SZAKDOLGOZAT

Sempergel József

Debrecen
2007

Debreceni Egyetem
Matematikai Intézet

A SZÁMELMÉLET MEGJELENÉSE A KÖZÉPISKOLAI OKTATÁSBAN

Témavezető:
Dr. Bérczes Attila

Készítette:
Sempergel József
Informatika - Matematika

Debrecen
2007

Ezúton szeretnék köszönetet mondani vezetőtanáromnak, Dr. Bérczes Attilának a támogatásért és a segítségért, melyet a szakdolgozatom megírásához nyújtott.

Tartalomjegyzék

Bevezetés

Egyetemi tanulmányaim során matematikából talán a számelmélet témaköre állt legközelebb hozzám. Ezért is választottam témául a számelmélet középiskolai megjelenését. Szakdolgozatomban a középiskolában előforduló számelméleti témaköröket igyekszem összegezni.

A dolgozatom egy rövid történelmi összefoglalóval kezdőik, melyben a számelmélet kialakulását és fejlődését követem napjainkig, e tudományterület nagy alakjai által végzett felfedezések és eredmények érintőleges felsorolásával.

A szakdolgozatom fejezetei a középiskolai oktatásban megjelenő nagy számelméleti témaköröket mutatják be. Minden fejezet tartalmaz egy történelmi összefoglalót, melyek egy rövid, tömör összefoglalást tartalmaznak az adott témakör kialakulásáról, fejlődéséről. Igyekeztem érdekességeket, figyelemfelkeltő információkat becsempészni ezekbe az ismertetőkbe, így lehetőség nyílik ezek megemlítésére iskolai órákon, szakkörökön is.

A fejezetek tartalmaznak még egy elméleti bevezető részt is. Ezek felépítése, összetétele, a témakör középiskolai oktatásának megfelelően eltérő. Egyes témakörökhöz nagyobb méretű, összetettebb bizonyítást is mellékeltem, ezekre úgy gondolom szükség van, hogy felébresszük a diákokban a bizonyításra való hajlamot.

Végül, minden egyes témakörhöz összeállítottam egy válogatott feladatokból álló csokrot. Ezek a feladatok eltérő nehézségűek és különböző irányból közelítik meg az adott témakört. Minden feladathoz mellékeltem a feladat egy megoldásának menetét is.

I. A számelmélet története

Az i.e. VI. században dolgozó Pitagorasz (i.e. kb. 570-480) filozófus és matematikus volt. A források szerint Szamosz szigetén született. Pitagorasz követői pitagoreusoknak nevezték magukat. Pitagorasz és tanítványai a világ örök igazságait a számok közötti változatlan törvényekben vélték felfedezni. Ezért tanulmányozták a számokat. Ezzel lényegében megalapították a matematika egyik legszebb ágát, a számelméletet.

A pitagoreusok szerint az „egy" a számok eredete, amely részekre nem bontható, amelyet osztani nem lehet, csak szorozni. Így az egynél kisebb szám nincs. Az egynél nagyobb számok az egyből keletkeznek, annak megsokszorozásával. A számok viszont részekre bonthatók, oszthatók, hiszen mindegyik valahány egységet tartalmaz. A két egyenlő részre osztható számok a páros számok, a két egyenlő részre nem bonthatók a páratlan számok. Első számelméleti tételeik is a páros és páratlan számok elméletéhez tartoztak. Ezek közül néhány:

- Páros számok összege és különbsége is páros.
- Két páratlan szám összege páros.
- Páros számú páratlan szám összege páros.
- Páratlan számú páratlan szám összege páratlan.
- Ha páros számból páratlant vonunk ki, akkor páratlant kapunk.
- Páratlan és páros szám szorzata páros.
- Olyan szám, amelynek a fele páratlan, csak úgy bontható kéttényezős szorzatra, hogy az egyik tényező páros, a másik páratlan.

A számok oszthatóságával kapcsolatban két, ma sem problémamentes felfedezésük volt, a tökéletes számok és a baráti számpárok. A pitagoreusok ismerték a 6, 28, 496 és a 8128 tökéletes számokat és a 220, 284 baráti számpárt. Ismerték a prímszám és az összetett szám fogalmát is.

Érdekes momentum, hogy egy babiloni agyagtáblán megtalálható egy „Pitagoraszi számhármas" sor, amit jóval Pitagorasz előtt, Kr. e. 1600 és 1900 között készítettek. Ez az emberiség egyik legrégebbi számelméleti dokumentuma.

Az irracionális számok első szisztematikus vizsgálatát általában az i.e. 350 és 300 között élt Euklidész nevéhez kapcsolják, ő igazolta először, hogy az $\sqrt{2}$ irracionális. Euklidész legfontosabb és legismertebb műve az Elemek. A tizenöt könyvből álló alkotásnak, három része (a VII., VIII. és IX.) foglalkozik számelmélettel. Mindannak nagy része, amit a középiskolában matematikából - különösen amit mértanból, geometriából - tanítanak, megvan már az Elemekben. Sőt, sok helyütt a világon még nem is olyan régen ezt - az Elemeket - tanították az iskolában matematika órán.

Ugyancsak az ókorban jelentek meg a diophantoszi problémák is, amelyekben rendszerint egyenletek egész szám megoldásait keresték.

A görög, később kínai és hindu számelméleti eredmények után egészen a XVII. századig ezen a területen nem történt semmi említésre méltó fejlődés. Ebben a században viszont Fermat munkássága felkeltette álmából a matematikának ezt a mellőzött ágát. Olyan tömegű új ismeretekkel bővítette, ami felkeltette mások érdeklődését is, Ezért Fermat munkásságától szokás a számelméletet önálló kutatási ágként kezelni. Nagy hatással voltak munkásságára Diophantosz eredményei. Nevéhez fűződik az úgynevezett „nagy Fermat-tétel", mely szerint az egész kitevős $x^n + y^n = z^n$ egyenletnek nincs a triviálistól különböző megoldása a természetes számok körében, ha $n > 2$.

Szintén számelmélettel foglalkozott Mersenne, aki először írta fel 1644-ben a nevét őrző, 2^p-1 alakú, ún. Mersenne-féle számok (ahol p prímszám) formuláját. Ez nem ad prímszámot p minden prímszámértékére, de hosszú időn át fontos szerepe volt a prímszámok tanulmányozásában, újabb prímszámok megtalálásában.

Leonhard Euler (aki az 1700-as években élt, és alkotott) később Fermat több tételét bizonyította. Gauss mellett Euler számít a matematika egyik legtermékenyebb, legsokoldalúbb tudósának, aki huszonnyolc nagyobb mű, hétszázötven értekezés, és több tankönyv megalkotója. Ő bizonyította be, hogy a $2^{32} + 1$ alakú Fermat-féle szám nem prím, és hogy minden páros tökéletes szám 2^k $(2^{k+1} - 1)$ alakú. Felfedezte a nyolcadik tökéletes számot, és hatvanegy barátságos számpárt talált. Vizsgálatai nyomán tovább fejlődhetett a számelmélet valamennyi ága, többek között az analitikus és algebrai számelmélet is. Euler a számelmélet mellett a matematika szinte valamennyi ágában maradandót alkotott. A

síkgeometriában, térgeometriában, trigonometriában szintén jelenős eredmények őrzik nevét, s a „königsbergi hidak” problémája kapcsán a gráfelmélet alapjait is ő rakta le.

A XIX. század számelméleti kutatásainak irányát Gauss szabta meg az 1801-ben megjelent Disquisitiones arithmeticae című és későbbi műveivel. Alkotásaival kiérdemelte a „princeps mathematicorum”, vagyis a matematikusok fejedelme címet. Munkássága nemcsak azért jelentős, mert sok számelméleti feladatot megoldott, hanem mert új módszereket vezetett be, és új kutatási irányokat jelölt ki. Gauss mondta: „Ha a matematika a tudományok királya, akkor a számelmélet a matematika királynője.”

A legújabbkor további jeles gondolkodói voltak még például Dirichlet, Dedekind, Csebisev, illetve Vinogradov, akik szintén számos jelentős új felismerésekkel, bizonyításokkal tették még teljesebbé a számelmélet színes és nagyszerű világát.

II. A matematika tanítás célja és feladatai

A matematikatanítás célja és ennek kapcsán feladata: megismertetni a tanulókat az őket körülvevő konkrét környezet mennyiségi és térbeli viszonyaival, megalapozni a korszerű, alkalmazásra képes matematikai műveltségüket, fejleszteni a gondolkodásukat, az életkornak megfelelő szinten biztosítani a többi tantárgy tanulásához, a mindennapok gyakorlatához szükséges matematikai ismereteket és eszközöket, bemutatni azok egyszerű, konkrét gyakorlati hasznosságát.

Különös figyelmet kell fordítani a fogalmak alapozására, kialakítására, elmélyítésére, s ez nem nélkülözheti a sokoldalú tevékenységeket, változatos cselekvéseket. A kísérletezés, a játék szerepe nem szűnhet meg a középiskolai évfolyamokon sem. Alapvető célunk a megértésen alapuló gondolkodás fejlesztése, a valóságos szituációk és a matematikai modellek közötti kétirányú út megismertetése, és azok használatának fokozatos kialakítása.

A matematikával való foglalkozás fejlessze a tapasztalatból kiinduló önálló ismeretszerzést, alakítsa ki az önálló gondolkodás igényét, ismertesse meg a problémamegoldás örömét, és szolgálja a pozitív személyiségjegyek kialakulását.

Törekedni kell a tanulók pozitív motiváltságának biztosítására, önállóságának fejlesztésére, a pontos és kitartó munkára való nevelésre, a reális önbizalom, az akaraterő, az igényes kommunikáció kialakítására, a gondolatok érvekkel való alátámasztásának fejlesztésére. Nagy szerepet kap az elemző gondolkodás fejlesztése, a problémamegoldás mellett az igazolások keresése, egyszerűbb következtetések megértése, észrevétele, önálló megfogalmazása.

Különböző területekről érkező, más és más módon megfogalmazott információk önálló értelmezésével és az ismeretek meg tanulásával fokozatosan el kell sajátítani – és alkalmazni is tudni kell – a deduktív út formáit. Eközben nem csökken az induktív út jelentősége sem. Hangsúlyt kell helyezni a sokszínű tevékenységre, a tapasztalatok tudatosítására, különböző módokon való rögzítésére, értelmezésére, rendszerezésére, összefüggések keresésére. A matematika tanításának-tanulásának a felső tagozaton is

jellemzője a felfedeztetés, a probléma felvetésétől a megoldásig vezető – néha tévedésektől sem mentes – útnak az egyre önállóbb bejárása.

Nagy jelentőséget tulajdonítunk a következtetésre épülő problémamegoldásnak, az algoritmusok kialakításának, követésének is. Mindezt eleinte konkrét helyzetekben végezzük, majd erre építve általánosítunk.

A matematika – a lehetőségekhez igazodva – támogassa az elektronikus eszközök (zsebszámológép, grafikus kalkulátor, számítógép, internet stb.), információhordozók célszerű felhasználásának megismerését, alkalmazásukat az ismeretszerzésben, a problémák megoldásának egyszerűsítésében.

III. A számfogalom és a számrendszerek

Történelmi áttekintés

A számfogalom már az őskorban megjelent, az ősember kezdetben az egy, kettő és sok között tett különbséget, amint azt a nyelvészek számos ma még létező primitív népnél is megfigyelték. Különböző népeknél különböző számrendszerek kialakulását lehetünk tanúi, példaként említeném a hetes, tizenkettes és hatvanas számrendszereket. A római számoknál egy érdekes dolgot figyelhetünk meg, ugyanis ezt a számrendszert az ötös és tízes számrendszer keverékének tekinthetjük.

A számok írásának legősibb módja a csontok, illetve fadarabok vésése majd kötélcsomózással, illetve gyöngyök felfűzésével jegyezték fel a különböző számértékeket. Később a papirusz Egyiptomi megjelenésével elterjedhettek az írott számjegyek. Az egyiptomiak tízes számrendszert használtak és a tíz minden hatványára külön jelölést alkalmaztak, a nagyobb számokat, pedig a jelek ismétlésével írták le.

A babiloniak hatvanas számrendszert használtak, ők határozták meg a négyzetgyök kettő értékét négy tizedes jegy pontossággal.

A legelterjedtebb számrendszerünk a tízes, melynek kialakulását és elsajátítását a kézen lévő ujjak megszámlálása egyszerűsítette. Nagyon gyakran használt a számrendszer még a kettes melynek elterjedését a számítógépek térhódítása tette lehetővé, mivel a számítógépes adattárolás két jel, a 0 és 1 bit használatán alapul. Ugyanígy a számítógépek terjedése miatt gyakori még a nyolcas és tizenhatos számrendszerek használata.

A megfelelően kialakított számfogalom, a bővülő számkörben végzett műveletek értése és begyakorlottsága alapfeltétele a további eredményes munkának. Azt, hogy minden számot fel tudunk írni a 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 számjegyek és a tíz hatványainak segítségével, ma már az általános iskola hetedik osztályában megtanulják a diákok.

Tétel:

Tetszőleges A>0 egész szám felírható

$A = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$ alakban, ahol /1/

$0 \le a_i \le 9$ és $a_n \neq 0$. /2/

Ebben a felírásban a számjegyek egyértelműen vannak meghatározva.

Bizonyítás:

A maradékos osztás alapján az A szám

$A = 10q_0 + a_0, \quad (0 \le a_0 \le 9)$ /3/

alakba írható, ahol q_0 és a_0 egyértelműen meg vannak határozva. Hasonlóan

$q_0 = 10q_1 + a_1, \quad (0 \le a_1 \le 9)$ /4/

alakba írható, ahol q_1 és a_1 is egyértelműen vannak meghatározva. Így folytatva

$q_1 = 10q_2 + a_2, \quad (0 \le a_2 \le 9)$

$\vdots$ /5/

$q_k = 10q_{k+1} + a_{k+1}, \quad (0 \le a_{k+1} \le 9)$

$\vdots$

előállításra jutunk. Véges sok lépésen belül be kell, hogy következzen, hogy $q_n = 0$, ugyanis $q_0 > q_1 > \ldots > q_{n-1} > q_n$ szigorúan csökkenő nem negatív egészek. Így

$q_{n-1} = 10 \cdot 0 + a_n, \quad (0 \le a_n \le 9)$ /6/

Visszahelyettesítve rendre a /4/, /5/, /6/ egyenleteket /3/ -ba, azt nyerjük, hogy

$A = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$, ahol $a_n, a_{n-1}, \ldots, a_0$ egyértelműen vannak meghatározva.

Megjegyzés

A tízes számrendszer mellet természetesen bármely 1-nél nagyobb alapú számrendszer használható. Amennyiben 10-nél nagyobb számrendszerrel dolgozunk, gondoskodnunk kell a számjegyek megfelelő jelöléséről, vegyük például a 16-os számrendszert: nullától-kilencig egyezik a jelölés a tízes számrendszerbelivel, plusz a 10=A, 11=B, 12=C, 13=D, 14=E, és a 15=F megfeleltetést alkalmazzuk. Ezt az elfogadott jelölést használva már fel tudjuk írni

tizenhatos számrendszerbe a következő számot: $2315_{10}=9\cdot16^2+0\cdot16^1+B\cdot16^0$, vagyis $2315_{10}=90B_{16}$.

Feladatok:

1. példa

Írjuk fel a következő számokat kilences számrendszerben:

a, 100

b, $5\cdot9^2+2\cdot9^4+2\cdot9+7\cdot9^3+6$

c, $21\ 021\ 101_3$

Megoldás

a, $100_{10}= 1\cdot9^2+2\cdot9^1+1\cdot9^0=121_9$

b, Rendezzük a kifejezést! $2\cdot9^4+7\cdot9^3+5\cdot9^2+2\cdot9^1+6\cdot9^0=27526_9$

c, Csoportosítsuk kettesével a hármas számrendszerben felírt számjegyeket, majd az így kialakított kétjegyű számokat váltsuk át kilences számrendszerben és az átváltások eredményeit írjuk az eredeti sorrendnek megfelelően egymás után. 21, 02, 11, 01, ebből 21=7, 02=2, 11=4, 01=1. Vagyis $21021101_3=7241_9$.

Megjegyzés

A c feladathoz hasonlóan írhatók át a számok a alapú számrendszerről a^k alapúra, és viszont ($1< k$, és $k\in \mathbf{N}$).

2. példa

Egy sportszergyártó cég a pingponglabdák csomagolására az alábbi szabványt tartja a legjobbnak:

- a pingponglabdákat hatosával csomagolják kis fehér dobozba;
- hat fehér dobozt egy kék dobozba tesznek;
- hat kék dobozt beleraknak egy nagyobb zöld dobozba;
- hat zöld dobozt egy nagy sárga tartóba pakolnak;
- hat sárga tartót egy óriási piros dobozba csomagolnak.

Hogyan lehet a szabványokat betartva 10 000 pingponglabdát becsomagolni? Lesz-e kimaradó labda? Melyik dobozból hányat látunk a csomagolás végén?

Megoldás:

Osszunk 6-tal maradékosan!
A tízezret maradékosan elosztva hattal 4-et kapunk, vagyis 4 labda kimarad a csomagolás során.
A 9996 előáll a következő formában:

$$9996_{10}=1\cdot6^5+1\cdot6^4+4\cdot6^3+1\cdot6^2+4\cdot6^1.$$

Az egyes ládák az egyes helyi értékeknek felelnek meg, így végül 1 piros, 1 sárga, 4 zöld, 1 kék, 4 fehér dobozt látunk és a 4 kimaradt labdát.

3. példa

a, A lehető legkevesebb mérősúly segítségével szeretnénk lemérni egész kilogramm tömegű, 100 kg-nál nem nehezebb tárgyakat. Használhatunk egy kétkarú mérleget, melynek az egyik serpenyőjébe tesszük a megmérendő tárgyat, a másikba pedig a mérősúlyokat.
Milyen mérősúlyokat használjunk? (Olyan súlykészletre van szükség, hogy minden esetre felkészülve az összes tárgy lemérhető legyen.)

b, Milyen súlyokat használjunk akkor, ha a mérleg mindkét serpenyőjébe tehetjük őket?

Megoldás

a) 1, 2, 4, 8, 16, 32, 64 kg-os súlyok megfelelőek (vagyis a kettő hatványai), ezek segítségével minden súlyt ki elő tudunk állítani 100 kilogrammig.
6 súly azért nem elég, mert minden súlyt vagy használunk, vagy nem. Ez súlyonként két lehetőséget jelent, így 6 súly esetén legfeljebb $2^6 = 64$-féle tömeget mérhetünk.

b) 1, 3, 9, 27, 81 kg-os súlyok megfelelőek (vagyis a három hatványai).
4 súly nem elég számunkra, mert minden súlyt vagy az egyik serpenyőbe, vagy a másikba tesszük, vagy nem használjuk. Ez súlyonként három lehetőség, így 4 súly esetén legfeljebb $3^4 = 81$-féle tömeget mérhetünk.

IV. Prímszámok

Történelmi áttekintés

Gauss, a matematikusok fejedelme így fogalmazott: „a tudomány méltósága megkövetelni látszik, hogy egy olyan alapvető kérdést miszerint egy számról eldöntsük, hogy prím-e, és ha nem, akkor megtaláljuk prímtényezőit, megfelelően kezelni tudjunk.”

A prímtényezők gyors előállítására máig nincs kielégítő módszer. Teszt segítségével könnyen találhatunk prímszámokat, két nagy prímszámot gyorsan össze tudunk szorozni, de kellően nagy prímeknél a szorzatot még senki sem képest felbontani tényezőire, annak ellenére, hogy képes felismerni azt, hogy a szám összetett. Ezen az elven alapulnak a nyilvános kulcsú titkosírások közül a leghatékonyabbak.

Egy gyakori tévedés a középiskolában tanuló diákoknál, hogy prímszám minden olyan szám, amely csak önmagával és 1-gyel osztható. Ez a definíció nem pontos, mert eszerint az 1 is prím. A pontosabb középiskolába szánt meghatározása: prímszámok azok az egész számok, amelyeknek pontosan két osztójuk van. Ebből következően a 0 és az 1 nem prím és a kettő az egyetlen páros prímszám.

Definíció

Ha $q \neq 0$, $q \neq \epsilon$ és $q \mid ab$ –ből a $q \mid a$ és $q \mid b$ oszthatóságoknak legalább az egyike következik, akkor a q számot prímszámnak nevezzük.

Tétel

Végtelen sok prím van.

Bizonyítás (Indirekt)

Tegyük fel, hogy csak a $p_1, p_2, p_3, \ldots, p_n$ számok prímek. Képezzük a következő számot:

$$A = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$$

Ennek a számnak nem osztója egyik felsorolt prím sem. Tehát vagy A prím, vagy van egy olyan prím osztója, amely nem szerepelt a fentiek között. Minkét eset arra utal, hogy van a felsoroltakon kívül más prím is, ami ellentmond a kezdeti feltevésünkkel. Tehát ebből az következik, hogy végtelen sok prímszám van.

A következőkben a számelmélet alaptételét és bizonyítását fogalmazom meg. Úgy gondolom, a bizonyítást, ha tanórákon nem is, de matematika szakkörön érdemes bemutatni, mert sok jó ötletet tartalmaz.

Tétel (Számelmélet alaptétele)

Minden 1-nél nagyobb pozitív egész szám egyértelműen felbontható pozitív prímszámok szorzatára.

Bizonyítás

Először is osszuk az egynél nagyobb pozitív egészeket két csoportba: legyen az egyik csoport a prímszámok, a másik pedig az összetett számok csoportja.

A bizonyításhoz szükségünk lesz a következő állításra: egy összetett szám legkisebb valódi osztója mindig prímszám. Az állítást indirekt módon bizonyítjuk.

Legyen az összetett számunk m, a legkisebb valódi osztója pedig n. Ha n nem prím, akkor létezik n-nek valódi osztója, amely - mivel n osztója m-nek - nyilván m-nek is osztója. Tehát találtunk m-nek egy n-nél kisebb valódi osztót, amely ellentmond a kiindulási feltételünknek, amely szerint m legkisebb valódi osztója n. Ebből következően n csak prímszám lehet, tehát az állítást beláttuk.

A tétel két dolgot mond ki: az első az, hogy minden szám felbontható prímtényezők szorzatára, a második pedig, hogy ez a felbontás csak egyféleképpen végezhető el, ha a tényezők sorrendjét nem vesszük figyelembe (a szorzásban a tényezők sorrendje nem érdekes). Először az első állítással foglalkozunk.

Az állítást prímekre már beláttuk, hiszen minden prím önmagában egy „egytényezős szorzat". Tekintsünk tehát egy összetett számot, majd osszuk el a legkisebb valódi osztójával, amelyről már tudjuk, hogy csak prím lehet. Az osztás után két lehetőség van: a hányados vagy prím, vagy összetett szám. Ha prím, akkor készen vagyunk – van egy kéttényezős szorzatunk –, ha összetett szám, akkor ismételjük meg a hányadosra az előbbi műveletet (osszuk el a legkisebb valódi osztójával), és ezt addig folytassuk, amíg prímszámot nem kapunk. Mivel végig csak prímekkel osztottunk, és a végeredmény is prím, ezért az állítást igazoltuk: tetszőleges összetett szám felbontható prímtényezők szorzatára.

Az alaptétel második fele: egy számhoz csak egy szorzatot kaphatunk, ha a szorzótényezők sorrendjét nem vesszük figyelembe. Az állítást a már ismert indirekt módszerrel fogjuk bizonyítani; tegyük fel tehát, hogy van olyan szám, amely kétféleképpen is felbontható. Ezt felírhatjuk úgy, hogy $k=p_1 \cdot p_2 \cdot \ldots \cdot p_a = q_1 \cdot q_2 \cdot \ldots \cdot q_b$, ahol minden p és q prímszám. Ha p-k és q-k között vannak egyenlők (tehát pl. $p_4=q_7=19$), akkor ezekkel oszthatjuk az egyenletet és a végén egy olyan egyenlőséghez jutunk, amelynek mindkét oldalán prímszámok szorzata szerepel, ám ezek között különböző oldalakon már nincsenek egyenlők. Válasszuk ki most az így kapott egyenlet bal oldaláról az első prímszámot! Tudjuk, hogy a másik oldalon ez a szám nem szerepelhet, hiszen akkor osztottunk volna vele. Viszont mivel prímek szorzatáról van szó, tudjuk, hogy ezzel a kiválasztott számmal a bal oldal osztható, a jobb oldal pedig nem. Így az egyenlőség nem teljesülhet, tehát ellentmondásra jutottunk, azaz a kiinduló állítást beláttuk.

Prímszámok a: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, … stb. számok. Az alábbi módszerrel meghatározhatjuk azon p prímeket, melyek 1 és n között helyezkednek el. Írjuk fel 1-től n-ig a számokat. Tudjuk, hogy 2 az prím, húzzuk át 2 összes többszörösét. A 2-nél nagyobb, legkisebb, át nem húzott szám a 3, amely prím lesz és a 3 kivételével 3 összes többszörösét húzzuk át. Ismét a 3-nál nagyobb számok közül a legkisebb prím az 5 lesz és ezt az eljárást folytatva n-ig, az át nem húzott számok megadják az összes prímet 1 és n között. Ezt az eljárást *Eratoszthenészi szitának* nevezzük.

Megjegyzés:

Elegendő az 1 és $\sqrt{n}$ között p prímekkel elvégezni a szitálást, mivel ha valamely a szám n-nél kisebb és összetett, akkor van $\sqrt{n}$ -nél kisebb prím osztója.

Feladatok

1. feladat

Bizonyítsuk be, hogy ha 2^k-1 prímszám (k Є N), akkor k is prímszám.

Megoldás (Indirekt bizonyítás)

Tegyük fel, hogy k nem prímszám.

Ha k = a · b, ahol a > 1, b >1, akkor

$2^{ab} – 1 = (2^a)^b - 1^b$

és ez osztható a 2^a-1>1 természetes számmal. Vagyis ellentmondásra jutottunk, ezzel bizonyítottuk az állításunkat.

2. feladat

Bizonyítsuk be, hogy bármely prímszámot 30-cal elosztva, a maradék vagy 1, vagy prímszám.

Megoldás

Egy prímszám 30-cal osztva nem adhat 2 maradékot (kivéve a p = 2-t), mert akkor páros lenne, de nem lehet a maradék 3 sem (kivéve a p = 3-t), mert akkor p osztható lenne 3-mal. Így tovább haladva azt kapjuk, hogy egy p prímet 30-cal osztva a maradék csak az 1, 7, 11, 13, 17, 19, 23, 29 természetes számok valamelyike lehet.

3. feladat

Bizonyítsuk be, hogy bármely 3-nál nagyobb prím négyzete 24-gyel osztva 1 maradékot ad.

Megoldás

Egy szám 24-el oszthatóságának feltétele, hogy a szám osztható nyolccal és hárommal. A feladat állítását felhasználva végezzük el a következő átalakítást:

$$p^2-1=(p-1)(p+1).$$

Azt kell bizonyítanunk, hogy ez kifejezés 3-mal és 8-cal is osztható.

A (p-1), p, (p+1) számok szomszédos számok, így valamelyikük osztható 3-mal (három szomszédos szám közt mindig van hárommal osztható). De az nem lehet a p, így vagy p - 1 vagy p + 1 osztható 3-mal.

A p - 1 és p + 1 számok mindegyike páros, a páros számok sorozatában szomszédos számok. Mivel minden második páros szám nem csak 2-vel, de 4-gyel is osztható, így (p-1)(p+1) osztható 8-cal. Ezzel az állítást bebizonyítottuk.

4. feladat

András és Béla már elmúltak 5 évesek, mindkettőjük életkora prímszám. Ha András annyi idős lesz, mint Béla most, akkor Béla életkora is prímszám lesz. Bizonyítsuk be, hogy amikor András született, Béla éveinek a száma osztható volt 6-tal.

Megoldás

Azt kell megmutatnunk, hogy ha három db 5-nél nagyobb prímszám egy számtani sorozat egymást követő elemei, akkor a differencia osztható 6-tal.
Hogy a differencia páros, az nyilvánvaló. Így azt kell bizonyítani, hogy osztható 3-mal. Legyenek e prímek p, p+d, p+2d.

1. Ha p 3-mal osztva 1 maradékot ad és d is 3-mal osztva 1 maradékot ad, akkor p+ 2d osztható 3-mal,
   ha d 3-mal osztva 2 maradékot ad, akkor p+d osztható 3-mal.

2. Ha p 3-mal osztva 2 maradékot ad és d 3-mal osztva 1-et, akkor p+d osztható 3-mal,
   ha d 3-mal osztva 2-t ad maradékul, akkor pedig p+d osztható 3-mal.

Tehát d-nek 3-mal oszthatónak kell lennie (ilyen sorozat pl.: 5, 1, 17).

3. feladat

Öt darab egymást követő pozitív egész szám közül a negyedik prímszám. Bizonyítsuk be, hogy e számok szorzata osztható 240-nel.

Megoldás

A (p-3) · (p-2) · (p-1) ·p· (p+1) szorzatról kell belátni, hogy osztható 5-tel, 3-mal és 16-tal.
Öt db egymás utáni szám között biztosan van 5-tel, illetve 3-mal osztható, tehát a szorzat 15-tel biztosan osztható.
Mivel p prím, ezért $(p-3)$, $(p-1)$ és $(p+1)$, biztosan párosak, s mivel a páros számok sorozatának ők egymást követő elemei, ezért valamelyikük biztosan osztható 4-gyel is, vagyis szorzatuk osztható 16-tal.

V. Oszthatóság

Történelmi áttekintés

Már az egyiptomiak is foglalkoztak az oszthatóság témakörével, ezt bizonyítják a felfedezett leletek is. Különbséget tettek a páros és páratlan számok között. Az egyiptomi Rhind-papiruszon (i.e. 2000 – 1700) a „törzstörtek” felsorolásában csak a páratlan nevezőjűek szerepelnek.

A hárommal való oszthatóság szabályával a pizai Leonardónál találkozunk először a „Liber Abaci” című könyvében.

Az öttel való oszthatósági szabályt már a régi hinduk is tudták.

A tizeneggyel való oszthatósági szabályt Al-Karkhi arab matematikus ismertette először. Szabatos megfogalmazást Lagrange francia matematikus adott rá.

Teljes általánosságban vizsgálta a természetes számok oszthatóságának a kérdését Pascal francia matematikus.

Definíció:

Az a és b egész számok esetén (jelekkel: a ,b $\in$ Z), akkor mondjuk az „a” számot a „b” számmal oszthatónak, ha létezik olyan „q”, amelyre a = b·q, ahol q is egész szám. Ekkor b-t osztónak, a-t többszörösnek nevezzük.

Jelölése: a | b.

Ha ilyen q szám nem létezik, akkor azt mondjuk, hogy b nem osztója a-nak.

Jelölés: b ł a.

Az oszthatóság tulajdonságai:

1. Minden szám osztója önmagának. Az a | a, hiszen a·1 = a
2. Ha egy szám osztója egy másiknak, akkor annak többszöröseinek is osztója.

   Ha a | b , akkor a | b·c
3. Egy szám osztójának osztója a számnak is osztója.

   Ha a | b és b | c akkor a | c
4. Ha egy szám osztója két számnak, akkor összegüknek és különbségüknek is osztója.

   Ha a | b és b | c akkor a | c
5. Ha egy szám osztója egy összegnek és az összeg egyik tagjának, akkor osztója a másik tagnak is.

   Ha a | b + c és a | b, akkor a | c
6. Ha egy szám egy összeg valamelyik tagjának nem osztója, akkor az összegnek sem osztója.

   Ha a | b és a ł c, akkor a ł b + c

7. Az a, b természetes számokra, ha a | b és b | a, akkor a = ± b.
8. A 0 minden számnak osztója. Bármely a egész szám esetén a | 0, hiszen 0 · a = 0.

Tétel

Az oszthatóság reflexív, antiszimmetrikus és tranzitív reláció.

Bizonyítás

1) reflexivitás: a | a, ugyanis a = 1 · a.

2) antiszimmetria: Ha **a | b** és **a ≠ ϵ · b**, akkor **b ł a**, ugyanis, ha **b | a** is fennállna, akkor alkalmas **q** és **q'**-vel **b = aq**, **a = bq'** volna, tehát azt nyernénk, hogy **b = b· (q·q')**, vagyis **q·q'=1**, amiből **b ≠ 0** esetén **q = q' = ± 1** következik. Ha pedig **b = 0**, akkor ebből már **a = 0** adódik, ami viszont ellentmond annak, hogy **a ≠ ϵ · b.**

3) tranzitivitás: Ha **a | b** és **b | c**, akkor **a | c**, ugyanis **b = a·q**, **c = b·q'** tehát **c = (a·q) ·q' = a· (q·q')**, és ebből **a | c** következik.

Tétel:

Tetszőleges a és b egész számokhoz léteznek olyan egyértelműen meghatározott q és r egész számok, amelyekre a = b·q + r, ahol $0 \leq r < |b|$.

Bizonyítás:

A létezés bizonyítása:

Legyen **a** $\geq$ **b > 0**, ahol **a** és **b** egész. Tekintsük az **a – b** különbséget. Ha **a – b < b**, akkor **a – b = r** jelöléssel **a = b + r** előállításra jutunk, ahol már **0** $\leq$ **r < b**. Ebben az esetben az **a** szám **b**-vel való osztásánál az 1 hányados, az r pedig maradék. Ha azonban a – b $\geq$ **b,** akkor a – b -ből újra levonjuk a b számot. Lehet, hogy már b-nél kisebb számra jutunk. Ha nem, akkor újra és újra ismételjük az eljárást. Véges sok lépés után el kell jutnunk egy olyan a – qb = r számhoz, amelynél már $0 \leq r < b$. Ebből $a = qb + r$, $0 \leq r < b$. Az ilyen tulajdonságú q számot hányadosnak, az r számot pedig maradéknak nevezzük.

Egyértelműség bizonyítása:

Tegyük fel az állítással ellentétben, hogy adott a és b-hez legalább két különböző q_1 és q_2 illetve r_1 és r_2 tartozna. Ekkor $a = bq_1 + r_1$, $0 \leq r_1 < |b|$, és $a = bq_2 + r_2$, $0 \leq r_2 < |b|$ teljesülne. De ebből $b(q_1 – q_2) = r_2 – r_1$, vagyis $b \mid r_2 – r_1$ következne, azonban az előző mondat alapján $|r_2 – r_1| < |b|$. Tehát $b \mid r_2 – r_1$, és a segédtétel miatt ez csak $r_2 – r_1 = 0$, vagyis $r_2 = r_1$ mellett teljesülhet. Ebből viszont $bq_1 = bq_2$, illetve $b \neq 0$ –val való egyszerűsítés után $q_1 = q_2$ következik, ami ellentmondás. Ezzel bizonyítottuk az egyértelműséget.

Az általános iskola hetedik osztálya a hozott számelméleti ismeretek összefoglalásával kezdődik. A gyerekek már ebben az évfolyamban megismerkednek a következő fogalmakkal: az oszthatósággal, az osztópárokkal, és az oszthatóság elemi tulajdonságaival az egész számok körében. Ebben az életkorban történik először az oszthatósági szabályok ismertetése is: 2-vel, 3-mal, 5-el, 9-cel, 11-gyel való osztás. Megismerkednek a legnagyobb közös osztó és a legkisebb közös többszörös fogalmával.

Amikor ez az anyag kerül tárgyalásra, a diákoknak már ismerniük kell például a természetes, egész, illetve a racionális számok halmazát. Az oszthatóság oktatása során nyomatékosítanunk kell a diákok irányába, hogy az egész számok körében vizsgálódunk!

Ezen ismeretek megtanítási módja a spiralitás elvét követi, ennek megfelelően a hetedik osztálytól kezdve minden évfolyamban előfordulnak az oszthatóság témaköréhez kapcsolódó feladatok.

Feladatok

1. feladat

Legyenek n, k és m pozitív egész számok. Bizonyítsuk be, hogy ekkor $n \cdot k \cdot m \cdot (n^2 - k^2) \cdot (n^2 - m^2) \cdot (k^2 - m^2)$ osztható 120-al.

Megoldás

Azt kell megmutatni, hogy az $n \cdot k \cdot m \cdot (n - k) \cdot (n + k) \cdot (n - m) \cdot (n + m) \cdot (k - m) \cdot (k + m)$ 3-mal, 8-cal és 5-tel is osztható.

1. Ha n, k, m valamelyike osztható 3-mal, akkor a szorzat is.

   Ha egyik sem osztható 3-mal, akkor n, k, m közül kell lennie kettőnek, melyek 3-mal osztva ugyanazt a maradékot adják, így ezek különbsége osztható 3-mal.

2. Ha n, k, m mindegyike páros, akkor a szorzat osztható 8-cal.

   Ha két páros van közöttük, akkor ezek összege is, különbsége is osztható 2-vel, így a szorzat osztható 8-cal.

   Ha egy páros van közöttük, akkor a két páratlan összege és különbsége is osztható 2-vel, így a szorzat megint osztható 8-cal.

   Ha mindhárom páratlan, akkor bármely kettő összege és különbsége is páros, tehát a szorzat osztható 8-cal.

3. Ha n, k, m valamelyike osztható 5-tel, akkor a szorzat is osztható 5-tel.

   Ha egyik sem, de van közöttük kettő, melyek 5-tel osztva ugyanazt a maradékot adják, ekkor ezek különbsége osztható 5-tel. Ha mind a három más-más maradékot ad 5-tel osztva, akkor ezek a maradékok 1, 2, 3 vagy 4. Ha 1, 2, 3, akkor 2+3 osztható 5-tel, ha 1, 2, 4, akkor1+4osztható 5-tel, ha 1, 3, 4, akkor 1+4, ha 2, 3, 4, akkor 2+3osztható 5-tel.

2. feladat

Melyek azok a k, l, m természetes számok, amelyekre [k; l; m]=60984, 88k=9l és 11m=2k.

Megoldás

A prímtényezős felbontást előállítva: $60984 = 2^3 \cdot 3^2 \cdot 7 \cdot 11^2$, ezért – a feltételeket figyelembe véve – a keresett számok: $n=2^3 \cdot 7 \cdot 11^2=6776$, $k=3^2 \cdot 7 \cdot 11=693$, $m=2 \cdot 3^2 \cdot 7=126$.

3. feladat

Bizonyítsa be, hogy ha $n \in N^+$ esetén pontosan egy olyan n szám van, amelyre n-9, n-3, n-1, n+3, n+5 számok mindegyike prímszám!

Megoldás

A számokat az öttel való oszthatóság szempontjából vizsgáljuk:

- n=5k esetén n+5
- n=5k+1 esetén n-1
- n=5k+2 esetén n+3
- n=5k+3 esetén n-3
- n=5k+4 esetén n-9 osztható 5-tel.

Belátható, hogy ezen esetek közül csak n-9=5 esetben lesznek a keresett számok prímek: 5, 11, 13, 17, 19.

4. feladat

Bizonyítsa be, hogy három közvetlenül egymás után következő pozitív egész szám szorzata osztható 504-gyel, ha középső szám köbszám.

Megoldás

Bontsuk fel az 504-et prímtényezők szorzatára: $504=7\cdot8\cdot9$.

Azt kell bizonyítanunk, hogy $(a^3-1)\cdot a^3\cdot(a^3+1)$ osztható 7-tel, 8-cal, 9-cel. ($a \in Z$).

1. Ha $a=7k$, akkor a kifejezés osztható 7-tel.

2. Ha $a=7k\pm1$, akkor a^3 7-tel osztva 1-et (6-ot),

   ha $a=7k\pm2$, akkor a^3 7-tel osztva 8-at (6-ot),

   ha $a=7k\pm3$, akkor a^3 7-tel osztva 27-et (6-ot) ad maradékul.

   Ez azt jelenti, hogy vagy a^3-1, vagy a^3+1 osztható 7-tel.

3. a^3-1 és a^3+1 közvetlenül egymás után következő páros számok, ha *a* páratlan: szorzatuk tehát osztható 8-cal. Ha *a* páros, akkor $8|a^3$.

4. Ha $a=3k$, akkor a^3 osztható 9-cel, ha $a=3k\pm1$, akkor $a^3=9A\pm1$, tehát vagy a^3-1, vagy a^3+1 osztható 9-cel.

5. feladat

Legyen a, b, c mindegyike pozitív egész szám. Milyenek lehetnek a 3-mal való oszthatóság szempontjából, ha azt akarjuk, hogy $a^2+b^2+c^2$ osztható legyen 3-mal?

Megoldás

1. Ha az a, b, c pozitív egész számok mindegyike osztható hárommal, akkor az $a^2+b^2+c^2$ is osztható vele.

2. Ha az a, b és c pozitív egész számok közül egyik sem osztható hárommal, akkor a=3k±1, b=3m±1, c=3n±1 alakú.

   $a^2+b^2+c^2$ =9($k^2+m^2+n^2$)+6A, ahol A a k+m+n, k+m-n, k-m+n, k-m-n, -k+m+n, -k+m-n, -k-m+n, -k-m-n kifejezések egyikével egyenlő, tehát egész szám: 3|a2+b2+c2.

3. Ha az a, b és c pozitív egész számok közül pontosan egy nem osztható 3-mal, akkor $a^2+b^2+c^2$, 9($k^2+m^2+n^2$)+6B+1 alakú.

4. Ha a, b és c közül pontosan kettő nem osztható 3-mal, akkor a négyzeteik hárommal való osztás utáni maradékainak összege 1+1, 1+4, 4+4 lehet, egyik sem osztható 3-mal.

Ezek szerint az $a^2+b^2+c^2$ akkor és csak akkor osztható 3-mal, ha vagy mind a három adott szám osztható 3-mal, vagy egyik sem osztható vele.

VI. Diofantoszi egyenletek

Történelmi áttekintés

A diofantikus vagy diophantoszi egyenletek elmélete az ókorba nyúlik vissza. Diophantosz, aki kétezer éve Alexandriában élt, már vizsgált olyan szöveges feladatokat, amelyek elsőfokú kétismeretlenes egyenletekre vezetnek, s ezek megoldásait a pozitív egészek körében kereste. Írt is erről egy könyvet.

A görögök már ismerték az úgynevezett pithagoraszi egyenletet, az $x^2+y^2 = z^2$ bizonyos megoldásait. Tudták, hogy ennek a háromismeretlenes másodfokú egyenletnek végtelen sok egész megoldása létezik. Ugyanez az egyenlet az egyiptomiaknál és az indiaiaknál is előbukkan. Az egyiptomiak a derékszögű háromszög megszerkesztésére, derékszög kijelölésére használták, például a piramisépítésnél.

Később évszázadokig ez a kérdéskör csak elszórtan bukkant elő, mígnem a 17. századtól élénk érdeklődés kezdődött a diofantikus egyenletek iránt. Mindez elsősorban Pierre de Fermat és több más matematikus munkásságának volt köszönhető.

Fermat Diophantosz könyvének olvasásakor vetette fel híres problémáját, mellyel csak a közelmúltban birkózott meg a matematikusvilág, pontosabban Andrew Wiles. Fermat azt sejtette, hogy két harmadik, negyedik..., n-edik hatvány összege nem lehet harmadik, negyedik stb. hatvány. Vagyis nincsenek olyan x, y, z pozitív egész számhármasok, melyek kielégítenék az $x^n + y^n = z^n$ egyenletet, ahol n = 3, 4, 5... egész számok valamelyike. Diophantosz könyvének margójára írta: "Csodálatos bizonyítást találtam erre a tételre, de ez a margó túl keskeny, semhogy ideírhatnám." Örök titok maradt, hogy Fermat mire gondolhatott.

Évszázadokon át matematikusok serege próbálta meglelni Fermat feltételezett bizonyítását, igazolni állítását. A sejtés ellenállt a próbálkozásoknak. A matematika sokat köszönhet ezeknek a diofantikus problémáknak, mivel a megoldási kísérletek során olyan módszerek, elméletek születtek, amelyek később igen hasznosnak bizonyultak. Csak egyet említek: Kummer a Fermat-sejtés bizonyítására vonatkozó vizsgálatai során kidolgozta az ideálelméletet, ami termékenyítően hatott az algebra fejlődésére. A Fermat-sejtést 1995-ben

bizonyította be Wiles amerikai matematikus, roppant mély algebrai és számelméleti segédeszközökkel.

Hilbert 1900-ban, Párizsban a matematikus világkongresszuson a 20. század matematikusai számára megoldandó problémákat fogalmazott meg. Hilbert 10. problémája olyan általános eljárás keresését tűzte ki célul, amellyel bármilyen egész együtthatós polinomiális diofantikus egyenletről az együtthatók és a fokszám ismeretében véges sok lépésben eldönthető, hogy megoldható-e az egész számok körében vagy sem.

A harmincas években Gödel és Church kimutatták, hogy a matematikában vannak olyan kérdések, melyek az adott rendszeren belül nem megválaszolhatók. Matijaszevics pedig 1970-ben bebizonyította, hogy nincs olyan univerzális eljárás, amely minden polinomiális diofantikus egyenlet esetén választ adna a megoldhatóságra. Ezzel Hilbert 10. problémájáról bebizonyosodott, hogy megoldhatatlan.

A kétismeretlenes, elsőfokú diofantikus egyenleteket lineáris diofantikus egyenleteknek nevezzük. Általános alakjuk:

$$Ax + By = C, \text{ ahol } A,B,C \text{ eleme } Z\text{-nek.}$$

Könnyen belátható, hogy a megoldás egy szükséges feltétele, hogy az A és B számok legnagyobb közös osztója legyen osztója a C számnak. A baloldal osztható az lnko-val, így a jobboldalnak is oszthatónak kell lennie vele. Egy tétel mondja ki, hogy ez a feltétel már elegendő is a megoldás létezéséhez:

Tétel:

A lineáris diofantikus egyenletek megoldhatóságának szükséges és elegendő feltétele, hogy (A,B) osztható C-vel. A megoldások száma végtelen.

A megoldás módszere egy példában:

Egyenletünk: **26 x - 58 y = 10**

Első lépésként osszunk le a két baloldali együttható lnko-jával, azaz *2*-vel.

$$13x-29y=5$$

Fejezzük ki *x*-et (általában a kisebb együtthatójú) ismeretlent:

$$x=(29y+5)/13=2y+(3y+5)/13$$

Mivel *x* és *2y* is egész, kell hogy

$u=3y+5/13$ is egész szám legyen.

Így $13u=3y+5$ Innen megint a kisebb együtthatójú ismeretlent fejezzük ki:

$$13u-5=3y$$

$$y=(13u-5)/3$$

$$y=4u-1+(u-2)/3$$

Mivel *y* és a *4u-1* kifejezés is egész, ezért a tört is egész számot ad, azaz

$v=(u-2)/3$ is egész szám.

Átalakítva:

3v=u-2

3v+2=u

Ezt az egyenletet már nem kell átalakítani, az *u* együtthatója 1 (ez a kisebb együttható). A megoldásokat úgy kapjuk meg, hogy v értékeit végigfuttatjuk az egész számok halmazán. Mivel mi az *x* és *y* ismeretleneket keressük, ezért az utolsó egyenlet alapján először *y*-t számolhatjuk ki:

y=4u-1+(u-2)/3 =4*(3v+2)-1+(3v+2-2)/3=12v+7+v=13v+7

x=(29y+5)/13=2y+(3y+5)/13=2*(13v+7)+26v*(3*(13v+7)+5)/13+14+(39y+26)/13=29v+16

A megoldások tehát: y=13v+7, x=29v+16, ahol v bármely egész szám lehet.

A megoldások számpárok formájában:

...(-6,-13), (16,7), (45,20)...

az x értékei 29-el, az y értékei 13-al növekednek.

Látható, hogy végtelen sok megoldás van. y a 13-mal osztva 7-et, x a 29-el osztva 16 maradékot adó számok közül kerül ki. Nem véletlen a két megoldás periodicitását adó számok (13 és 29) felbukkanása: az lnko-val való osztás után keletkező együtthatók adják az ismétlődés nagyságát.

Hilbert azt a feladatot tűzte ki, hogy keressünk olyan általános módszert (algoritmust), amely minden egész együtthatós algebrai egyenlet esetén eldönti: van-e annak egész megoldása. Nem gondolt arra, hogy esetleg ilyen módszer nem létezik.

Feladatok

1. feladat

Egy derékszögű háromszög oldalai egész számok. Bizonyítsuk be, hogy ekkor valamelyik oldala osztható 5-tel.

Megoldás

Megmutatjuk, hogy ha egyik befogó sem osztható 5-tel, akkor az átfogó osztható 5-tel.

1. Ha egyik befogó sem osztható 5-tel, akkor ezek négyzete 5-tel osztva csak 1 vagy 4 maradékot adhat.

2. Ha mindkettő 1 maradékot ad, akkor az átfogó $n^2=5k+2$ alakú négyzetszám, így n^2 vagy 2-re, vagy 7-re végződik, ami lehetetlen.

3. Ugyanígy ellentmondásra jutunk, ha mindkét befogó négyzete 5-tel osztva 4 maradékot ad.

Így az egyik befogó négyzete 5-tel osztva 1, a másiknégyzete 4 maradékot ad, vagyis ezek összege – s így az átfogó is – osztható 5-tel.

2. feladat

Egy tál süteményt szeretnénk feldarabolni a téglalap alakú tepsi oldalaival párhuzamos vágásokkal úgy, hogy szeletelés után a tepsi szélével érintkező (kicsit égett) sütemények száma egyenlő legyen a tepsi szélével nem érintkező sütemények számával. Hogyan tehetjük ezt meg?

Megoldás

Legyen a felszeletelt süteményben n oszlop és k sor. Ekkor a sütemények

száma $n \cdot k$. A tepsi szélével nem érintkező sütemények száma $(n-2) \cdot (k-2)$.

A feltételek szerint:

$$n \cdot k = 2 \cdot (n-2) \cdot (k-2),$$

ahonnan

$$n \cdot k - 4 \cdot n - 4 \cdot k + 8 = 0,$$

azaz

$$(n-4) \cdot (k-4) = 8.$$

Innen n= 5, k = 12 vagy n= 6, k = 8. (Természetesen, ha a tepsit elforgatjuk 90_-kal, akkor n és k szerepe felcserélődik.)

3. feladat

Oldjuk meg az egész számok körében az alábbi egyenleteket:

a) $1!+2!+3!+\ldots+x!=y^2$

b) $1!+2!+3!+\ldots+x!=y^z$.

Megoldás:

a) Közvetlen behelyettesítéssel azt kapjuk, hogy x<5 esetén az egyenlet megoldásai az x = 1, y = ±1 és az x = 3, y = ±3 számok lesznek. Megmutatjuk most, hogy x≥5 esetén nincs megoldása az egyenletnek. Vegyük figyelembe ehhez, hogy 1!+2!+3!+4!=33 utolsó számjegye 3; 5!,6!,7!,… utolsó számjegye pedig 0. Ilyen módon x≥5 esetén az 1!+2!+…+x! összeg 3-ra végződik, ezért nem lehet egyetlen y egész szám négyzete (nincs olyan négyzetszám ugyanis, amely 3-ra végződik).

b) Vegyük a következő két esetet:

1.) z=2n páros szám. Ez az eset könnyen visszavezethető az előzőre, mivel $y^{2n}=\left(y^n\right)^2$. Ilyen módon páros *z*-re a következő megoldásokat kapjuk:

x=1; y=±1; ha z tetszőleges páros szám

x=3; y=±3; ha z=2.

2.) z páratlan szám. Ha z=1, az egyenlőség bármilyen x értékre igaz, minthogy $y=1!+2!+\ldots+x!$. Legyen z≥3. Vegyük észre, hogy $1!+2!+\ldots+7!+8!=46233$ osztható 9-cel, de nem osztható 27-tel, n≥9 esetén azonban az n! szám osztható 27-tel; minthogy azonban 1!+2!+…+8! 9-cel osztható, de 27-tel nem, az 1!+2!+…+x! összeg x≥8 esetén osztható 9-cel, de 27-tel nem. Ahhoz, hogy y^z osztható legyen 9-cel, szükséges, hogy y osztható legyen 3-mal. Ekkor azonban

y^z osztható 27-tel (mert z≥3), következésképpen x≥8, z≥3 esetén az egyenlőségnek nincs megoldása az egész számok körében. Meg kell még vizsgálnunk az x<8 esetet. A következő lehetőségek vannak:

$$1!=1=1^z,$$

itt z tetszőleges természetes szám lehet;

$$1!+2!=3,$$

azaz nem egyenlő semmiféle egész szám 1-től különböző természetes kitevőjű hatványával;

$$1!+2!+3!=3^2,$$

továbbá:

$$1!+2!+\ldots+4!=33$$
$$1!+2!+\ldots+5!=153$$
$$1!+2!+\ldots+6!=873$$
$$1!+2!+\ldots+7!=5913$$

A 33, 153, 873 és 5913 számok azonban nem egyenlők egyetlen természetes szám 1-től különböző egész kitevőjű hatványával. Ilyen módon páratlan z esetén a következő megoldásokat kapjuk:

x=1, y=1, z tetszőleges páratlan szám

y tetszőleges természetes szám, y=1!+2!+…+x!, z=1.

4. feladat

Oldja meg a $2\cdot\overline{xyz}+30=x!\,y!\,z!$ egyenletet! (x≠0)

Megoldás

Megvizsgálva az egyenletet:

- Az x, y, z között nem lehet két darab 6-os (6! = 720),
- sem két darab 5-ös (5! = 120),
- sem egy 5-ös és egy 4-es.

- Ha pontosan egy 6-os lenne, akkor 2·600+30=1230 miatt a 720 szorzója csak 1·1 lehetne ($2 \cdot 720 > 1330$),

  6! = 720 azonban nem egyenlő a 6, 0, 0; 6, 1, 1; 6, 1, 0 számjegyek permutálása nyomán nyert háromjegyű számok kétszeresének és 30-nak az összegével.

  Ezek szerint 6-os nem lehet a számjegyek között.

- A háromjegyű szám számjegyeinek mindegyike nem lehet (egyszerre) 3:

  $333 + 20 > 216 = 3! \cdot 3! \cdot 3!$

- A számjegyek között van tehát 4-es, vagy 5-ös. Ez azt jelenti, hogy

  8|x! ·y! ·z!, tehát $8|\overline{xyz} + 30$.

$\overline{xyz}8k+1$, vagy 8k+5 alakú, tehát páratlan.

Ez azt jelenti, hogy ha a számjegyek között 4-es van, akkor csak egy van:

$4! \cdot 4! \cdot 1! = 576 > 441$. (Az egyesek helyén nem állhat 4-es).

Nyilvánvaló, hogy 3|x! ·y! ·z!, tehát $3|2\cdot\overline{xyz} + 30$, továbbá $3|\overline{xyz}$, 3|x+y+z.

Csak az x+y+z=6, és x+y+z=9 eseteket kell vizsgálnunk. 4, 3, 2; 5, 1, 0; 4, 1, 1; 5, 3, 1; 5, 2, 2; esetek felelnek meg, az egyenleteknek csak az 5, 2, 2 számjegyekből létrehozható 225.

5. feladat

Van-e olyan négyzetszám, melyhez 10-et adva ismét négyzetszámot kapunk?

Megoldás

Az $n^2 + 10 = m^2$ egyenlet egész szám megoldását keressük. $m^2 - n^2 = 10$.

Képezzük néhány négyzetszám különbségét:

1 4 9 16 25 36 49

3 5 7 9 11 13

8 12 16 20 24

A felírtak alapján az a sejtésünk, hogy az 1 és minden 4k+2 alakú szám kivételével bármely pozitív egész szám előállítható két négyzetszám különbségeként.

$$m^2-n^2=(m+n)\,(m-n).$$

1. $m^2 - n^2 = 1$ csak akkor teljesülhet, ha $m - n = 1$ és $m + n = 1$, ez lehetetlen adott feltételek mellett.
2. $m = n + 1$ esetén $m^2 - n^2 = 2n + 1$, tehát bármely pozitív páratlan szám előállítható.
3. $(m + n)(m - n)$ akkor és csak akkor páros, ha mind m, mind n
   a. páros,
   b. páratlan.

   $4k + 2 = 2(2k + 1)$, tehát a szorzat egyik tényezője páros, a másik páratlan. Nincs tehát $n^2 + 4k + 2$ alakú négyzetszám, vagyis nincs $n^2 + 10$ alakú sem.

6. feladat

Oldja meg az $x^2+3y^2=x^3-y^3$ egyenletet! ($x \in Z$, $y \in Z$)

Megoldás

$x^2 + 3y^2 \geq 0$, tehát $x \geq y$.

Legyen $x = y + k$ ($k \in N$).

k=0 esetén x=0, y=0 az egyenletnek megoldása.

$$(y + k)^2 + 3y^2 = (y + k)^3 - y^3,$$

$$D = k^2(3k - 2) - 4k^2(3k - 4)(k - 1) \geq 0.$$

Az egyenlőtlenség akkor teljesül, ha

$$\frac{16 - \sqrt{112}}{6} \leq k \leq \frac{16 + \sqrt{112}}{6}. \; 1 \leq k \leq 4.$$

k=1,

$$(y + 1)^2 + 3y^2 = (y + 1)^3 - y^3,$$

$y(y - 1) = 0;$

$y_1 = 0, x_1 = 1; y_2 = 1, x_2 = 2.$

Mindkét (x, y) számpár megoldás.

k=2,

$(y + 1)^2 + 3y^2 = (y + 2)^3 - y^3,$

$y^2 + 4y + 2 = 0$, az egyenletnek nincs racionális gyöke.

k=3,

$5y^2 - 21y + 19 = 0$, az egyenletnek nincs racionális gyöke.

k=4,

$y^2 + 5y + 6 = 0,$

$y_1 = -2, x_1 = 2; y_2 = -3, x_2 = 1.$

Mindkét számpár megoldás.

Az egyenletnek öt megoldása van

VII. egész számok kongruenciája

Definíció

Az a kongruens b-vel modulo m, ha m|(a - b).
Jelölés: a = b mod (m)

Definíció

$a \equiv b \bmod (m)$, ha a és b is m-mel osztva ugyanazt a maradékot adja, azaz $a = mq_a + r_a$, $b = mq_b + r_b$ és $r_a = r_b$.

Megjegyzés:

Az 1. és 2. definíció ekvivalens.

Tételek

1. Az $a \equiv b \bmod (m)$ reláció ekvivalencia reláció.
2. Ha $a \equiv b \bmod (m)$ és $a = a'd$, $b = b'd$ és $m = m'd$, akkor $a' \equiv b' \bmod (m')$.
3. Ha $a \equiv b \bmod (m)$ és $c \equiv d \bmod (m)$, akkor $a \pm c \equiv b \pm d \bmod (m)$ és $ac \equiv bd \bmod (m)$.

Feladatok

1. feladat

a) Adjunk új bizonyítást a 11-gyel való oszthatóság szabályára kongruenciák felhasználásával.

b) Adjunk szabályt egy 12-es számrendszerben föírt szám 13-mal való oszthatóságára.

c) Adjunk szabályt egy 10-es számrendszerben fölírt szám 7-tel, ill. 13-mal való oszthatóságára.

Megoldás

a) Ha egy n számnak a számjegyei (visszafelé haladva) sorra a_0, a_1, … a_k, akkor

$$n = a_k 10^k + \ldots + a_1 10^1 + a_0 \equiv a_k(-1)^k + \ldots + a_1(-1)^1 + a_0 \pmod{11},$$

ami pont azt jelenti, hogy n pontosan akkor osztható 11-gyel, ha a számjegyeinek a váltott előjelű összege osztható 11-gyel.
(Valójában az is kijött, hogy a két számnak még az esetleges maradéka is megegyezik.)

b) Egy szám pontosan akkor osztható 13-mal, ha a 12-es számrendszerben fölírt alakjából kapott számjegyek váltott előjelű összege osztható 13-mal.

c) A 7-tel való oszthatóság ellenőrzéséhez az egyesek, tízesek stb. helyén álló számjegyeket sorra 3-mal, 2-vel, -1-gyel, -3-mal, -2-vel és 1-gyel (majd ugyanilyen sorrendben folytatva tovább ismét 3-mal, 2-vel stb.) kell szorozni, s a kapott számokat összeadni:

az eredeti szám pontosan akkor osztható 7-tel, ha az előbb kapott súlyozott összeg osztható 7-tel. (Persze, az eljárás ismételhető, amíg csak elég kis számot nem kapunk!). A szorzók a megfelelő 10-hatványok maradékaiból adódtak.
Hasonló tényezők a 13-mal való oszthatóság ellenőrzésére: -3, -4, -1, 3, 4, 1, majd a sorozat ismétlődik.

2. feladat

Melyik az a második legkisebb pozitív egész szám, amely 2-vel osztva 1-et, 5-tel osztva 3-at, 7-tel osztva pedig 4-et ad maradékul?

Megoldás

Oldjuk meg az alábbi szimultán kongruenciarendszert:

$$x \equiv 1 \pmod 2,$$
$$x \equiv 3 \pmod 5,$$

$$x \equiv 4 \pmod 7.$$

Az első kongruenciának a megoldásai a

$x = 2k + 1$ alakú számok, ahol k tetszőleges egész szám.

Ezt behelyettesítve a második kongruenciába, a

$2k + 1 \equiv 3 \pmod 5$ kongruenciát kapjuk,

majd ekvivalens átalakítással a

$k \equiv 1 \pmod 5$ kongruenciát.

Ennek megoldásai a $k = 5l + 1$ alakú számok, ahol l tetszőleges egész szám.

k értékét visszahelyettesítve az x kifejezésébe, azt kapjuk, hogy az első két kongruencia közös megoldásai az

$x = 2k + 1 = 2(5l + 1) + 1 = 10l + 3$ alakú számok.

Ezt a kifejezést most a harmadik kongruenciába helyettesíthetjük:

$10l + 3 \equiv 4 \pmod 7$,

s ezt megoldva azt kapjuk, hogy $l \equiv 5 \equiv (4 - 3) = 5 \pmod 7$.

Tehát $l = 7m + 5$, és így $x = 10l + 3 = 10(7m + 5) + 3 = 70m + 53$. Ez azt jelenti, hogy a szimultán kongruenciarendszernek a megoldása az

$x \equiv 53 \pmod{70}$ maradékosztály,

s így a második legkisebb pozitív szám, ami a feltételt kielégíti, a 123.

3. feladat

Megoldhatók-e, s ha igen, mi a megoldásuk az alábbi kongruencia rendszereknek?

a) $9x \equiv 6 \pmod{24}$; $7x \equiv 4 \pmod{66}$;

b) $x2 \equiv 3 \pmod{23}$; $5x \equiv \pmod{11}$;

Megoldás

a) Érdemes észrevennünk az elején, hogy az egyes kongruenciákat még külön-külön meg kell oldanunk, és az első kongruencia megoldásánál a modulus is megváltozik, ahogy első lépésként a

$9x \equiv 6 \pmod{24}$ kongruenciát a

$3x \equiv 2 \pmod 8$ kongruenciává alakítjuk át.

Az első kongruencia megoldása $x \equiv 6 \pmod 8$, melyből a másodikba behelyettesítve a

$7(8k + 6) = 56k + 42 \equiv 4 \pmod{66}$ kongruenciát kapjuk.

Ezt megoldva $k \equiv 17 \pmod{33}$ adódik.

Megoldásként az

$x = 8k + 6 = 8(33l + 17) + 6 = 264l + 142$ alakú számokat,

azaz az $x \equiv 142 \pmod{264}$ maradékosztályt kapjuk.

(Vegyük észre, hogy $264 = [24; 66]$.)

b) Az $x^2 \equiv 3 \pmod{23}$ kongruencia két megoldása az

$x \equiv 7 \pmod{23}$ és $x \equiv -7 \equiv 16 \pmod{23}$,

s ezeket külön-külön kell párba állítani a második kongruenciával, majd megoldani a két rendszert.

Az első rendszer megoldása $x \equiv 30 \pmod{253}$, a másodiké $x \equiv 85 \pmod{253}$.

4. feladat

Adott n pozitív egész számhoz tekintsük azon $A \subset \{1,2,...,n\}$ halmazokat, amelyekben az

$x + y \equiv u + v \pmod{n}$

kongruenciának nincs más megoldása, mint az

$x = u$, $y = v$, illetve $x = v$, $y = u$

triviális megoldások. Legyen $f(n)$ az ilyen halmazok elemszámának maximuma.

a) Bizonyítsuk be, hogy $f(n) < \sqrt{\{n\}} + 1$.

b) Mutassunk példát végtelen sok olyan n-re, amikor. $f(n) > \sqrt{\{n\}} - 1$

Megoldás

a) Tekintsük az A-beli elemek különbségeit modulo n; az x - y és y - x különbségeket különböztessük meg. Ha $|A| = k$, akkor összesen $k(k-1)$ ilyen van, egyik sem 0. Ha valamelyik két különbség megegyezne, akkor azokból nem triviális megoldást kapnánk.

Ezért $k(k-1) \leq n-1$, amiből $k \leq \frac{1}{2} + \sqrt{n - \frac{3}{4}} < \sqrt{n} + 1$.

b) Legyen p tetszőleges prímszám és n=p(p-1), legyen továbbá g egy primitív gyök modulo p. Az A halmaz álljon azokból az x számokból, amelyekre $x \equiv g^x \pmod p$. Először is bebizonyítjuk, hogy a modulo n maradékosztályok között pontosan p-1 ilyen van.
Legyen r egy tetszőleges, 0-tól különböző maradék modulo p, és keressük az $x \equiv r$, $g^x \equiv r \pmod p$ kongruenciarendszer megoldásait. Az x számot az $x \equiv r$ kongruencia meghatározza modulo p, a $g^x \equiv r$ kongruencia pedig meghatározza modulo (p-1). Mivel p és p-1 relatív prímek, a kínai maradéktétel szerint a megoldások az egyik modulo p(p-1) maradékosztály elemei.

Konkrét példa: Legyen p=7, n=42 és g=3. (A 3 primitív gyök modulo 7, mivel a 3 hatványai 7-tel osztva minden 0-tól különböző maradékot kiadnak: $3^0=1$, $3^1=3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$ és $3^5 \equiv 5 \pmod 7$.) Az $x \equiv 3^x \pmod 7$ kongruencia megoldásai az alábbi táblázatban vannak összefoglalva:

r	$3^x \equiv r \pmod 7$ megoldása	$x \equiv r$, $3^x \equiv r \pmod 7$ megoldása
1	$x \equiv 0 \pmod 6$	$X \equiv 36 \pmod{42}$
2	$x \equiv 2 \pmod 6$	$X \equiv 2 \pmod{42}$
3	$x \equiv 1 \pmod 6$	$X \equiv 31 \pmod{42}$
4	$x \equiv 4 \pmod 6$	$X \equiv 4 \pmod{42}$
5	$x \equiv 5 \pmod 6$	$X \equiv 5 \pmod{42}$
6	$x \equiv 3 \pmod 6$	$x \equiv 27 \pmod{42}$

Az A halmaz elemei tehát: 2,4,5,27,31,36.

Végül megmutatjuk, hogy az A halmaz eleget tesz a feltételeknek.
Mint láttuk, az A halmaz elemei páronként különbözők modulo p. Tetszőleges $x,y \in A$ esetén az x+y érték meghatározza a szorzatot is modulo p, hiszen $xy \equiv g^x g^y \equiv g^{x+y}$. Ha tehát ismerjük x+y-t, akkor meghatározhatjuk xy-t is modulo p, és felírhatunk egy modulo p másodfokú egyenletet, amelynek két gyöke x és y. A másodfokú egyenlet pedig - a sorrendtől eltekintve - egyértelműen meghatározza a gyökpárt.
Ha tehát ismerjük x + y értékét, akkor x és y értékét is meghatározhatjuk modulo p; ez pedig meghatározza magát a két elemet is.

Az előbbi példában tegyük fel, hogy azokat az x,y elemeket keressük, amelyekre

$$x + y \equiv 16 \pmod{42}.$$

Ekkor

$$x + y \equiv 2 \pmod 7 \text{ és } xy \equiv 3^{16} \equiv 4 \pmod 7.$$

Az x és y számok tehát a

$$t^2-2t+4 \equiv 0 \pmod 7 \text{ kongruencia gyökei.}$$

Mivel

$$t^2-2t+4 \equiv (t-3)(t-6) \pmod 7,$$

az x, y számok egyike 7-tel osztva 3-at ad maradékul a másik pedig 6-ot. Az egyik szám tehát a 31, a másik a 27.

A bemutatott konstrukcióban n = p(p-1) és |A|=p-1, ezért $f(n) \geq p-1 > \sqrt{n}-1$.

Végtelen sok olyan n-et sikerült tehát találni, amikor $f(n) > \sqrt{n}-1$.

VIII számelméleti függvények

A nem zérus természetes számok halmazán értelmezett függvényeket számelméleti függvényeknek nevezzük.

Definíció

Az f(n) számelméleti függvényt multiplikatívnak nevezzük, ha f(ab) = f(a)f(b), $\forall$ (a,b)=1. Ha az f(ab) = f(a)f(b) összefüggés tetszőleges a, b természetes számok mellett is érvényes, akkor a függvényt totálisan (teljesen) multiplikatív függvénynek nevezzük

Definíció

A g(n) számelméleti függvényt additívnak nevezzük, ha g(ab) = g(a) + g(b) $\forall$ (a, b) = 1. Ha a g(ab) = g(a) + g(b) összefüggés tetszőleges a, b természetes számok mellett is érvényes, akkor a függvényt totálisan (teljesen) additív függvénynek nevezzük.

Példák

multiplikatív függvényre: $f(n)=(-1)^{n+1}$
totálisan multiplikatív függvényre: $f(n)=n^c$, c konstans
additív függvényre: $1+(-1)^n$
totálisan additív függvényre $g(n)=c\cdot\log n$

Nevezetes számelméleti függvények:

1. φ(n) jelenti az 1, 2, …,n számok közül az n-hez relatív prímek számát. A φ(n) függvényt Euler-féle φ függvénynek nevezzük.

   Tulajdonságok:

   φ(1)=1
   Ha p prím, akkor φ(p)=p-1.
   Ha p prím, akkor $f(p^{\alpha})= p^{\alpha}-p^{\alpha-1}$.

2. d(n) jelenti az n∈N összes pozitív osztóinak számát.
3. σ(n) jelenti az n∈N pozitív osztóinak az összegét. Ha σ(n)>2n, akkor bővelkedő számról, ha σ(n)<2n, akkor szűkölködő számról beszélünk.

4. Moebius-féle μ(n) függvény: $\mu(n)=\begin{cases}1, n=1\\ (-1)^r, n=p_1\cdots p_r\\ 0, egyébként\end{cases}$, $p_i\neq p_j$.

5. χ(n) jelenti az n∈N összes különböző prímtényezőinek a számát.

6. ν(n) jelenti az n∈N összes különböző prímtényezőinek a számát multiplicitással együtt.

Tétel (Euler-Fermat tétel)

Ha (a,n)=1, akkor $a^{\varphi(n)}\equiv 1 \bmod (n)$.

Tétel (Kis Fermat-tétel)

Ha p prím és pła, akkor $a^{p-1}\equiv 1 \bmod (p)$ vagy (egy másik alakja a Kist Fermat-téetelnak $a^p\equiv a \bmod(p)$.

Feladatok:

1. feladat

A nevezetes számelméleti függvények értékeit határozzuk meg az n=2000 helyen.

Megoldás

$n=2000=2\cdot 10^3=2^4\cdot 5^3$

$\varphi(2000)=2000\cdot\left(1-\frac{1}{2}\right)\bullet\left(1-\frac{1}{5}\right)=800$

$d(2000)=(4+1)\cdot(3+1)=20$

$\sigma(2000)=\frac{2^5-1}{2-1}\cdot\frac{5^4-1}{5-1}=4836$

$\chi(2000)=2$

$\nu(2000)=7$

$\mu(n)=0$

2. feladat

Határozzuk meg azon m, n Є N*, (m,n)=1 természetes számokat, amelyekre

$$\varphi(m\cdot n)=\varphi(m)+\varphi(n)$$

Megoldás:

Mivel (m,n) = 1, az egyenlet egyenértékű a következő egyenletekkel:

$$\varphi(m\cdot n)=\varphi(m)+\varphi(n)$$

$$\varphi(m)\cdot\varphi(n)=\varphi(m)+\varphi(n)$$

$$\frac{1}{\varphi(m)}+\frac{1}{\varphi(n)}=1$$

Nyilvánvaló, hogy $\varphi(m)\neq 1$.

Ha $\varphi(m)>2$, akkor

$$\frac{1}{\varphi(m)}+\frac{1}{\varphi(n)}<\frac{1}{2}+\frac{1}{2}=1$$

Következik, hogy $\varphi(m)=\varphi(n)=2$, ahonnan m,n Є{3 ,4, 6}. Ezen számok közül csak a 3 és 4 relatív prímek, így az egyenlet megoldásai:

m = 3, n = 4, illetve m = 4, n = 3.

Irodalomjegyzék

1. Ambrus András: Bevezetés a matematikadidaktikába
2. Bakos Tibor, Lőrincz Pál, Tusnády Gábor: Középiskolai matematikai versenyek 1973-74
3. Bege Antal, Demeter Albert, Lukács Andor: Számelméleti feladatgyűjtemény
4. Dr. Gerőcs László, Orosz Gyula, Paróczkay József, Szászné Simon Judit: Matematika
5. Freud Róbert – Gyarmati Edit: Számelmélet.
6. Kántor Sándorné – Sümegi László: Elemi matematika II.
7. Obádovics J. Gyula: Matematika.
8. Surányi János: Bevezetés az algebrába és a számelméletbe.

Elektronikus kiadványok, jegyzetek:

www.om.hu

www.elte.hu

www.sulinet.hu