Pierre Fermat és a nyilvános kulcsú rejtjelzés

P. Fermat születésének 400. évfordulójára

Pierre Fermat (1601–1665) pontosan 100 évvel Girolamo Cardano (1501–1576) születése után, 1601-ben született.

A következőkben a nevéhez kötődő kis Fermat-tételről lesz szó, amelynek jelzője ellenére alapvető hatása van napjaink információ-titkosítására. Fermat eredeti tételét ma a következő formában mondjuk ki:

Kis Fermat-tétel: *Ha p prímszám és a nem osztható p-vel, akkor*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

(A kongruencia[1] fogalmát Gauss vezette be.)

Fermat bizonyítása azonban ebben az esetben sem maradt fenn. Az első bizonyítás majd 100 évig váratott magára és Leonhard Eulertől (1707–1783), a XVIII. század matematikus óriásától származik. Euler egyben a tétel általánosítását is bebizonyította, így ma Euler–Fermat-tételnek nevezzük:

Euler–Fermat-tétel: *Ha $m > 1$ egész szám és $(a, m) = 1$, azaz a és m relatív prímek,*[2] *akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2}$$

A tételben szereplő Euler-féle $\varphi(m)$ függvény jelenti az $1, 2, \ldots, m$ számok közül az m-hez relatív prímek számát.

Például: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$ ...

Általában igaz, hogy ha $m = p$ prímszám, akkor

$$\varphi(p) = p - 1. \tag{3}$$

Ebből az is könnyen belátható, hogy ha p és q különböző prímek, akkor

$$\varphi(pq) = (p-1)(q-1). \tag{4}$$

A prímszámoknak és a számok osztóinak fontos jelentést tulajdonítottak az ókori számmisztikában olyannyira, hogy Pithagorasz és követői, (i.e. VI–V. század), úgy tartották, hogy „*A dolgok természete, lényege: a szám.*” De nemcsak hirdették, hanem

[1] $a \equiv b \pmod{c}$, amit a kongruens b modulo c-nek olvasunk, és azt jelenti, hogy ha a-t és b-t a c-vel osztjuk, akkor egyenlő maradékot kapunk, azaz $a = xc + b$, ahol x egész szám.

[2] Két egész számot (például a és m) relatív prímnek mondunk, ha 1-en kívül nincs közös pozitív osztójuk. Jelölése: $(a, m) = 1$.

szerintük a természeti és társadalmi jelenségeket valóban a számok csodálatos tulajdonságai „testesítették meg”. A pitagoreusok ugyanis nem a számokat személyesítették meg, hanem – többek között – a személyes (emberi) tulajdonságokat „számosították meg”.

Tökéletesnek tartottak például egy számot, ha az megegyezett a nála kisebb pozitív osztóinak összegével. Tökéletes számok[3] a $6=1+2+3$ és a $28=1+2+4+7+14$. A pitagoreusok csak néhány tökéletes számot ismertek, így a 496-ról és a 8128-ról is tudtak. A matematikusok az ókor óta nem tudják, hogy van-e végtelen sok tökéletes szám. Az ötödik tökéletes számot, a 33 550 336-ot a XV. században találták meg, míg a XVI. század adta a hatodik és hetedik tökéletes számot, ezek a $2^{16}(2^{17}-1)$ és a $2^{18}(2^{19}-1)$. Látható, hogy amint a tökéletes számok között haladunk „előre”, egyre nagyobb távolságok vannak, így nem meglepő, hogy egyre nehezebb újabb tökéletes számokat találni. A nyolcadik tökéletes szám megtalálására a XVIII. századig kellett várni, amikor Leonhard Euler kimutatta, hogy a $2^{30}(2^{31}-1)$ is tökéletes szám. A számítógépek megjelenéséig még négy tökéletes számot sikerült megtalálni a XIX. században kézi számolással, ezek a $2^{60}(2^{61}-1)$, $2^{88}(2^{89}-1)$, $2^{106}(2^{107}-1)$ és a $2^{126}(2^{127}-1)$.[4] Modern számítógépekkel a XX. században még nagyobb tökéletes számokat sikerült előállítani, így ma már tudjuk, hogy $2^{520}(2^{521}-1)$, $2^{616}(2^{617}-1)$, $2^{1278}(2^{1279}-1)$, $2^{2170}(2^{2171}-1)$, $2^{2202}(2^{2203}-1)$, $2^{2280}(2^{2281}-1)$, $2^{3216}(2^{3217}-1)$, $2^{44496}(2^{44497}-1)$ is tökéletes számok.[5]

A pitagoreusok beszéltek barátságos számokról is. Azt mondták, hogy két szám barátságban áll egymással, ha bármelyikük nála kisebb pozitív osztóinak összege pontosan a másik számot adja. Barátságos számok például a 220 és 284, ugyanis

a 220 osztóinak összege: $1+2+4+5+10+11+20+22+44+55+110=284$,

a 284 osztóinak összege: $1+2+4+71+142=220$.

A barátságos számok története is sok évszázados történet. Már a régiek ismerték a barátságos 1184 és 1210 számpárt, majd Pierre Fermat mutatta ki ugyanezt a 17 296 és 18 416 számpárról. René Descartes (1596–1650), a matematika másik nagy alakja volt,[6]

---

[3] Már Euklidesz (i.e. 300 körül) jellemezte a páros tökéletes számokat: *Ha* $1+2+\ldots+2^n=2^{n+1}-1$ *prímszám (azaz* 1*-en és önmagán kívül nincs más pozitív osztója), akkor* $2^n(2^{n+1}-1)$ *tökéletes szám, és minden páros tökéletes szám ilyen alakú. Nem ismeretes páratlan tökéletes szám.*

[4] Ezek leírásához a tízes számrendszerben 40, 60, 80 számjegyre van szükség. Képzeljük el, hogy mekkora munkát jelentett ezekkel a számokkal számítógép (vagy akár egyszerű számológép) nélkül számolni!

[5] Ezek a számok még a mai számítógépek számára is kemény feladatot jelentenek, hiszen a fenti utolsó szám pontos leírásához majdnem 30 000 tízes számrendszerbeli számjegyre van szükség. Vajon hány tökéletes szám van még a hátralevő végtelen sok természetes szám között? Még 20, vagy 100? Egyáltalán véges számú, vagy végtelen sok? A kérdés egyszerűnek tűnik, mégis máig megfejtetlen titok.

Egy adott számról aránylag könnyű feladat eldönteni, hogy tökéletes szám-e, de mint láthattuk a tökéletes számokat megtalálni nagyon nehéz. Általánosságban is igaz, hogy ismert kulccsal a hozzá tartozó zárat kinyitni könnyű, de egy zárhoz megtalálni számtalan kulcs közül azt, amelyik kinyitja, már jóval nehezebb.

[6] Ma már minden általános iskolás gyerek találkozik vele például a derékszögű koordinátarendszer tanulásakor, amelyet róla neveztek el Descartes-féle koordinátarendszernek.

fedezte fel a barátságos 9 363 584 és 9 437 056 számpárt, majd Euler a XVIII. században még 61 barátságos számpárt talált meg.

A számmisztika már régen homályba merült, de a harmóniába, a harmonikus szépségbe vetett hit napjainkig fennmaradt. És fennmaradt az a számtalan örökérvényű gondolat, tudományos tétel is, amely e misztikus gondolkodás talaján fogant és mégis a természet mély összefüggéseit írja le. Mint a bemutatott példák is mutatják, néha olyan mély titkokat sikerült a pitagoreusoknak „számszerűsíteni", hogy még a mai napig sem ismerjük hozzájuk a kulcsot. Napjaink kriptográfiája[7] nagy részben ezekre az évezredes meg nem fejtett titkokra épül.

Igen érdekes magyar vonatkozásokra derül fény a prímszámokkal és a kis Fermat-tétellel kapcsolatban, *Kiss Elemér* marosvásárhelyi matematikus és Bolyai-kutató tollából. 1999-ben megjelent könyvében (lásd [8]) eddig ismeretlen dokumentumokra alapozva egészen új képet kapunk Bolyai Jánosról. Kiss Elemér könyvéből kiderül, hogy az idősödő Bolyai János sokat foglalkozott a prímszámokkal. Erről így ír ő maga:

„*Az egész számtan sőt az egész tan mezején alig van szebb és érdekesebb . . . s a legnagyobb nyiászok (matematikusok) figyelme és eleje óta elfoglalt tárgy, mint a főszámok (prímszámok) oly mély homályban rejlő titka.*"[8]

Bolyai is, mint a pitagoreusok óta annyi matematikus, az úgynevezett prímszám képletet kereste, vagyis olyan formulát, amely közvetlen összefüggést ad meg az n-edik prímszám értékére. 1855 tájékán még úgy gondolta, hogy sikerült megtalálnia a titok megfejtését:

„*Azt megmutatni, hogy bármely* 2^p-1 *alakú szám prím mihelyt* p *prím, ugyanakkor amikor a* $2^{2^m}+1$*-gyel bajlódám, magam is megkísértettem, mert amint irataim is megmutatják én is abban a sejtelemben voltam, hogy* 2^p-1 *mindig prím, ha* p *prím. Ez egy történeti fontosságú felfedezése volna a legelső olyan függvénynek, mely mindig prímet ad. Azonban ez sem valósul meg, mert például* $2^{11}-1=2047=23\cdot 89\ldots$"[9]

Apja, Bolyai Farkas ösztönzésére megkísérelte bebizonyítani a kis Fermat-tétel megfordítását, mivel ha ez sikerül, akkor megkapta volna a vágyott prímszámképletet. Így például igaz-e, hogy *ha* $2^{p-1}-1$ *osztható* p*-vel, akkor* p *biztosan prímszám.* Néhány kísérlet után azonban rádöbbent, hogy a bizonyítás lehetetlen, a kis Fermat tétel általában nem fordítható meg. Ellenpéldákat keresve felfedezte a legkisebb úgynevezett pszeudoprím számot, a 341-et. Könnyű ellenőrizni, hogy $341=11\cdot 31$ osztója $(2^{230}-1)$-nek. Ez persze túl enyhe követelménynek tűnik, a kis Fermat-tétel minden, az n-hez relatív prím a számra megköveteli, hogy

$$a^{n-1}\equiv 1 \pmod{n} \tag{5}$$

teljesüljön. Gyorsan kiderül, hogy

$$3^{340}\equiv 56 \pmod{341},$$

[7] A kriptográfia a rejtjelzéssel foglalkozó tudomány.

[8] Idézet [8] 77. oldal.

[9] Idézet [8] 87. oldal.

így a 341 nem teljesíti a kis Fermat-tétel állításában kimondottakat.

A valódi megfordítás azt jelentené, hogy ha (5) mindannyiszor teljesül, valahányszor $(a, n) = 1$, akkor az n prímszám. A kis Fermat-tétel azonban még így sem fordítható meg: vannak olyan összetett számok, a legkisebbik az 1729, amelyek a kis Fermat-tétel szerint prímként viselkednek.

Az ilyen n számokat nevezzük *Carmichael-számoknak,* amelyekről csak 1992-ben sikerült bebizonyítani, hogy végtelen sok létezik belőlük.

A modern kriptográfia az 1970-es években újra „felfedezte” a számelméleti eszközöket. Az időpont talán nem véletlen, hiszen ekkorra tehető a globális információs rendszerek, a globális kommunikáció, az „információ robbanás” korszakának kezdete, amely óriási feladatot jelentett az információ biztonságos tárolásával és továbbításával foglalkozóknak.

A klasszikus titkosítás megfelelő (szigorú) titoktartást és pontos szervezést igényelt, hiszen illetéktelen kezekben a „titkos kulcs” végzetes lehetett. Az *illetéktelen küldő* ugyanis képessé vált olyan üzenetek küldésére, amelyekről a fogadó nem tudhatta, hogy nem a valódi feladótól származnak, míg az *illetéktelenül a titkos kulcs birtokába jutott fogadó* el tudta olvasni a másnak címzett üzenetet. A kockázat csökkentése érdekében a titkos kulcsot rendszeresen változtatták, ami viszont igen pontos (és titkos!) szervezést igényelt, hiszen erről a változásról a küldő és fogadó fél „egyszerre” kellett, hogy értesüljön.

W. S. Jevons már 1873-ban megjelent könyvében megfogalmazta (lásd [7]) azt az elvet, hogy vannak bizonyos matematikai műveletek, amelyek elvégzése nagyon egyszerű (ilyen például az összeadás, vagy a szorzás), de az eredményből a kiindulási komponensek visszaállítása igen nehéz, sokszor reménytelen. Illusztrációként bemutatja az azóta róla elnevezett 10 jegyű számot, a Jevons-számot (8 616 460 799), amely két prímszám szorzata, ám a prímtényezők meghatározását (a prímfaktorizációt) akkor reménytelennek látta.[10] Hogy Jevons ezzel a felvetésével mennyire megelőzte korát, azt mi sem bizonyítja jobban, mint hogy pontosan 100 év szunnyadás után, az 1970-es évek elején merült fel ismét e gondolat. Erdős Pál és Surányi János [5]-ben így fogalmazza meg a problémát:

„Létezhet-e azonban olyan rejtjelzés, amelyiknél nem lehet kitalálni, hogy hogyan kell azt visszacsinálni? Első pillanatban ez valószínűtlennek látszik, mégis az Euler–Fermat-tétel, továbbá a számítógépek rendkívüli teljesítőképessége egy oldalról, a teljesítőképességük határa a másik oldalról lehetőséget ad erre.”

Világos, hogy ahhoz, hogy az Euler–Fermat-tétel alkalmazható legyen, az üzenetnek numerikusnak kell lennie, vagyis a betűkből és egyéb írásjelekből álló szövegeket számokká kell alakítani. Ez azonban könnyen megtehető a klasszikus helyettesítéses titkosítási eljárással, amikor minden egyes írásjelnek egy-egy számot feleltetünk meg.[11] Napjaink digitális világában már nem csupán a szöveges üzeneteket, hanem a kép és hang üzeneteket is számok sorozatává alakítják, így tárolják és továbbítják a kommunikációs vonalakon, aminek sok egyéb mellett az az előnye, hogy így jóval biztonságosabb

---

[10] A Jevons-szám faktorizációjára e cikk végén visszatérünk.

[11] Az egyik legismertebb ilyen eljárás a számítástechnikában nemzetközi szabványként alkalmazott ASCII kód, amely az ábécé kis és nagybetűihez, az elválasztó és műveleti jelekhez a 0–255 intervallum számait rendeli hozzá.

adatvédelem érhető el, mint az úgynevezett analóg jeleknél. Ez azt jelenti, hogy nincs akadálya annak, hogy a továbbiakban üzeneten mindig számokat értsünk. Így már kézenfekvőbbnek tűnik, hogy a számelmélet eredményeit, ezen belül az Euler–Fermat-tételt is felhasználjuk a titkosításra. Legyen eljárásunk a következő:

a) Válasszunk két különböző p, q prímszámot, amelyek szorzata

$$pq = N. \tag{6}$$

b) Ha a továbbítandó üzenet (mint szám) nagyobb mint N, akkor bontsuk fel N-nél kisebb részekre. Egy ilyen rész legyen h. Tehát fennáll, hogy

$$0 < h < N. \tag{7}$$

c) Legyen továbbá r és m két pozitív egész szám, amelyekre

$$rm \equiv 1 \pmod{\varphi(N)}, \tag{8}$$

ami pontosan azt jelenti, hogy

$$rm = 1 + k\varphi(N), \tag{9}$$

ahol (4) szerint $\varphi(N) = (p-1)(q-1)$.

d) Ekkor az $R(h)$ rejtjelzés legyen h^r nemnegatív maradéka N-nel osztva.

e) Ha az így rejtjelzett üzenet h', akkor a megoldó kulcs $M(h')$, a $(h')^m$ nemnegatív maradéka, amely az N-nel való osztáskor keletkezik.

Be kell tehát látnunk, hogy e két kulcs kielégíti az alábbi összefüggést:

$$M(h') = M(R(h)) = h. \tag{10}$$

Nos, a fentiek szerint igazak az alábbi összefüggések:

$$M(h') = M(R(h)) \equiv h^{rm} = h^{1+k\varphi(N)} = h \cdot h^{k\varphi(N)} \pmod{N} \tag{11}$$

Ha $(h, N) = 1$, akkor az Euler–Fermat-tétel szerint:

$$h^{k\varphi(N)} = \left(h^{\varphi(N)}\right)^k \equiv 1 \pmod{N}. \tag{12}$$

Tehát

$$h^{rm} \equiv h \pmod{N}, \tag{13}$$

és (7) szerint (13) jobb oldala éppen h^{rm} legkisebb nemnegatív maradéka, azaz ebben az esetben teljesül a (10) összefüggés.

Vizsgáljuk most meg a még lehetséges $(h, N) = p$ esetet (a $(h, N) = q$ eset ugyanígy kezelhető). Ekkor

$$(h, q) = 1, \tag{14}$$

így a kis Fermat-tétel alapján

$$h^{q-1} \equiv 1 \pmod{q} \qquad \text{tehát} \qquad h^{k(p-1)(q-1)} \equiv 1 \pmod{q}. \tag{15}$$

Szorozzuk a fenti kongruenciát h-val:

(16) $$h \cdot h^{k(p-1)(q-1)} \equiv h \pmod{hq}.$$

Ekkor $p \mid h$ folytán most is teljesül:

(17) $$h^{rm} = h \cdot h^{k\varphi(N)} \equiv h \pmod{N}.$$

A fenti eljárás tehát kielégíti a (10) összefüggést. Ezt vették észre az 1970-es évek közepén R. L. Rivest, A. Shamir és L. Adleman az MIT (Massachusetts Institute of Technology) munkatársai, majd a részletes kidolgozás után, 1978-ban hozták nyilvánosságra (lásd [13]) és szabadalmaztatták (lásd [14]). Nevük kezdőbetűi alapján RSA algoritmusként lett közismert az egész világon és vált az egyik legnagyobb példányszámban felhasznált szoftver és hardver termékké.

Fermat 250 évvel korábbi eredményére alapozva tehát Jevons javaslata 100 évvel később megvalósult. Az RSA algoritmus valóban a titkosítás egészen új korszakát nyitotta meg, amelyet *„nyilvános kulcsú rejtjelzésnek”* hívunk. Miért?

A KöMaL szeptemberi számában (KöMaL 2001/6. 325–335. oldal) bemutatott klasszikus titkosítási eljárásokkal szemben, itt két kulccsal dolgozunk, amelyek közül az egyik nyilvánosságra hozható (ez a nyilvános kulcsnak nevezett N, r pár) anélkül, hogy a rejtjelzés biztonsága sérülne. Lássuk, miért hozható nyilvánosságra N és r.

– Jól választva két elég nagy p, q prímszámot (ezek ma már többszáz jegyű prímszámok) kiszámíthatjuk N-et és $\varphi(N) = (p-1)(q-1)$-et.

– Ezután alkalmasan választott r-rel az euklideszi algoritmust végrehajtva ellenőrizzük, hogy $(r,\varphi(N)) = 1$ teljesül-e.

– Végül r-hez meghatározzuk azt az m számot, amelyre (8) teljesül, amihez szintén euklideszi algoritmust használunk.

Mindezen műveletek közül a nagy prímszámok előállítása a legkritikusabb, de erre ma már elég gyors eljárásokkal rendelkezünk.

Ha tehát N-et és r-et mint nyilvános kulcsot közzétesszük, akárcsak a telefonkönyvben a telefonszámokat, és p, q, m-et tartjuk csupán titokban (ez utóbbi a csak általunk használható és használandó titkos kulcs), akkor ahhoz, hogy valaki illetéktelenül hozzájusson titkunkhoz, N-et kell törzstényezőkre bontania. Erről pedig érdemes felidézni Martin Gardner, a Scientific American világhírű rovatvezetőjének 1977-es gondolatait, amely éppen R. L. Rivest-re hivatkozik: *„Ha a ma ismert legjobb algoritmust és a leggyorsabb számítógépeket használjuk, egy ilyen* 125*-jegyű RSA kulcs megfejtésére, Rivest becslése szerint a szükséges megfejtési idő körülbelül* 40 *kvadrillió év! Ez azt jelenti, hogy praktikusan a belátható jövőben reménytelen az RSA kulcsok faktorizáció útján történő megfejtése. Ugyanakkor maga Rivest és kollégái is elismerik, hogy semmilyen elméleti bizonyítékuk nincs arra, hogy az RSA titkosítási eljárás megfejthetetlen.”*

Érdekes a gondolatok hasonlósága miatt is felidézni Jevons több mint száz évvel korábbi nézetét, amelyet a Jevons számmal kapcsolatban írt le [7]-ben:

„Meg tudja mondani az Olvasó, hogy melyik két szám összeszorzásából adódik a 8 616 460 799 *szám? Úgy gondolom, reménytelen, hogy akárki (magamat is beleértve), valaha megtudja.”*

Természetesen akkor még nem voltak másodpercenként millió műveletet végző számítógépek, így a megoldás csak kézi számolással volt elképzelhető (illetve elképzelhetetlen). A technika azóta nagyot fejlődött. Ma már egy ekkora szám faktorizációja számítógéppel nem okoz problémát. Ezért használnak az RSA algoritmusnál többszáz jegyű számokat, amelyek faktorizációja a számítástechnika mai szintjén ugyanolyan reménytelennek tűnik, mint 1870-ben a Jevons számé.

Ha jól megfigyeljük, a fenti érvelésekben, amelyek a kulcs gyakorlati megfejthetetlenségéről szóltak, az elméleti érvek mellett igen *nagy szerepet kapott a technika korlátaiba vetett remény.*

Ezt a reményt (vagy reménytelenséget) azonban beárnyékolja, hogy például 1996-ban S. W. Golomb amerikai matematikus olyan egyszerű eljárást adott, amely *kézi* számolással 56 lépésben megadja a Jevons szám szorzattá bontását, és kimutatta, hogy $8\,616\,460\,799 = 96\,079 \cdot 89\,681$ (lásd [06]).

Végül a prímszámokra vonatkozó néhány egyszerű észrevételt említünk meg (bizonyítás nélkül), amelyekre építve megadható a Golomb-féle eljárás jelen szerző által javított változata, ami a Jevons-számhoz hasonlóan két, egymáshoz „közeli" prím szorzatának faktorizálására használható.

(I) *Minden* 3*-nál nagyobb* p *prímszám* $6k+1$ *vagy* $6k-1$ *alakú.*

Ha a természetes számokat az alábbi módon hat oszlopba rendezzük, (lásd 1. tábla), akkor (I) alapján az összes prímszám az 1. és az 5. oszlopban helyezkedik el; az 1. oszlopban a $6k+1$, míg az 5. oszlopban a $6k-1$ alakúak.

(I) alapján tehát a 3-nál nagyobb prímszámok keresésekor elegendő csupán a $6k \pm 1$ alakú természetes számokat vizsgálni. Az alábbi állítás az ún. komplementer prímszita annak szükséges és elegendő feltételét adja meg, hogy egy ilyen $6k \pm 1$ alakú szám összetett legyen.

(II) *(Komplementer prímszita)*

$N = 6k+1$ akkor és csak akkor összetett szám, ha alkalmas u, $v \geq 1$ egészekkel $k = 6uv + u + v$ vagy $k = 6uv - u - v$;

$N = 6k-1$ akkor és csak akkor összetett szám, ha alkalmas u, $v \geq 1$ egészekkel $k = 6uv - u + v$ vagy $k = 6uv + u - v$

(II) következményeként megkapjuk N kéttényezős felbontását is, azaz

(18) $N = 6k+1$ ebből $N = (6u+1)(6v+1)$ vagy $N = (6u-1)(6v-1)$,

(19) $N = 6k-1$ ebből $N = (6u+1)(6v-1)$ vagy $N = (6u-1)(6v+1)$.

Fontos megjegyezni, hogy mivel a komplementer prímszita nem feltételezi a $\sqrt{N}$-nél kisebb prímszámok ismeretét, így a (18), (19) felbontás megtalálására jól alkalmazható osztott (párhuzamos) algoritmus.

Most térjünk vissza a Jevons számhoz. S. W. Golomb [6] cikkében a Jevons-szám faktorizációja kapcsán bemutat egy általános eljárást a két prímtényezős szorzatok prímtényezőinek meghatározására. Ha J jelöli a szorzatot, akkor a módszer egyszerű alapötlete a következő: keressük a tényezőket $p = a+b$ és $q = a-b$ alakban, azaz próbáljuk meg a J számot két négyzetszám különbségeként előállítani:

(20) $$J = p \cdot q = a^2 - b^2 = (a+b)(a-b),$$

$6k+1$ ↓				$6k-1$ ↓	
			4	$\underline{5}$	6
$\underline{7}$	8	9	10	$\underline{11}$	12
$\underline{13}$	14	15	16	$\underline{17}$	18
$\underline{19}$	20	21	22	$\underline{23}$	24
25	26	27	28	$\underline{29}$	30
$\underline{31}$	32	33	34	35	36
$\underline{37}$	38	39	40	$\underline{41}$	42
$\underline{43}$	44	45	46	$\underline{47}$	48
49	50	51	52	$\underline{53}$	54
55	56	57	58	$\underline{59}$	60
$\underline{61}$	62	63	64	65	66
$\underline{67}$	68	69	70	$\underline{71}$	72
$\underline{73}$	74	75	76	77	78
$\underline{79}$	80	81	82	$\underline{83}$	84
85	86	87	88	$\underline{89}$	90
91	92	93	94	95	96
$\underline{97}$	98	99	100	$\underline{101}$	102
...					

1. tábla

ahol a és b természetes számok, p és q prímszámok.

A (20) összefüggéshez igen egyszerűen számolható algoritmust mutat be az a, b számok meghatározására. Az algoritmus lényeges lépései:

– Képezzük az $a_0=[\sqrt{J}]$ kezdőértéket.

– Legyen $a_k=a_0+k$, ahol $k=1, 2, 3, \ldots$

– Képezzük az a_k^2-J sorozatot, amíg teljes négyzetet kapunk, azaz

$$a_k^2-J=b_k^2. \tag{21}$$

Ekkor tehát a_k, b_k természetes számok, és így teljesül, hogy

$$J=(a_k+b_k)(a_k-b_k). \tag{22}$$

Az eljáráshoz mindössze egy memóriára van szükség, amelyben az aktuális a_k értéket tároljuk. Így akár egy zsebszámológép segítségével elvégezhetők a számítások. Igen meggyőző, hogy a Jevons által 1870-ben megoldhatatlannak tartott feladat, a $J=$

$= 8\,616\,460\,799$ szám faktorizációja, S. W. Golomb módszerével $k = 56$ lépésben célhoz vezet, és megadja az $a_{56} = 92\,880$, $b_{56} = 3199$ megoldást.[12]

Más megközelítésben láttuk, hogy (II) (a komplementer prímszita) szintén megadja bármely $6k \pm 1$ alakú összetett szám kéttényezős prímfelbontását,[13] amelynek alakja

$$J = (6u \pm 1)(6v \mp 1) \qquad (u, v = 1, 2, 3, \ldots). \tag{23}$$

Ha tehát feltételezzük, hogy J-nek két prímtényezője van (lásd (20)), akkor fennáll:

$$J = (a_k + b_k)(a_k - b_k) = (6u \pm 1)(6v \mp 1). \tag{24}$$

A két prímtényezőre vonatkozó feltétel miatt (24)-ből következik, hogy

$$a_k + b_k = 6u \pm 1, \quad \text{valamint} \quad a_k - b_k = 6v \mp 1. \tag{25}$$

A két egyenlet összeadásával adódik:

$$2a_k = 6u + 6v \Rightarrow a_k = 3(u + v). \tag{26}$$

(26)-ból következik, hogy a_k mindig osztható 3-mal. Ha tehát az a_0 kezdőértéket úgy választjuk, hogy

$$h \equiv [\sqrt{J}] \pmod 3) \Rightarrow a_0 = [\sqrt{J}] - h, \tag{27}$$

azaz a_0 osztható 3-mal, akkor a Golomb algoritmus szerint:

$$a_k = a_0 + k, \tag{28}$$

amely (27) és (28) alapján csak akkor teljesülhet, ha k is osztható 3-mal. Így a lépések számát harmadára csökkenthetjük, hiszen a $k = 1, 2, 3, \ldots$ lépések helyett csak a $k = 3, 6, 9, \ldots$ esetek vizsgálatára van szükség. A Jevons-szám esetén tehát:

$$\begin{aligned} &a_0 \xrightarrow{(25)} 92823 \qquad (h = 1) \\ &a_{19\cdot 3} = 92\,880, \end{aligned} \tag{29}$$

azaz 56 lépés helyett 19 lépésben előáll a megoldás. Ez az eredmény (és több másik, lásd pl. [1]) alapvetően megkérdőjelezi az RSA módszer elméleti biztonságát. A ma működő információs és kommunikációs rendszerek (internet, hálózati szoftverek, távközlési hálózatok, stb.) több mint 80%-ában RSA alapú információ-védelem van. Hogy mennyire nem alaptalan az aggodalom, azt mutatják az utóbbi 1–2 év jelentős (és sikeres) hacker támadásai, amelyeknek egy része a kulcsok megfejtésén alapult (lásd [2]).

Szeretném végül felhívni a figyelmet a matematikus és a kriptográfus gondolkodásmódbeli különbségére. Az, hogy egy adott típusú kulcsból összesen hány különböző létezik, csak akkor lenne meggyőző, ha a rejtjelfejtési támadások az úgynevezett *„teljes*

---

[12] $a_{56}^2 - b_{56}^2 = (a_{56} - b_{56})(a_{56} + b_{56}) = \underbrace{89\,681}_{p} \cdot \underbrace{96\,079}_{q} = 8\,616\,460 = J.$

[13] (II)-ből kiderül, hogy ha J-nek két prímtényezője van, akkor mindig $6k \pm 1$ alakú. A Jevons-szám esetében például: $J = 8\,616\,460\,799 = 6 \cdot 1\,436\,076\,800 - 1$.

kipróbálás" módszerét használnák, amelyre szinte sosem kerül sor. Ekkor lenne döntő érv az egyébként rohamosan fejlődő számítástechnikai kapacitások korlátait jellemző több évezredes és évmilliós érték.

Az érvelés ezen kívül azt is figyelmen kívül hagyja, hogy a hagyományos becslések egy-számítógépes modellekre épülnek és csak ezek sebesség és tároló kapacitását veszik figyelembe, míg a már ma is létező óriási számítógép hálózatok több száz, ezer vagy akár százezer gép kapacitását egyesítik. Ilyen internetes projektek már működnek, például a SETI program keretében, amely a földön kívüli élet kutatásával foglalkozik és a világűrből érkező óriási mennyiségű adat több százezer, internetre kapcsolt számítógépen történő osztott feldolgozásával működik. A globális hálózatok tehát egészen új technikai dimenziókat vezetnek be, amelyek szükségessé teszik azon módszerek újragondolását, amelyeknél a technikai korlátok is szerepet kapnak.

Irodalomjegyzék

[1] *Dan Boneh:* Twenty years of attack on the RSA cryptosystem. *Notices of the AMS,* February 1999, 203–213.

[2] *Dénes Tamás:* REJTJELFEJTÉS Trükkök, módszerek, megoldások. *Magyar Távközlés,* XI. évf. 4.szám, 2000. április.

[3] *T. Dénes:* Complementary Prime-Sieve *P.U.M.A.,* megjelenés alatt.

[4] *Dénes Tamás:* Titoktan, avagy kódtörő ABC (Segédeszköz és játék mellékletekkel). Kriptográfia Mindenkinek, megjelenés alatt.

[5] *Erdős Pál, Surányi János:* Válogatott fejezetek a számelméletből. *POLYGON,* Szeged, 1996.

[6] *S. W. Golomb:* On factoring Jevons' number. *CRYPTOLOGIA,* (vol. XX. no.3.) 1996.

[7] *W. S. Jevons:* The Principles of Science: A Treatise on Logic and Scientific Method. *Macmillan & Co., London,* 1873. Second edition 1877.

[8] *Kiss Elemér:* Matematikai kincsek Bolyai János kéziratos hagyatékából. *Typotex Kft.,* Budapest, 1999.

[9] *Sain Márton:* Nincs királyi út! (Matematikatörténet). *GONDOLAT,* Budapest, 1986.

[10] *Bruce Schechter:* Agyam nyitva áll! (Erdős Pál matematikai utazásai). *Vince Kiadó, Park Kiadó,* 1999.

[11] *Szalay Mihály:* Számelmélet. *Tankönyvkiadó,* Budapest, 1991.

[12] *W. Diffie, M. E. Hellman:* New directions in cryptography. *IEEE Trans.* 1976. IT-22.

[13] *R. L. Rivest, A. Shamir, L. Adleman:* A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM,* 1978. 21/2.

[14] *R. L. Rivest:* RSA chips (past/present/future); presented at Eurocrypt 84. Paris, France, 1984.

[15] *Jack Davies:* Pierre de Fermat (1601–1665) Mathematician and Jurist. Thesis for the Degree of Master of Philosophy, *Faculty of Arts, University of Liverpool,* 1996.

Dénes Tamás

Olimpiai megjegyzések I.

Októberi számunkban közöltük az idei Nemzetközi Matematikai Diákolimpia feladatainak megoldását. Ebben a cikkben az egyik feladatra visszatérve olyan további megoldást mutatunk, amelyik lényegesen különbözik az októberben közölttől, ugyanakkor tanulságos lehet mindazoknak, akik a jövőben országos vagy nemzetközi versenyeken szeretnének eredményesen részt venni. Ebben a megjegyzésben a 2. feladattal foglalkozunk.

A 2. feladat. *Bizonyítsuk be, hogy*

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

minden a, b, c pozitív valós számra.

A feladat első pillantásra ártalmatlan egyenlőtlenségnek tűnik, ami nem lehet nagyon nehéz... vagy mégis? A magyar csapat számára ez a feladat bizonyult a legnehezebbnek. Hat versenyzőnk együttvéve csupán 2 pontot szerzett meg a lehetséges 42-ből.

A megoldáshoz első lépésként kézenfekvő lehet behelyettesíteni a $x=\frac{bc}{a}$, $y=\frac{ca}{b}$, $z=\frac{ab}{c}$ változókat. Ezek szintén pozitív számok, a szorzatuk 1, és a behelyettesítés után az (1) egyenlőtlenség a következő, egyszerűbb alakot ölti:

(2) $$\frac{1}{\sqrt{1+8x}}+\frac{1}{\sqrt{1+8y}}+\frac{1}{\sqrt{1+8z}}\ge 1.$$

Azt is megállapíthatjuk, hogy az $x=y=z=1$ (azaz $a=b=c$) esetben egyenlőség áll fenn.

Hogyan tovább? Láthatjuk, hogy a feladat nehézsége abból fakad, hogy összegek négyzetgyökeit kell felülről becsülnünk, ehhez pedig meglehetősen kevés eszköz áll rendelkezésünkre. Ha alsó becslésre volna szükség, akkor egészen más lenne a helyzet. A három négyzetgyökös kifejezést kényelmesen tudjuk alulról becsülni például a számtani és mértani közepek közötti egyenlőtlenséggel. Közben persze vigyáznunk kell, hogy $x=y=z=1$ esetén mindig egyenlőség álljon:

(3) $$\sqrt{1+8x}\ge\sqrt{9\cdot\sqrt[9]{1\cdot x^8}}=3x^{4/9};\quad \sqrt{1+8y}\ge 3y^{4/9};\quad \sqrt{1+8z}\ge 3z^{4/9}.$$

Ezek alapján a három gyökös kifejezés szorzatát és összegét sem nehéz alulról megbecsülni.

Az olimpiai feladatok megoldása a KöMaL 2001/7. számának 389–394. oldalán olvasható.

De mi a helyzet a felső becsléssel? A felső becsléshez jó lenne megszabadulni a kellemetlen négyzetgyökjeltől. Ez pedig legegyszerűbben négyzetre emeléssel lehetséges. Szorozzuk be a (2) egyenlőtlenséget a nevezőkkel. Az így kapott egyenlőtlenségben csupán egyetlen négyzetgyökös kifejezést kell felülről becsülnünk, a jobb oldalt:

$$\sqrt{1+8y}\sqrt{1+8z}+\sqrt{1+8z}\sqrt{1+8x}+\sqrt{1+8x}\sqrt{1+8y}\geq\sqrt{1+8x}\sqrt{1+8y}\sqrt{1+8z}. \tag{4}$$

Most pedig vegyünk nagy levegőt, emeljük mindkét oldalt négyzetre, és rendezzük az egyenlőtlenséget! (Ne felejtsünk el xyz helyére 1-et írni.) A rendezés után a következő egyenlőtlenséget kapjuk:

$$4x+4y+4z+\sqrt{1+8x}\sqrt{1+8y}\sqrt{1+8z}\left(\sqrt{1+8x}+\sqrt{1+8y}+\sqrt{1+8z}\right)\geq 255. \tag{5}$$

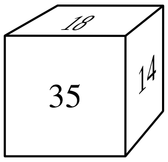
A rendezés során azt tapasztaljuk, hogy (4) jobb oldalának négyzetét „lenyelik” a baloldalon álló tagok négyzetei, csupán egy konstans marad.

A megoldás innen kezdve triviális: behelyettesítjük a (3) egyenlőtlenség-hármast és alkalmazzuk a számtani és mértani közép közötti egyenlőtlenséget.

Kós Géza

A 2000–2001. évi Arany Dániel Matematikai Tanulóverseny feladatai

KEZDŐK
Első forduló
Mindhárom kategória

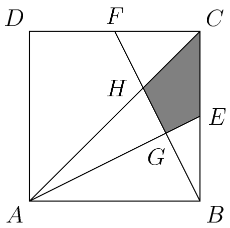


1. Egy kocka minden lapjára egy-egy pozitív egész számot írtunk. Ezek közül az ábrán feltüntettünk három számot. Tudjuk, hogy a szemközti lapokon levő számok összege egyenlő, és a fel nem tüntetett számok mindegyike prímszám. Melyek ezek a számok? (6 pont)

2. Az A halmazt a páros természetes számok négyzeténél eggyel nagyobb számok, a B halmazt a négyzetszámok háromszorosai alkotják. Határozza meg $A\cap B$-t! (Az A és B halmazok közös elemeiből álló halmazt jelöljük $A\cap B$-vel.) (6 pont)

3. Az $ABCD$ téglalap oldalai $AB=13$ cm és $BC=5$ cm. Az AB oldalegyenesen milyen távolságra lehet az A ponttól egy olyan pont, amelyből a DA és DC szakaszok egyenlő szögben látszanak? (Hány ilyen pont van?) (8 pont)

4. Igaz-e, hogy négy irracionális szám között mindig van három olyan, amelyek összege is irracionális szám? (10 pont)



5. Az $ABCD$ négyzet területe 60 cm^2. A BC és CD oldalak felezőpontjai E, illetve F. Az AE és BF szakaszok metszéspontja G, az AC és BF szakaszoké H. Mekkora a $CHGE$ négyszög területe? (10 pont)

Második (döntő) forduló

I. kategória: Szakközépiskolások

1. Bizonyítsa be, hogy az

$$1^{2001}+2^{2001}+\ldots+1999^{2001}+2000^{2001}$$

összeg osztható 2001-gyel!

2. Egy 10 cm befogójú egyenlő szárú derékszögű háromszögbe két olyan egyenlő sugarú kört írunk, amelyek érintik egymást és az átfogót, illetve egy-egy befogót. Mekkora a sugár pontos értéke?

3. Oldja meg a valós számok halmazán a következő egyenletet:

$$\left\{\frac{1}{2}x\right\}=\frac{1}{16}x+\frac{1}{32},$$

ahol $\{z\}$ a z valós szám törtrészét jelenti!

II. kategória: Általános matematika tantervű gimnáziumi tanulók

1. Azonos az 1. kategória 3. feladatával.

2. Melyek azok az $(x;y)$ egész számokból álló számpárok, amelyekre teljesül az alábbi egyenlőség:

$$5x^2+2y^2-2xy+4x-4y=5?$$

3. Az ABC háromszög területe t, beírt körének sugara r. Az A csúcsból induló két oldalt és a beírt kört kívülről érintő kör sugara r_a, a B csúcsból induló két oldalt és a beírt kört kívülről érintő kör sugara r_b, a C csúcsból induló két oldalt és a beírt kört kívülről érintő kör sugara r_c. A beírt kör és a másik három kör közös belső érintője egy-egy kis háromszöget vág le az ABC háromszögből, amelyek területe rendre t_a, t_b, t_c. Igazolja, hogy

$$\frac{t_a}{r_a}+\frac{t_b}{r_b}+\frac{t_c}{r_c}=\frac{t}{r}!$$

III. kategória: Speciális matematika tantervű gimnáziumi tanulók

1. Határozza meg az x^4-15x^2-18x kifejezés legkisebb értékét, ha x valós szám!

2. Azonos a 2. kategória 3. feladatával.

3. Mi lehet a pozitív egész értékű szigorúan monoton növekvő sorozat, ha $a_2=2$, továbbá relatív prím m és n esetén $a_{m\cdot n}=a_m\cdot a_n$?

HALADÓK

Első forduló

I. kategória: Szakközépiskolai tanulók

1. Határozza meg az összes olyan pozitív egész számot, amelyre

$$1!+2!+3!+\ldots+n!$$

egy egész szám négyzete! ($n!=1\cdot 2\cdot 3\cdot\ldots\cdot n$, azaz 1-től n-ig az egész számok szorzata, ha $n>1$, egész és $1!=1$.)

2. Bizonyítsuk be, hogy ha tetszőleges négy egymást követő pozitív egész szám szorzatához

a) 2000-et hozzáadunk,

b) 2001-et hozzáadunk,

akkor az eredmény sem prímszám, sem pedig négyzetszám nem lehet!

3. Legyen e az ABC háromszög S súlypontján áthaladó, a csúcsok egyikét sem tartalmazó egyenes. Bizonyítsuk be, hogy az e egyenes azonos oldalán lévő csúcsok e-től mért távolságainak összege megegyezik a harmadik csúcsnak az e egyenestől mért távolságával!

4. Határozza meg a k paraméter értékét úgy, hogy a

$$4x^4-(4k+13)x^2+(9k+9)=0$$

egyenlet valós gyökeit növekvő sorrendben felírva mindhárom szomszédos gyökpár különbsége ugyanannyi legyen!

5. Egy háromszög alapú gúla éleire olyan pozitív egész számokat írtunk, amelyekre igaz, hogy bármelyik csúcsba futó három élre írt számok összege ugyanakkora. Hányféle lehet a gúla éleire írt számok összege, ha az élekre írt számok szorzata 3600?

II. kategória: Általános tantervű gimnáziumi tanulók

1. Azonos az I. kategória 2. feladatával.

2. Azonos az I. kategória 3. feladatával.

3. Oldjuk meg a valós számok körében a következő egyenletet:

$$\frac{1+\sqrt{x+1}}{1-\sqrt{x+1}}+\frac{1-\sqrt{x+1}}{1+\sqrt{x+1}}-\frac{1}{\sqrt{x-1}}=\sqrt{x+1}\left(\frac{1+\sqrt{x+1}}{1-\sqrt{x+1}}-\frac{1-\sqrt{x+1}}{1+\sqrt{x+1}}\right)+\sqrt{x-1}.$$

4. Azonos az I. kategória 5. feladatával.

5. Melyek azok a nullától különböző a, b, c számjegyek, amelyekre minden pozitív egész n esetén teljesül, hogy az n-jegyű $\overline{aa\ldots a}$ szám négyzetének és az n-jegyű $\overline{bb\ldots b}$ számnak az összege egyenlő a $2n$-jegyű $\overline{cc\ldots c}$ számmal?

III. kategória: Speciális matematika tantervű gimnáziumi tanulók

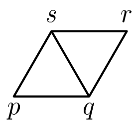
1. Bizonyítsuk be, hogy tetszőleges háromszögre

$$18Rr \le ab+ac+bc,$$

ahol R a köréírt, r a beírt kör sugara, továbbá az oldalak hossza a, b és c.

2. A 2000 egység oldalú ABC szabályos háromszöget az oldalakkal párhuzamos egyenesekkel egységoldalú szabályos háromszögekre daraboltuk. Az így keletkezett 2000^2 db kis háromszög minden csúcsa mellé egy-egy valós számot írtunk. Az A, B, C csúcsok mellé rendre az a, b, c számot írtuk, a többire pedig úgy írtunk számokat, hogy minden olyan rombuszban, amely két, közös oldallal rendelkező kis háromszögből áll, a szemköztes csúcsok mellé írt számok összege egyenlő.

Például:



$$p+r=q+s.$$

Határozzuk meg az eredeti ABC háromszög kerületére írt számok összegét!

3. Egy háromszög oldalainak mérőszáma egész szám. A háromszögbe írható kör sugara egységnyi hosszúságú. Határozzuk meg az oldalak hosszát!

4. Adott n pont a síkon úgy, hogy semelyik 3 sincs egy egyenesen. Bizonyítsuk be, hogy összeköthetők egy önmagát nem metsző zárt töröttvonallal!

Második forduló

I. kategória: Szakközépiskolai tanulók

1. Bizonyítsuk be, hogy a derékszögű háromszög területének mérőszáma megegyezik azon két szakasz hosszának szorzatával, amelyre a háromszögbe írható kör érintési pontja bontja az átfogót!

2. Oldjuk meg a valós számok halmazán a

$$2\sqrt{|2x-5|}-\sqrt[4]{(2x-5)(x-2)}-\sqrt{|x-2|}\le 0$$

egyenlőtlenséget!

3. Egy konvex négyszög egyik középvonala felezi a területét. Bizonyítsuk be, hogy a négyszög trapéz!

4. Bizonyítsa be, hogy nem létezik olyan konvex nyolcszög, amelynek szögei egyenlők, oldalai pedig valamilyen sorrendben 1, 2, 3, 4, 5, 6, 7 és 8 egység hosszúak!

II. kategória: Általános tantervű gimnáziumi tanulók

1. Tekintsük az $f(x)=x^2-\dfrac{a^2-1}{a}x-1$ $(a\neq 0)$ függvényt, ahol $x\in\mathbf{R}$. A függvény grafikonja az y tengelyt egy, az x tengelyt két pontban metszi. Bizonyítsuk be, hogy a három metszéspont által meghatározott háromszög területe nagyobb vagy egyenlő, mint 1.

2. Legyen X egy adott AB szakasz belső pontja. Vegyük fel a szakasz ugyanazon oldalára az APX és XQB szabályos háromszögeket! Legyen M és N az AQ, illetve BP szakasz felezőpontja!

Bizonyítsuk be, hogy XMN háromszög szabályos, továbbá határozzuk meg azt az X pontot, amelyre az MN szakasz hossza minimális!

3. Jelölje $s(n)$ az n szám 10-es számrendszerbeli alakjában a számjegyek szorzatát. Mennyi

$$s(2000)+s(2001)+s(2002)+\ldots+s(3000)?$$

4. Egy asztalon 2000 darab pénzérme van, mindegyik a „fej” oldalával felfelé fordítva.

Egy-egy alkalommal pontosan k darab érmét a másik oldalára fordíthatunk.

Bizonyítsuk be, hogy az adott művelet ismétlésével elérhető bármely adott k szám esetén $(1\le k\le 2000)$, hogy a 2000 érme „írás” oldalával felfelé legyen fordítva!

Harmadik (döntő) forduló

I. kategória: Szakközépiskolások

1. Az x, y, z egész számokra teljesül, hogy

$$(x-y)(y-z)(z-x)=x+y+z.$$

Bizonyítsuk be, hogy ekkor az $x+y+z$ összeg osztható 54-gyel!

2. Az ABC hegyesszögű háromszög AB oldalának tetszőleges belső pontja az X pont. Az AXC és CXB háromszögek beírt körének az AB egyenestől különböző közös külső érintője a CX szakaszt az Y pontban metszi.

Bizonyítsuk be, hogy a CY szakasz hossza független az X pont megválasztásától!

3. Bizonyítsuk be, hogy bármely 1-nél nagyobb négyzetszám 2-es számrendszerben felírt alakja legalább 2 darab 0 számjegyet tartalmaz!

II. kategória: Általános tantervű gimnáziumi tanulók

1. Igazoljuk, hogy ha az $\{a_n\}$ sorozat első tagja egy 0-tól különböző egész szám, akkor $a_{n+1}=a_n^2+a_n-1$ esetén $(n\in\mathbf{Z}^+)$ az $\dfrac{a_n}{a_k}$ tört nem egyszerűsíthető, ahol n és k egymástól különböző pozitív egész szám!

2. Legyen az ABC hegyesszögű háromszög A-ból induló magasságvonalának talppontja T. Az AT szakasz mint átmérő fölé írt körnek az AB, illetve AC oldallal való, A-tól különböző metszéspontja legyen D, illetve E. Bizonyítsuk be, hogy az ABC háromszög köré írt körének középpontja az ADE háromszög A-ból induló magasságvonalának egyenesén van!

3. Az a és b befogójú derékszögű háromszög beírt körének sugara r. Ha az átfogóhoz tartozó súlyvonal a beírt körből r hosszúságú húrt metsz ki, akkor mekkora az $\dfrac{a}{b}+\dfrac{b}{a}$ értéke?

III. kategória: Speciális matematika tantervű gimnáziumi tanulók

1. Az ABC hegyesszögű háromszög AB oldalának tetszőleges belső pontja az X pont. Az AXC és CXB háromszögek beírt körének az AB egyenestől különböző közös külső érintője a CX szakaszt az Y pontban metszi.

Mely X pont esetén lesz az AYB háromszög területe minimális?

2. Legyen a $H=\{n,n+1,n+2,\ldots,n+4096\}$, ahol n páratlan természetes szám. Bizonyítandó, hogy H elemei két diszjunkt A és B halmazba oszthatók úgy, hogy egyszerre teljesül a következő két feltétel:

$a)$ A elemszáma 2000,

$b)$ A és B elemei felírhatók egy-egy kör kerületére úgy, hogy a szomszédos számok relatív prímek.

3. 2001 darab különböző pozitív egész számról tudjuk, hogy a számok szorzatának pontosan 2000 darab különböző pozitív prímosztója van. Bizonyítsuk be, hogy a 2001 darab szám közül kiválasztható egy vagy több úgy, hogy azok szorzata négyzetszám legyen (vagy az egy kiválasztott szám már maga is négyzetszám)!

A 2000–2001. évi Országos Középiskolai Matematikai Tanulmányi Verseny feladatai

I. kategória: Szakközépiskolák

Első (iskolai) forduló

1. Az $A_1A_2A_3A_4A_5A_6$ síkbeli konvex hatszögben az A_1A_2, A_2A_3, A_3A_4, A_4A_5, A_5A_6, A_6A_1 oldalak felezőpontjai rendre a B_1, B_2, B_3, B_4, B_5, B_6 pontok.

Bizonyítsa be, hogy a

$$\overrightarrow{B_1B_4},\qquad \overrightarrow{B_3B_6},\qquad \overrightarrow{B_5B_2}$$

vektorok összege nullvektor! (9 pont)

2. Az $A=\overline{xyzu}$ és a $B=\overline{uzyx}$ tízes számrendszerben felírt, pontosan négyjegyű számok. Szorzatuknak pontosan az utolsó három számjegye 0. Határozza meg az összes ilyen tulajdonságú A és B számpárt! (14 pont)

3. Az
$$x^4-px^3+q=0$$
egyenletről tudjuk, hogy

a) a p és a q paraméterek pozitív prímszámok,

b) az egyenletnek van olyan gyöke, amelyik egész szám.

Határozza meg a p és a q paramétereket, valamint a lehetséges p, q értékekhez tartozó egyenlet összes egész gyökét! (14 pont)

4. Az $ABCD$ trapéz párhuzamos oldalai AB és CD. Az AC átló hossza 3 cm, a BD átló hossza 4 cm, továbbá
$$CAB\sphericalangle=2\cdot DBA\sphericalangle.$$
Számítsa ki a trapéz területét! (14 pont)

5. Oldja meg a valós számok halmazán a
$$18\sqrt{2x-3}-9\sqrt[4]{(2x-3)(x-2)}\ge 2\sqrt{x-2}$$
egyenlőtlenséget! (18 pont)

6. Egy $x\mapsto f(x)$ valós számokra értelmezett függvényről azt tudjuk, hogy minden valós x-re értelmezve van, és
$$2\cdot f(x)+f(1-x)=x^2.$$

a) Mennyi a függvény értéke az $x=5$ helyen?

b) Adja meg a hozzárendelést meghatározó $f(x)$ képletét! (19 pont)

Második forduló

1. Oldja meg a valós számok halmazán a

(1) $$\sqrt{7x+y}+\sqrt{x+y}=6,$$

(2) $$\sqrt{x+y}-y+x=2$$

egyenletrendszert! (15 pont)

2. Egy egyenlőszárú háromszögről tudjuk, hogy a köré írt kör területe kilencszerese a beírt kör területének. Számítsa ki a háromszög szögeit! (17 pont)

3. Hogyan kell a
$$3\ 000\ 003$$
tízes számrendszerben felírt hétjegyű számban (a legnagyobb helyiértéktől kiindulva) a harmadik és az ötödik helyen álló nullák közül legalább egyet úgy megváltoztatni, hogy a változtatás után kapott hétjegyű szám osztható legyen 13-mal? (17 pont)

4. Bizonyítsa be, hogy az
$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{1999}+\frac{1}{2000}+\frac{1}{2001}$$
összeg nem egész szám! (18 pont)

5. $ABCD$ egységnyi oldalú négyzet. Az AB oldalon az E pont egy belső pont, az AD oldalon az F pont ugyancsak belső pont.

Bizonyítsa be, hogy ha az AEF háromszög kerülete 2 kerületegység, akkor a $BEFC$ négyszög nem lehet húrnégyszög. (21 pont)

Harmadik (döntő) forduló

1. Milyen x, y, z valós számok elégítik ki a következő egyenletrendszert?

$$x^3+y^3+z^3=8,$$
$$x^2+y^2+z^2=22,$$
$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{z}{xy}=0.$$

2. Az $ABCD$ négyzet belsejében elhelyezkedő P pontnak az A, B, C csúcsoktól mért távolságai rendre 1, 2, 3 hosszúságegységek.

Számítsa ki az APB szög nagyságának pontos értékét!

3. Az $ABCD$ téglalap oldalai

$$AB=CD=5a \qquad \text{és} \qquad BC=DA=3a$$

hosszúságúak ($a>0$). Az oldalakra ugyanazon körüljárási irányban felmérjük az

$$x=AA_1=BB_1=CC_1=DD_1$$

szakaszokat úgy, hogy az $A_1B_1C_1D_1$ négyszöget az $ABCD$ téglalap tartalmazza.

a) Hogyan kell az x szakaszt megválasztani, hogy az $A_1B_1C_1D_1$ négyszög területe a lehető legkisebb legyen?

b) Legyen az $A_1B_1C_1D_1$ négyszög területe k^2 ($k^2\neq 0$). A k^2-től függően hány megoldása van a feladatnak?

II. kategória: Általános tantervű gimnáziumok

Első (iskolai) forduló

1. Közelítő értékek használata nélkül adjuk meg a

$$K=\operatorname{tg}47^\circ+\operatorname{tg}43^\circ-\operatorname{tg}2^\circ(\operatorname{tg}47^\circ-\operatorname{tg}43^\circ)$$

kifejezés pontos értékét! (7 pont)

2. Az $ABCD$ trapéz AB és CD oldalai párhuzamosak, kerületének hossza 2. A B és C csúcsokhoz tartozó külső szögfelezők a P pontban, az A és D csúcsokhoz tartozó külső szögfelezők pedig a Q pontban metszik egymást. Mekkora a PQ szakasz hossza? (7 pont)

3. Az A halmaz a $\dfrac{3n-4}{5n-3}$, a B halmaz a $\dfrac{4k-3}{7k-6}$ alakban előállított számokból áll, ahol n és k befutják a nemnegatív egész számok halmazát. Írjuk fel az A és B közös részének ($A\cap B$-nek) az elemeit. (7 pont)

4. Azok közül a téglatestek közül, amelyek térfogatának a mérőszáma kétszerese a felszínük mérőszámának, melyiknek a legkisebb a térfogata? (7 pont)

5. Az ABC egyenlő szárú háromszögben $AC = BC$. Jelölje a háromszög tetszőleges P belső pontjának az oldalegyenesektől mért távolságait x, y, z. Tudjuk, hogy $x^2 + y^2 + z^2$ a C csúcshoz tartozó CT magasság F felezőpontjára a legkisebb. Mekkorák a háromszög szögei? (7 pont)

Második forduló

1. Az M pozitív egészből az N pozitív egész úgy származtatható, hogy M jegyeit valamilyen más sorrendben írjuk fel (első jegyük nem lehet 0). Lehet-e mindkét szám 2-nek pozitív egész kitevőjű hatványa?

2. Egy háromszög két kisebbik oldalát, a-t és b-t érintő hozzáírt körök sugarai r_a és r_b. A háromszög területe $t = r_a \cdot r_b$. Mekkora a háromszög legnagyobb szöge?

3. Oldjuk meg a valós számok halmazán a következő egyenletet:

$$\left(5^x - 2^{x-2}\right)^2 + 2 \cdot \lg\left(5^x + 2^{x-2}\right) = x.$$

4. Bizonyítsuk be, hogy nincs olyan n pozitív egész, amelyre a valós számok halmazán értelmezett

$$f(x) = \cos x + \cos\left(x\sqrt{n^2+1}\right)$$

függvény periódikus.

Harmadik (döntő) forduló

1. Legyen a $H = \{1, 2, 3, \ldots, 2000, 2001\}$ halmaz 77 elemű részhalmazai közül azoknak a száma, amelyekben az elemek összege páros, S-sel egyenlő, és azoknak a száma, amelyekben az elemek összege páratlan, N-nel egyenlő. Melyik nagyobb: S vagy N? És mennyivel?

2. Egy hatoldalú szabályos gúla alaplapja és oldallapjai által bezárt szög egyenlő bármely két másodszomszédos oldallap síkjának a hajlásszögével. Mekkora szöget zárnak be a gúla oldalélei az alaplappal?

3. Bizonyítsuk be, hogy az $a_1, a_2, \ldots, a_n$ pozitív számokra teljesül az

$$\frac{a_1^2}{a_1+a_2} + \frac{a_2^2}{a_2+a_3} + \ldots + \frac{a_{n-1}^2}{a_{n-1}+a_n} + \frac{a_n^2}{a_n+a_1} \geq \frac{1}{2}(a_1 + a_2 + \ldots + a_n)$$

egyenlőtlenség.

III. kategória: Speciális matematika tantervű gimnáziumok

Első forduló

1. Legyenek x, y és z pozitív, 4-nél kisebb valós számok. Bizonyítsuk be, hogy az

$$\frac{1}{x}+\frac{1}{4-y},\qquad \frac{1}{y}+\frac{1}{4-z}\quad \text{és}\quad \frac{1}{z}+\frac{1}{4-x}$$

számok között van olyan, amely nagyobb vagy egyenlő 1-nél.

2. Oldjuk meg az egész számok körében az $5x^2-14y^2=11z^2$ egyenletet.

3. Melyek azok a háromszögek, amelyekben az egyik csúcsból induló szögfelező egyenesére szimmetrikusan helyezkedik el az ugyanonnan induló súlyvonal és magasságvonal?

4. Igazoljuk, hogy bármely $1\le m\le n$ esetén

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

osztható m-mel.

5. Határozzuk meg a legkisebb olyan c valós számot, amely rendelkezik az alábbi tulajdonsággal: Bármely háromszög kerületén található két olyan pont, amelyek a háromszög kerületét felezik, és a távolságuk nem nagyobb a kerület c-szeresénél.

Második (döntő) forduló

1. Legyen c pozitív egész, és jelölje c_1, c_3, c_7, illetve c_9 rendre a c azon pozitív osztóinak számát, amelyek utolsó számjegye (tízes számrendszerben) 1, 3, 7, illetve 9. Bizonyítsuk be, hogy $c_1+c_9\ge c_3+c_7$.

2. Adottak a síkon a k_1 és k_2 körök, valamint a P pont. Szerkesztendő olyan, a P-n átmenő e egyenes, amely a k_i köröket ($i=1,2$) az A_i és B_i pontokban metszi úgy, hogy a k_i körvonalak alkalmas C_i pontjaira $A_1C_1=A_2C_2=B_1C_1=B_2C_2$ teljesül. (Nem szükséges annak diszkutálása, hány ilyen e egyenes létezik, illetve létezik-e egyáltalán ilyen e egyenes.)

3. Adott $k+m$ darab különböző, 1-nél nagyobb egész szám, $a_1,\ldots,a_k$, $b_1,\ldots,b_m$, ahol mindegyik a_i páros sok, mindegyik b_j pedig páratlan sok (nem feltétlenül különböző) prímszám szorzata. Hányféleképpen lehet a $k+m$ darab szám közül néhányat (akár egyet sem, akár az összeset) kiválasztani úgy, hogy bármelyik b_j-nek ($j=1,2,\ldots,m$) a kiválasztott számok között páros sok osztója legyen?

KENGURU

Helyesbítés

Októberi számunkban a KENGURU verseny időpontja tévesen jelent meg. A helyes időpont 2002. március 21. 10 órától 11^{15}-ig. Olvasóinktól elnézést kérünk.

Felvételi előkészítő feladatsor

Kokits Zsigmond matematikus, egyetemi docens emlékére

1. Oldjuk meg a következő egyenleteket a valós számok halmazán.

a) $\dfrac{x-3}{x-2}+\dfrac{10}{x+2}=\dfrac{44}{4-x^2}$; *b)* $\dfrac{x-13}{x-2}+\dfrac{10}{x+2}=\dfrac{44}{4-x^2}$;

c) $\dfrac{x-4}{x-2}+\dfrac{10}{x+2}=\dfrac{44}{4-x^2}$; *d)* $\dfrac{x-8}{x-2}+\dfrac{10}{x+2}=\dfrac{44}{4-x^2}$.

2. Egy téglalap egyik oldalának hossza a másik oldal hosszának négyszerese. Határozzuk meg a téglalap területe és a téglalap szögfelezői által határolt négyszög területének arányát, valamint a téglalap átlója és a szögfelelzők által határolt négyszög oldalainak arányát.

3. Határozzuk meg az $f(x)=\dfrac{3x^3+11x-34}{x^2+4x-12}$ kifejezés legkisebb és legnagyobb értékét a $[-4;-1]$ intervallumon.

4. Oldjuk meg a valós számok halmazán a $3\operatorname{tg}\left(x+\dfrac{3\pi}{2}\right)=\operatorname{tg}2x$ egyenletet.

5. Igazoljuk, hogy

$$S_n=4\cdot 6+5\cdot 13+\ldots+(n+3)(7n-1)=\frac{n}{6}(14n^2+81n+49),$$

ahol n tetszőleges pozitív egész szám.

6. *a)* Az $x^2+px+q=0$ $(p,\,q\in\mathbf{R})$ egyenlet diszkriminánsa $D\geq 0$, az egyenlet gyökei x_1 és x_2. Igazoljuk, hogy $(x_1-x_2)^2=D$.

b) Az $x^2-2ax+2a^2-3a=0$ $(a\in\mathbf{R})$ egyenlet valós gyökei x_1 és x_2. Az a paraméter mely értékeinél veszi fel $(x_1-x_2)^2$ a legnagyobb értékét? Mennyi ez a legnagyobb érték?

7. Az ABC háromszög csúcsainak koordinátái: $A(0;16)$, $B(0;0)$, $C(3;0)$. Határozzuk meg annak az egyenesnek az egyenletét, amely átmegy a $P_0(-6;0)$ ponton, és két egyenlő területű részre osztja az ABC háromszög területét.

8. *a)* Igazoljuk, hogy ha $xy+yz+zx=1$ $(x,\,y,\,z\in\mathbf{R})$, akkor $x^2+y^2+z^2\geq 1$.

b) Tekintsük azokat a téglatesteket, amelyeknek a testátlója 2 egység hosszú. E téglatestek közül melyiknek legnagyobb a felszíne, és mennyi ez a legnagyobb felszín?

Rábai Imre

Megoldásvázlatok, eredmények a 2001/7. sz. feladataihoz

1. Jelölje a derékszögű háromszög két befogóját a és b, a kerületét $2s$. Ekkor $ab=86{,}4$, $s=\dfrac{T}{\varrho}=18$, $2s=36$.

Az érintő szakaszok egyenlősége miatt az átfogó $a+b-4{,}8$, tehát $2a+2b-4{,}8=3{,}6$, $a+b=20{,}4$. Az egyenletrendszer megoldása $a=14{,}4$, $b=6$ egység ($a\geq b$), az átfogó $c=20{,}4-4{,}8=15{,}6$ egység.

2. Az egyenlet diszkriminánsa

$$D=4(b+c)^2-4\cdot 2\cdot(ab+bc+ca-a^2)=4\left((a-b)^2+(a-c)^2\right)\geq 0$$

minden a, b, $c\in\mathbf{R}$ esetén, tehát mindig van valós megoldás. A két megoldás pontosan akkor egyenlő, ha $D=0$, azaz ha $a=b=c$. Ekkor $x_1=x_2=a$.

3. Jelölje az átlót e, a szárat c, a trapéz köré írt kör sugarát r. Ekkor $e\cos\alpha=\dfrac{a+b}{2}$, $c=2r\sin\alpha$. Mivel $c^2=e^2+a^2-2ea\cos\alpha$, azért $c^2=e^2-ab$, tehát

$$c^2=\left(\frac{a+b}{2\cos\alpha}\right)^2-ab=\frac{a^2+b^2+2ab-4ab\cos^2\alpha}{4\cos^2\alpha}=\frac{a^2+b^2-2ab\cos 2\alpha}{4\cos^2\alpha}.$$

A trapéz köré írt kör sugara

$$r=\frac{c}{2\sin\alpha}=\frac{\sqrt{a^2+b^2-2ab\cos 2\alpha}}{2\sin 2\alpha}.$$

4. A feltétel szerint $a_1=q+3$ és $S_n=35$. Ha $q=1$, akkor $a_1=4$, tehát $a_n=4$, így $a_1\cdot a_n=16\neq 100$, tehát $q\neq 1$. Ekkor $35=a_1\cdot\dfrac{q^n-1}{q-1}$ és $a_1^2\cdot q^{n-1}=100$, tehát $q-1=a_1-4$ és $a_1\cdot q^n=\dfrac{100}{a_1}(a_1-3)$; ezekből $35(a_1-4)=\dfrac{100}{a_1}(a_1-3)-a_1$,

$$36a_1^2-240a_1+300=0,\qquad a_1=5\quad\text{vagy}\quad a_1=\frac{5}{3}.$$

Ha $a_1=5$, akkor $q=2$ és $n=3$, hiszen $25\cdot 2^{n-1}=25\cdot 4$, ha $a_1=\dfrac{5}{3}$, akkor $q=-\dfrac{4}{3}$, és nincs megfelelő n, hiszen $\dfrac{25}{9}\left(-\dfrac{4}{3}\right)^{n-1}=100$ egyetlen n-re sem teljesül.

5. A P ponton áthaladó $x=5$ egyenletű egyenes a feltételnek nem felel meg. Minden ettől különböző, a P ponton áthaladó egyenes egyenlete $y-3=m(x-5)$ alakban is írható. Ha $m=-\dfrac{3}{2}$, akkor az egyenes párhuzamos az adott egyenesekkel, így $m\neq-\dfrac{3}{2}$. A keresett egyenes az első egyenest az $x_1=\dfrac{10+10m}{3+2m}$, a második egyenest az $x_2=\dfrac{5+10m}{3+2m}$ abszcisszájú pontban metszi. A feltétel szerint $|x_1-x_2|=1$, tehát $\dfrac{5}{|3+2m|}=1$, ahonnan $m=1$ vagy $m=-4$. A feltételnek két egyenes felel meg, ezek egyenlete: $x-y=2$, illetve $4x+y=23$.

(A feladat más úton is megoldható. Hogyan?)

6. Teljes négyzetté alakítással

$$(x-2\sin xy)^2+4\cos^2 xy=0, \tag{1}$$

hiszen $4-4\sin^2 xy=4\cos^2 xy$.

Az (1) egyenlet pontosan akkor teljesül, ha $\cos xy=0$ és $x=2\sin xy$.

Ha $xy=\frac{\pi}{2}+2n\pi$, $n\in\mathbf{Z}$, akkor $\sin xy=1$, tehát $x=2$ és $y=\frac{\pi}{4}+n\pi$, $n\in\mathbf{Z}$;

ha $xy=\frac{3\pi}{2}+2k\pi$, $k\in\mathbf{Z}$, akkor $\sin xy=-1$, tehát $x=-2$ és $y=-\frac{3\pi}{4}+k\pi$, $k\in\mathbf{Z}$.

(A feladat más módokon is megoldható. Hogyan?)

7. Legyen a keresett távolság x, a gúla magasságát jelölje m. A hasonló testek térfogatának arányára vonatkozó tétel alkalmazásával $x=\frac{m}{\sqrt[3]{2}}$. A gúla akkor létezik, ha $c>\frac{1}{2}\sqrt{a^2+b^2}$, azaz ha $4c^2>a^2+b^2$. Az átló tengelymetszet felhasználásával $m^2=c^2-\frac{a^2+b^2}{4}$, $m=\frac{1}{2}\sqrt{4c^2-a^2-b^2}$. A szóban forgó távolság $x=\frac{1}{2\sqrt[3]{2}}\cdot\sqrt{4c^2-a^2-b^2}$, a síkmetszet területe $t=\frac{ab}{\sqrt[3]{4}}$.

8. Az eredeti feladatban az egyenlet gyökeire helyesen: $x_1^2+x_2^2=\frac{9}{2}$.

Mivel a gyökök valósak, azért $p^2+4q\ge 0$, $x_1+x_2=-p$, $x_1x_2=-q$, így

$$\frac{9}{2}=x_1^2+x_2^2=(x_1+x_2)^2-2x_1x_2=p^2+2q, \qquad \text{azaz} \qquad 4q=9-2p^2, \qquad q=\frac{9}{4}-\frac{1}{2}p^2.$$

Az $f(p)=q-p=\frac{9}{4}-\frac{1}{2}p^2-p=\frac{11}{4}-\frac{1}{2}(p+1)^2$ kifejezés értékkészletét a $-3\le p\le 3$ intervallumban keressük, mivel $p^2+4q=p^2+9-2p^2\le 0$ pontosan akkor, ha $p^2\le 9$. Így $-2\le p+1\le 4$, amiből $0\le (p+1)^2\le 16$, ezért $-8\le -\frac{1}{2}(p+1)^2\le 0$, tehát $-\frac{21}{4}\le f(p)\le \frac{11}{4}$.

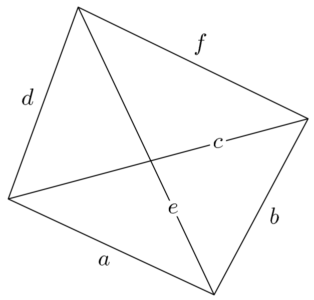
Rábai Imre

Matematika gyakorlatok megoldása

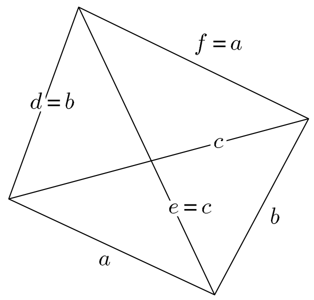
C. 633. *Egy tetraéder lapjainak területe egyenlő, továbbá a háromszög lapok beírható köreinek sugarai is egyenlőek. Mutassuk meg, hogy a tetraéder lapjai egybevágóak.*

Megoldás. Jelöljük a tetraéder éleit a, b, c, d, e és f-fel az *1. ábra* szerint. Egy háromszög t területe, s kerülete és beírt körének r sugara között fennáll a következő összefüggés: $t=\frac{rs}{2}$.

Tudjuk, hogy a tetraéder lapjainak területe és beírt köreinek sugara egyenlő. Az előző egyenlőségből következik, hogy akkor a lapok kerületei is egyenlők.



1. ábra



2. ábra

Írjuk fel a négy háromszöglap kerületének egyenlőségét. $a+b+c=a+d+e$; ebből következik, hogy

(1) $$b+c=d+e.$$

$b+f+e=f+d+c$, ebből

(2) $$b+e=d+c.$$

(1) és (2)-ből $d+e-c=d+c-e$, ebből pedig $2e=2c$, vagyis $e=c$, de akkor (2)-ből $b=d$.

Végül $a+b+c=d+f+c$, és mivel $b=d$, innen $a=f$, így az előbbi egyenlőségek miatt a tetraéder élei a *2. ábra* szerintiek: a, b, c, $d=b$, $e=c$, $f=a$, vagyis a határoló háromszögek mindegyikének az oldalai a, b és c, a lapok valóban egybevágók.

131 dolgozat érkezett. 5 pontos 108, 4 pontos 5, 3 pontos 10, 2 pontos 3, 1 pontos 3, 0 pontos 2.

Matematika feladatok megoldása

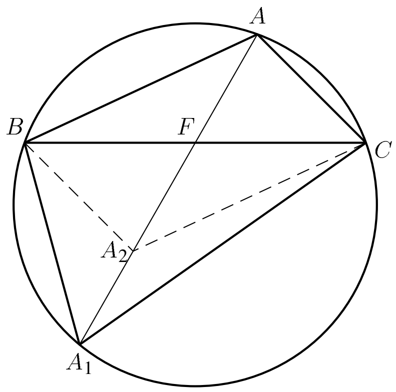
B. 3418. *Az ABC háromszögben az A, B, illetve C csúcsokból induló súlyvonalak a háromszög köré írt kört rendre az A_1, B_1, illetve C_1 pontokban metszik. Bizonyítsuk be, hogy $t_{A_1BC}+t_{B_1CA}+t_{C_1AB}\ge t_{ABC}$.*

(*5 pont*) Javasolta: *Varga István,* Békéscsaba

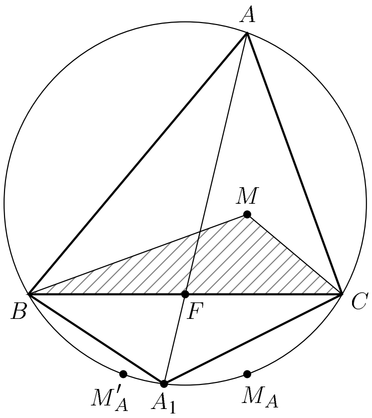
I. megoldás. Az állítást először a nem hegyesszögű háromszögekre látjuk be. Legyen például $BAC\sphericalangle \ge 90°$. Ekkor A-nak a BC oldal F felezőpontjára való A_2 tükörképe a körülírt körre vagy annak belsejébe esik (*1. ábra*). Így az A_1BC háromszög tartalmazza az ABC-vel egybevágó A_2BC háromszöget, ezért a területe legalább t_{ABC}.

Ha ABC hegyesszögű, akkor az M magasságpont a belsejébe esik, és – mint ismeretes – bármelyik oldalra vagy oldalfelező pontra való tükörképe a körülírt körön van. Jelölje az M tükörképét a BC-re M_A, az F-re pedig M'_A (*2. ábra*). Mivel az AF egyenes elválasztja az M_A, M'_A pontokat, azért A_1 az $M_AM'_A$ (rövidebb) körívre esik. Így

A_1-nek a BC-től való távolsága legalább akkora, mint M_A-nak (illetve M'_A-nak) a távolsága BC-től. Ezért az MBC háromszög területe legfeljebb akkora, mint az A_1BC háromszögé, és pontosan akkor egyenlők, ha $M_A = M'_A$, azaz $AB = AC$.



1. ábra



2. ábra

Hasonlóan kapjuk, hogy $T_{BMA} \leq T_{BC_1A}$ és $T_{AMC} \leq T_{AB_1C}$. A három egyenlőtlenséget összegezve a bizonyítandó állítást kapjuk, és az is látszik, hogy csak szabályos háromszögre van egyenlőség.

Nagy Ádám (Budapest, Szent István Gimn., 12. o.t.)

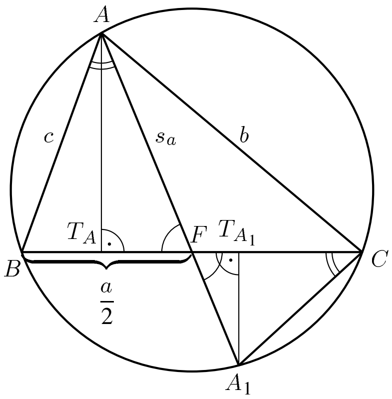
II. megoldás. Jelöljük a háromszög oldalait a, b, c-vel, súlyvonalait pedig s_a, s_b, s_c-vel. Legyen a BC oldal felezőpontja F, az A-ból, illetve A_1-ből a BC egyenesre bocsájtott merőlegesek talppontjai pedig T_A, illetve T_{A_1}.

Az AFB és a CFA_1 háromszögek hasonlóak, mert F-nél lévő szögük csúcsszögek, továbbá $FCA_1\sphericalangle = BAF\sphericalangle$, mert azonos íven nyugvó kerületi szögek (*3. ábra*). Ezért megfelelő oldalaik aránya megegyezik, tehát

$$\frac{A_1F}{FC} = \frac{FB}{AF},$$

ahonnan

$$A_1F = \frac{FC \cdot FB}{AF} = \frac{\frac{a}{2} \cdot \frac{a}{2}}{s_a} = \frac{a^2}{4s_a}.$$



3. ábra

Az AT_AF és $A_1T_{A_1}F$ derékszögű háromszögek is hasonlóak, hiszen megfelelő szögeik egyenlőek. Így $\frac{A_1T_{A_1}}{A_1F}=\frac{AT_A}{AF}$, azaz

$$(1) \qquad A_1T_{A_1}=\frac{A_1F\cdot AT_A}{AF}=\frac{a^2}{4s_a^2}\cdot AT_A.$$

Az AT_A, illetve $A_1T_{A_1}$ szakaszok az ABC, illetve az A_1BC háromszögek BC oldalhoz tartozó magasságai, ezért az ismert területképlet szerint

$$AT_A=\frac{2t_{ABC}}{a}.$$

Ezt behelyettesítve (1)-be és ismét alkalmazva a területképletet, kapjuk, hogy

$$t_{A_1BC}=\frac{a\cdot A_1T_{A_1}}{2}=\frac{a}{2}\cdot\frac{a^2}{4s_a^2}\cdot\frac{2t_{ABC}}{a}=\frac{a^2\cdot t_{ABC}}{4s_a^2}.$$

Felhasználva az ismert $4s_a^2=2b^2+2c^2-a^2$ összefüggést, innen

$$t_{A_1BC}=\frac{a^2\cdot t_{ABC}}{2b^2+2c^2-a^2}.$$

Ugyanígy felírható t_{B_1CA} és t_{C_1AB} is. A bizonyítandó állítás tehát

$$\frac{a^2\cdot t_{ABC}}{2b^2+2c^2-a^2}+\frac{b^2\cdot t_{ABC}}{2c^2+2a^2-b^2}+\frac{c^2\cdot t_{ABC}}{2a^2+2b^2-c^2}\ge t_{ABC}.$$

Mivel $t_{ABC}>0$, azért azt kell megmutatnunk, hogy

$$S=\frac{a^2}{2b^2+2c^2-a^2}+\frac{b^2}{2c^2+2a^2-b^2}+\frac{c^2}{2a^2+2b^2-c^2}\ge 1.$$

A számtani és a harmonikus közepek közti egyenlőtlenség szerint ha x, y, z pozitív számok, akkor

$$x+y+z\ge\frac{9}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

Az egyenlőtlenséget az $x=\frac{a^2}{2b^2+2c^2-a^2}$, $y=\frac{b^2}{2c^2+2a^2-b^2}$ és $z=\frac{c^2}{2a^2+2b^2-c^2}$ számokra felírva, ezután felhasználva, hogy egy pozitív számnak és a reciprokának az összege legalább 2, kapjuk, hogy

$$S\ge\frac{9}{\frac{2b^2+2c^2-a^2}{a^2}+\frac{2c^2+2a^2-b^2}{b^2}+\frac{2a^2+2b^2-c^2}{c^2}}=$$
$$=\frac{9}{2\left(\frac{b^2}{a^2}+\frac{a^2}{b^2}\right)+2\left(\frac{c^2}{b^2}+\frac{b^2}{c^2}\right)+2\left(\frac{a^2}{c^2}+\frac{c^2}{a^2}\right)-3}\ge\frac{9}{2\cdot 2+2\cdot 2+2\cdot 2-3}=1.$$

Ezzel a feladat állítását beláttuk, s bizonyításunkból az is látszik, hogy egyenlőség akkor és csak akkor van, ha $a=b=c$, azaz ha ABC szabályos háromszög.

Balka Richárd (Sárvár, Tinódi S. Gimn., 12. o.t.) dolgozata alapján

54 dolgozat érkezett. 5 pontot kapott Babos Attila, Balka Richárd, Béky Bence, Bóka Gergely, Herczegh Attila, Jelitai Kálmán, Kármán Péter, Kiss-Tóth Christian, Kocsis Albert Tihamér, Kőrizs András, Körtvélyessy Csaba, Maga Péter, Nagy 444 Zoltán, Pogátsa Attila, Reiss Attila, Somogyi Dávid, Szekeres Balázs, Ta Vinh Thong, Tábor Áron, Takács Gergő, Tóth 370 Ágnes, Tran Thanh Long és Zalán Péter. 4 pontos 14, 3 pontos 3, 2 pontos 2, 1 pontos 3, 0 pontos 6 dolgozat. Nem versenyszerű 3.

B. 3467. *Keressük meg az $x(1+x)(3-x)$ kifejezés maximumát a pozitív számok körében a differenciálszámítás alkalmazása nélkül.*

(*4 pont*)

I. megoldás. Jelölje M a keresett maximumot. Ekkor a KöMaL 2001/5. szám 270–281. oldalán látottak szerint M az a legnagyobb pozitív szám, amelyre az $x(x+1)(3-x)=M$ egyenletnek egynél több megoldása van (*ábra*).

Az egyenlet $x^3-2x^2-3x+M=0$ alakba írható. Ebben a formában a Cardano-formula nem alkalmazható, ehhez először a másodfokú tagot ki kell küszöbölnünk. Ezt a szokásos $t=x-\dfrac{2}{3}$ helyettesítéssel érhetjük el:

$$x^3-2x^2-3x+M=\left(x-\frac{2}{3}\right)^3-\frac{13}{3}\left(x-\frac{2}{3}\right)+M-\frac{70}{27},$$

így a keresett M számra a

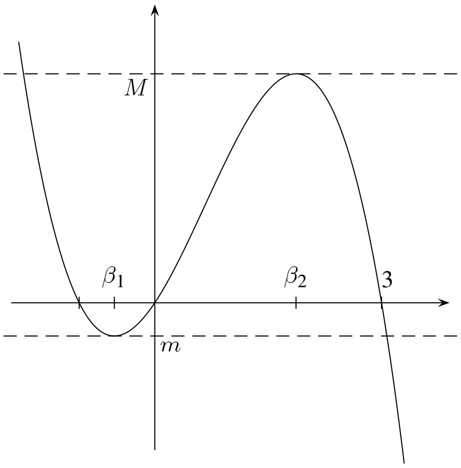
$$t^3-\frac{13}{3}t+M-\frac{70}{27}=0$$

egyenletnek kétszeres gyöke van. Az ismert feltétel,

$$\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3=0$$

most $q=M-\dfrac{70}{27}$ és $p=-\dfrac{13}{3}$ helyettesítésével

$$\left(\frac{M-\frac{70}{27}}{2}\right)^2=\left(\frac{13}{9}\right)^3.$$



Ez két számra teljesül, ezek $M=\dfrac{70+26\cdot\sqrt{13}}{27}$ és $m=\dfrac{70-26\cdot\sqrt{13}}{27}$. $M>0>m$, és a módszerünkkel kapott feltétel (az $x^3-2x^2-3x+M=0$ egyenletnek kétszeres gyöke van) nemcsak az $x(1+x)(3-x)$ lokális maximumára, M-re, hanem a negatív lokális minimumra, m-re is teljesül (*ábra*).

Az $x(1+x)(3-x)$ kifejezés maximuma tehát a pozitív számok halmazán

$$M=\frac{70+26\cdot\sqrt{13}}{27}.$$

Szekeres Balázs (Szolnok, Verseghy Ferenc Gimn., 10. o.t.)

Megjegyzések. 1. A fenti okoskodásból nem derül ki – a feladat ezt nem is kérdezte –, hogy az x milyen értékére kapjuk ezt a maximumot.

2. A kétszeres gyök meglétét feltételezve az x^3-2x^2-3x+M polinom $(x-\alpha)(x-\beta)^2$ gyöktényezős alakja is elvezet a megoldáshoz.

A gyökök és együtthatók közötti összefüggések szerint ugyanis

(1) $$\alpha+2\beta=2 \qquad \text{és}$$

(2) $$\beta^2+2\alpha\beta=-3.$$

Az (1) egyenletből α-t kifejezve a

$$3\beta^2-4\beta-3=0$$

egyenletet kapjuk, ennek megoldásai

$$\beta_1=\frac{2-\sqrt{13}}{3}<0<\beta_2=\frac{2+\sqrt{13}}{3}.$$

Ismét megkaptuk az $f(x)=x(1+x)(3-x)$ függvény lokális minimumát is, ez $f(\beta_1)$ (ld. *ábra*). A maximum értéke

$$f(\beta_2)=f\left(\frac{2+\sqrt{13}}{3}\right)=\frac{70+26\cdot\sqrt{13}}{27}\approx 6{,}0646.$$

3. A májusi számunkban közölt cikk bemutatja, hogy az ott vizsgált $x\cdot\frac{8+x}{2}\cdot\frac{8-x}{2}$ függvény maximuma hogyan határozható meg a számtani és mértani közepek közti egyenlőtlenség felhasználásával is. Ez akkor a tényezők szimmetriáján múlott, a függvény négyzete olyan háromtényezős szorzatként volt felírható, ahol a tényezők számtani közepe már nem függött az x-től. Ez a trükk most látszólag nem működik. Tanulságos megnézni, hogyan alkalmazható mégis, miközben ez I. megoldás t változója új szerepben tűnik fel.

II. megoldás. A $t=x-\frac{2}{3}$ változó bevezetésével az I. megoldásban látottak szerint $x(1+x)(3-x)=-t^3+\frac{13}{3}t+\frac{70}{27}$, azaz a vizsgált szorzat maximumához elegendő megtalálni a $g(t)=t\left(\frac{13}{3}-t^2\right)$ maximumát, a keresett érték ennél $\frac{70}{27}$-del nagyobb. Az $x>0$ feltétel most $t>-\frac{2}{3}$-ot jelent, de ha $0>t>-\frac{2}{3}$, akkor $g(t)<0=g(0)$, tehát a maximumot elegendő a $t\ge 0$ halmazon keresnünk, és $\max g(t)\ge 0$.

Most már minden további nélkül alkalmazható a májusi szám cikkében látott elemi módszer, $g(t)$ a $t\ge 0$ halmazon pontosan akkor maximális, ha

$$2g^2(t)=2t^2\left(\frac{13}{3}-t^2\right)\left(\frac{13}{3}-t^2\right)$$

maximális. A pozitív tényezők összege $\frac{26}{3}$, így a számtani és mértani közepek közti egyenlőtlenség szerint

$$2g^2(t) \le \left(\frac{26}{9}\right)^3,$$

azaz $g(t) \le \frac{\sqrt{26^3}}{27 \cdot \sqrt{2}} = \frac{26}{27} \cdot \sqrt{13}$.

Egyenlőség pontosan akkor teljesül, ha $2t^2 = \frac{13}{3} - t^2$, azaz $t = \frac{\sqrt{13}}{3}$.

Az $x(1+x)(3-x)$ szorzat maximuma tehát a pozitív számok halmazán $\frac{26}{27} \cdot \sqrt{13} + \frac{70}{27}$, és pontosan akkor van egyenlőség, ha $x = \frac{\sqrt{13}}{3} + \frac{2}{3}$.

Ambrus Gergely (Szeged, Radnóti M. Gimn., 12. o.t.)

Megjegyzés. Többen kísérleteztek a gyakran hatásos „határozatlan együttható” módszerével, ez azonban közvetlenül nem vezet eredményre. A módszer lényege az, hogy valamelyik tényezőt megkíséreljük egy olyan – pozitív – c szorzóval kiegészíteni, hogy az így módosított három tényező összegéből éppen kiessen a változó, a számtani és mértani közepek közti egyenlőtlenség felső becslésében konstans szerepeljen.

Az első két tényezőnél csak a triviális $c=1$ lehetséges, a harmadik tényezőre ugyan $c=2$ választással

$$x + (1+x) + \mathbf{2}(3-x) = 7,$$

tehát a számtani és mértani közepek közti egyenlőtlenség szerint most

$$x(1+x)(6-2x) \le \left(\frac{7}{3}\right)^3,$$

és így a vizsgált szorzatra

$$x(1+x)(3-x) \le \frac{1}{2}\left(\frac{7}{3}\right)^3$$

adódik, de ebben az egyenlőtlenségben az első két tényező x és $1+x$ **nem lehetnek egyenlők**, a felhasznált egyenlőtlenségben tehát nem állhat egyenlőség, a kapott felső becslés nem a maximum, hanem csupán egy felső korlát.

A fenti módszer finomítása azonban célhoz vezet.

III. megoldás. A keresett c együtthatót bontsuk tovább két határozatlan tényező, u és v szorzatára, vizsgáljuk az $u \cdot v \cdot f(x) = (ux) \cdot (v(1+x)) \cdot (3-x)$ szorzat három tényezőjét. Feltételeink a következők:

i) u és v pozitív számok;

ii) a tényezők összege, $ux + v(1+x) + (3-x)$ állandó;

iii) az $ux = v(1+x) = 3-x$ egyenletrendszernek létezik pozitív megoldása. (A szorzatra kapott felső becslésben tehát elérhető az egyenlőség.)

ii)-ből $u+v=1$. Ezt *iii*)-ba helyettesítve az

$$ux = (1-u)(1+x)$$

egyenlet megoldása $x=\dfrac{u-1}{1-2u}$, az $ux=3-x$ egyenleté pedig $x=\dfrac{3}{1+u}$.

Ha ez a két megoldás egyenlő, akkor innen u-ra az

$$u^2+6u-4=0$$

egyenlet adódik, ennek pozitív gyöke $u=\sqrt{13}-3$. (Ekkor az x-re kapott mindkét tört értelmes.)

Ha most $v=1-u=4-\sqrt{13}$, akkor láthatóan v is pozitív, $ux+v(1+x)+(3-x)=$ $=3+v$, és van olyan x, mégpedig $\dfrac{3}{1+u}=\dfrac{2+\sqrt{13}}{3}$, hogy az

$$(ux)\cdot(v(1+x))\cdot(3-x)$$

szorzat tényezői egyenlő pozitív számok.

Most már alkalmazható a számtani és mértani közepek közti egyenlőtlenség,

$$\sqrt[3]{u\cdot v\cdot f(x)}\le\frac{3+v}{3},$$

és az egyenlőség lehetséges, pontosan akkor, ha $x=\dfrac{2+\sqrt{13}}{3}$. A maximum értéke most már adódik, akár behelyettesítéssel, akár pedig úgy, hogy a jobb oldal köbét elosztjuk az uv szorzattal. Az eredmény összevonás és egyszerűsítés után $\dfrac{2}{27}(35+13\sqrt{13})$.

Márton Sándor (Szeged, Radnóti M. Gimn., 12. o.t.)

92 dolgozat érkezett. 4 pontos 68, 3 pontos 7, 2 pontos 1, 1 pontos 5, 0 pontos 11.

A C pontversenyben kitűzött gyakorlatok (645–649.)

C. 645. Ketten a következő játékot játsszák. Egy kupacból, amelyben kezdetben 7 szál gyufa van, felváltva vesznek el minden lépésben egy, két vagy három szál gyufát, amíg mind el nem fogy. Az nyer, akinél a végén páros számú gyufa van.

A kezdőnek, vagy ellenfelének van-e nyerő stratégiája? Hogyan kell játszania, hogy nyerjen?

Kvant

C. 646. A természetes számok sorozatából elhagyjuk a négyzetszámokat. A megmaradó számok sorozatában melyik a 2001-edik, és hányadik helyen áll a 2001?

Javasolta: *Nádor Péter,* Pécs

C. 647. Megrajzoltuk a koordinátarendszerben az $f(x)=\dfrac{1}{x}$ függvény grafikonját. Mekkorának válasszuk az új, egymással továbbra is egyenlő egységeket a tengelyeken, ha azt akarjuk, hogy a görbe a $g(x)=\dfrac{2}{x}$ függvény grafikonja legyen?

C. 648. Mennyi a $2^{\log_6 18}\cdot 3^{\log_6 3}$ pontos értéke?

C. 649. Egy csonkagúla alaplapjának a területe 8 cm^2, fedőlapjának a területe 1 cm^2. A gúlát az alaplappal párhuzamos síkkal két egyenlő térfogatú részre osztjuk. Mekkora a síkmetszet területe?

Javasolta: *Besenyei Ádám,* Tatabánya

❄

Beküldési határidő: 2001. december 15.
Cím: KöMaL Szerkesztőség (C gyakorlatok)
Budapest 112, Pf. 32. 1518

❄

A B pontversenyben kitűzött feladatok (3492–3501.)

B. 3492. Egy $n\times n$-es táblázatba beírjuk sorban az 1, 2, ..., n^2 számokat:

$$\begin{matrix} 1 & 2 & \dots & n\\ n+1 & n+2 & \dots & 2n\\ \vdots & \vdots & & \vdots\\ n^2-n+1 & n^2-n+2 & \dots & n^2 \end{matrix}$$

Minden sorból kiválasztunk egy-egy számot úgy, hogy semelyik kettő ne legyen ugyanabban az oszlopban.

Mik a kiválasztott számok összegének lehetséges értékei?

(*3 pont*) IMC 8, Prága, 2001

B. 3493. Ketten a következő játékot játsszák. Egy kupacból, amelyben kezdetben páratlan darab gyufaszál van, felváltva vesznek el minden lépésben egy, két vagy három szál gyufát, amíg mind el nem fogy. Az nyer, akinél a végén páros számú gyufa van.

A kezdőnek, vagy ellenfelének van-e nyerő stratégiája?

(*5 pont*) *Kvant*

B. 3494. Igazoljuk, hogy ha az $ax^3+bx^2+cx+d=0$ egyenletnek három különböző pozitív gyöke van, akkor $bc<3ad$.

(*4 pont*) Javasolta: *Bakonyi Gábor,* Budapest

B. 3495. Az $ABCD$ téglalap oldalai $AB=3$, $BC=2$. P az AB oldalnak az a pontja, amelyre a PD egyenes érinti, mégpedig E-ben, a BC átmérőjű kört. A kör középpontján és E-n átmenő egyenes az AB oldalt Q-ban metszi. Mekkora a PQE háromszög területe?

(*3 pont*) Javasolta: *Gerőcs László,* Budapest

B. 3496. Az $ABCD$ négyzet belsejében úgy vettük föl a P pontot, hogy $AP:BP:CP=1:2:3$. Mekkora az APB szög?

(*4 pont*)

B. 3497. Az x valós számra $\{x\}+\left\{x^{-1}\right\}=1$. Határozzuk meg

$$\left\{x^{2001}\right\}+\left\{x^{-2001}\right\}$$

értékét.

(*4 pont*) Javasolta: *Besenyei Ádám,* Tatabánya

B. 3498. Az ABC háromszögben C-nél derékszög van. A hegyesszögek szögfelezői a szemközti oldalakat az M és az N pontban metszik. Legyen P az MN szakasz és a C-ből induló magasság metszéspontja. Bizonyítsuk be, hogy a CP hossza egyenlő a beírt kör sugarával.

(*4 pont*) Javasolta: *Merényi Imre,* Budapest

B. 3499. Az x és y pozitív számok mértani közepe g. Bizonyítsuk be, hogy ha $g\ge 3$, akkor $\frac{1}{\sqrt{1+x}}+\frac{1}{\sqrt{1+y}}\ge\frac{2}{\sqrt{1+g}}$, ha pedig $g\le 2$, akkor $\frac{1}{\sqrt{1+x}}+\frac{1}{\sqrt{1+y}}\le\frac{2}{\sqrt{1+g}}$.

(*5 pont*)

B. 3500. Száz fiú és száz lány áll egy-egy sorban egymással szemben. Minden egyes fiú kiválaszt magának egy lányt (ugyanazt a lányt többen is választhatják) és egyenesen odamegy hozzá. Útközben a fiúk útvonalai nem keresztezik egymást. Ezután a fiúk visszaállnak a helyükre, most a lányok választanak, és most is teljesül, hogy miközben egyenesen odamennek a kiszemelt fiúhoz, az útvonalaik nem keresztezik egymást. Bizonyítsuk be, hogy van olyan lány és fiú, akik egymást választották.

(*4 pont*)

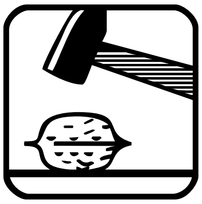
B. 3501. Adottak a térbeli koordinátarendszerben az $A(1,1,1)$ és a $P(1,1,0)$ pontok. Forgassuk el az OA félegyenes körül pozitív irányban 60°-os szöggel a P pontot. Határozzuk meg az elforgatott pont koordinátáit.

(*4 pont*)

Beküldési határidő: 2001. december 15.
Cím: KöMaL szerkesztőség (KöMaL feladatok)
Budapest 112, Pf. 32. 1518

❄

Az A pontversenyben kitűzött nehezebb feladatok (275–277.)



A. 275. Egy $n\times n$-es táblázatba beírjuk sorban az 1^2, 2^2, 3^2, $\dots$, $(n^2)^2$ számokat:

$$\begin{array}{cccc}
1^2 & 2^2 & \dots & n^2 \\
(n+1)^2 & (n+2)^2 & \dots & (2n)^2 \\
\vdots & \vdots & & \vdots \\
(n^2-n+1)^2 & (n^2-n+2)^2 & \dots & (n^2)^2
\end{array}$$

Minden sorból kiválasztunk egy-egy számot úgy, hogy semelyik kettő ne legyen ugyanabban az oszlopban.

Mik a kiválasztott számok összegének lehetséges értékei?

Terpai Tamás ötletéből

A. 276. Az $x_1, \dots, x_n$ pozitív számok szorzata $(n^\alpha-1)^n$, ahol $\alpha\ge 1$ valós szám. Bizonyítsuk be, hogy

$$\sum_{i=1}^{n}\frac{1}{(x_i+1)^{1/\alpha}}\ge 1.$$

A. 277. Legyen H_1 egy n-oldalú sokszög. Készítsük el a H_1, H_2, $\dots$, H_n sokszögsorozatot a következőképpen. Ha H_k-t már elkészítettük, akkor H_{k+1}-et úgy kapjuk, hogy H_k csúcsait rendre tükrözzük a pozitív körüljárás szerinti k-adik szomszédjukra.

Bizonyítsuk be, hogy ha n prímszám, akkor a H_1 és H_n sokszögek hasonlók.

❄

Beküldési határidő: 2001. december 15.
Cím: KöMaL szerkesztőség (KöMaL feladatok)
Budapest 112, Pf. 32. 1518

Matematika Határok Nélkül | Mathématiques Sans Frontieres

Versenyfelhívás

A 2001/2002-es tanévben is meghirdetjük a „Mathématiques Sans Frontieres – Matematika Határok Nélkül” nemzetközi vetélkedő magyarországi fordulóját budapesti, Békés megyei, Hajdú-Bihar megyei és Borsod-Abaúj-Zemplén megyei

középiskolák 9. évfolyamos osztályai számára.

A „Matematika Határok Nélkül” osztályok közötti erőpróba, tehát csak **teljes osztályok jelentkezését várjuk, ezen belül is csak a nem speciális matematika tagozatos osztályokét. (Versenyen kívül az utóbbiak is részt vehetnek a játékban.) A feladatokat az osztályok csoportmunkában oldhatják meg, tevékenységüket önállóan szervezve.**

A verseny időpontja: 2002. március 13. (szerda) 15 órától 16 óra 30 percig.

További információk a `http://berzsenyi.tvnet.hu/~kulcsar` honlapon találhatók.

A jelentkezési lapon a következő adatokat kérjük feltüntetni:

1. Iskola neve, típusa, címe, telefonszáma, e-mail címe.
2. Az osztály jele, létszáma, továbbá, hogy 4, 6 vagy 8 osztályos képzésben vesz-e részt az osztály.
3. A matematika heti óraszáma, a matematikatanár(ok) neve.
4. A felügyeletet vállaló tanár neve (benevezett osztályonként egy fő).

A jelentkezési határidő: 2001. december 15.

A jelentkezéseket az alábbi címre kérjük:

Budapestiek:
„Matematika Határok Nélkül”,
Berzsenyi Dániel Gimnázium,
1133 Budapest, Kárpát u. 49–53.
`msf@s2.berzsenyi.isk.tvnet.hu`

Békés megyeiek:
Szabó Zsófia,
Rózsa Ferenc Gimnázium,
5600 Békéscsaba, Andrássy út 56.

Borsod-Abaúj-Zemplén megyeiek:
Kiss István,
Ságvári Endre Gimnázium,
3700 Kazincbarcika, Jószerencsét út 2.
Tel.: (48) 510-050

Hajdú-Bihar megyeiek:
Deli Lajos, Hőgyes Endre Gimn. és Szakközépiskola,
4200 Hajdúszoboszló, Rákóczi út 44.

Miskolc:
Héjj Márta
Földes Ferenc Gimnázium
3525 Miskolc, Hősök tere 7.

Matematika Határok Nélkül Alapítvány