértéke $\frac{1}{2}$. Ezért az Y_1+4Y_3 véletlen változó 1 valószínűséggel beleesik a $[0,\frac{1}{2}]\setminus H$ halmazba, aminek a Lebesgue-

mértéke 0, vagyis az $Y_1 + 4Y_3$ véletlen változó nem lehet abszolút folytonos eloszlású. □

Második megoldás (Barczy Mátyás). Az $Y_1 + 2Y_2 + 4Y_3 + 8Y_4$ véletlen változó eloszlása megegyezik a $\sum_{k=1}^{\infty} \frac{X_k^{(1)}+2X_k^{(2)}+4X_k^{(3)}+8X_k^{(3)}}{16^k}$ eloszlásával, ahol $\left\{X_j^{(\ell)} : j \in \{1,2,\ldots\}, \ell \in \{1,2,3,4\}\right\}$ független kópiái az X_1 véletlen változónak. Nyilván a $\sum_{k=1}^{\infty} \frac{X_k^{(1)}+2X_k^{(2)}+4X_k^{(3)}+8X_k^{(3)}}{16^k}$ sor 1 valószínűséggel konvergens (hiszen a részletösszegek sorozata monoton növekvő, és nem nagyobb, mint $\sum_{k=1}^{\infty} \frac{15}{16^k} = 1$), ezért eloszlásban is konvergens. Tetszőleges pozitív egész n esetén $\sum_{k=1}^{n} \frac{X_k^{(1)}+2X_k^{(2)}+4X_k^{(3)}+8X_k^{(3)}}{16^k}$ egyenletes eloszlású a $\{0, \frac{1}{16^n}, \ldots, \frac{16^n-1}{16^n}\}$ halmazon, így eloszlásfüggvénye legfeljebb $\frac{1}{16^n}$-nel tér el a $(0,1)$ intervallumon egyenletes eloszlás eloszlásfüggvényétől, ezért $\sum_{k=1}^{n} \frac{X_k^{(1)}+2X_k^{(2)}+4X_k^{(3)}+8X_k^{(3)}}{16^k}$ eloszlásban konvergál a $(0,1)$ intervallumon egyenletes eloszláshoz, tehát $Y_1 + 2Y_2 + 4Y_3 + 8Y_4$ egyenletes eloszlású a $(0,1)$ intervallumon, ami abszolút folytonos eloszlás.

Az $Y_1 + 4Y_3$ véletlen változó eloszlása megegyezik a $\sum_{k=1}^{\infty} \frac{X_k^{(1)}+4X_k^{(3)}}{16^k}$ eloszlásával, ahol a $\sum_{k=1}^{\infty} \frac{X_k^{(1)}+4X_k^{(3)}}{16^k}$ sor is nyilván 1 valószínűséggel konvergens. A $\sum_{k=1}^{\infty} \frac{X_k^{(1)}+4X_k^{(3)}}{16^k}$ véletlen változó lehetséges értékeinek A halmazát azok a $[0,1]$ intervallumba eső számok alkotják, melyek felírhatók a 16-os számrendszerben a 0, 1, 4 és 5 számjegyek segítségével. Ez az A halmaz úgy keletkezik, hogy a $[0,1]$ intervallumból először kivesszük a $\left(\frac{2}{16}, \frac{4}{16}\right) \cup \left(\frac{6}{16}, \frac{16}{16}\right)$ halmazt, mert ebben vannak azok a $[0,1]$ intervallumbeli számok, amelyek 16-os számrendszerbeli alakjában a nulla utáni első számjegy különbözik a 0, 1, 4 és 5 számjegyektől, így a $\frac{2}{16} + \frac{10}{16} = \frac{3}{4}$ részt vesszük ki. Utána a maradék halmazból azt a halmazt vesszük ki, amelyben a nulla utáni második számjegy különbözik a 0, 1, 4 és 5 számjegyektől, így a maradéknak megint a $\frac{3}{4}$ részét kell eltávolítani, és így tovább. Tehát a $[0,1]$ intervallumból kivett halmaz Lebesgue-mértéke $\frac{3}{4} + \frac{3}{4^2} + \frac{3}{4^3} + \cdots = 1$, így az A halmaz Lebesgue-mértéke 0. Ezért az $Y_1 + 4Y_3$ véletlen változó 1 valószínűséggel beleesik az A halmazba, aminek a Lebesgue-mértéke 0, vagyis az $Y_1 + 4Y_3$ véletlen változó nem lehet abszolút folytonos eloszlású. □

Megjegyzések a feladathoz. Könnyű belátni, hogy a $\sum_{\ell=1}^{\infty} \frac{X_\ell}{4^\ell}$ véletlen változó eloszlásfüggvénye folytonos, ezért az eloszlása nem tartalmaz ato-

mot, vagyis nem diszkrét. Tehát $Y_1 + 4Y_3$ folytonos szinguláris eloszlású véletlen változó.

Az első megoldás első részében felhasználható, hogy minden $t \in \mathbb{R} \setminus \{0\}$ esetén $\prod_{\ell=1}^{\infty} \cos\left(\frac{t}{2\cdot 4^\ell}\right) = \frac{\sin(t/2)}{t/2}$, és így $Y_1 + 2Y_2 + 4Y_3 + 8Y_4$ karakterisztikus függvénye $\mathrm{e}^{\frac{\mathrm{i}t}{2}} \frac{\sin(t/2)}{t/2}$, ami éppen a $(0,1)$ intervallumon egyenletes eloszlás karakterisztikus függvénye.

Barczy Mátyás megjegyzése

Az első megoldás második részét úgy is be lehet fejezni, hogy az Y_1+4Y_3 karakterisztikus függvénye $\mathrm{e}^{\frac{(1+4)\mathrm{i}t}{30}} \prod_{k=1}^{\infty} \cos\left(\frac{t}{2\cdot 16^k}\right) \prod_{k=1}^{\infty} \cos\left(\frac{4t}{2\cdot 16^k}\right)$, $t \in \mathbb{R}$, amely a $16^N \cdot 2\pi$, $N \in \{1,2,\ldots\}$ sorozat mentén nem konvergál 0-hoz, mert az abszolút értéke egy pozitív konstans, mégpedig $\prod_{k=1}^{\infty} \cos\left(\frac{\pi}{16^k}\right) \prod_{k=1}^{\infty} \cos\left(\frac{4\pi}{16^k}\right)$, hiszen $\sum_{k=1}^{\infty}\left(1-\cos\left(\frac{\pi}{16^k}\right)\right) \leq \sum_{k=1}^{\infty} \frac{\pi^2}{2\cdot 16^{2k}} < \infty$ és hasonlóan $\sum_{k=1}^{\infty}\left(1-\cos\left(\frac{4\pi}{16^k}\right)\right) \leq \sum_{k=1}^{\infty} \frac{8\pi^2}{16^{2k}} < \infty$. Viszont ha az Y_1+4Y_3 véletlen változó abszolút folytonos eloszlású volna, akkor a karakterisztikus függvénye a Riemann–Lebesgue-lemma szerint 0-hoz konvergálna végtelenben, tehát az $Y_1 + 4Y_3$ véletlen változó nem lehet abszolút folytonos eloszlású. □

Tartalom

Contents