HATVÁNYÖSSZEGEK ELMÉLETE

IV. KÖTET
A FERMAT SEJTÉS TÖRTÉNETE

Szerző: Forrai György

Budapest 2009.07

TARTALOM

1 A „Fermat sejtés” története (másképpen...)

Ez az írás nem tudományos igényű - nem is lehetne az...

Csupán a Fermat sejtésről szóló, korába visszavetített, elképzelt történet, kommentárokkal, amely kerüli a mára vonatkozó utalásokat.

Mert ma már nem lenne helyénvaló *tudományos címkével*, valamely elkésett, egyszerű megoldással előhozakodni.

Hiszen a sejtést a kor nyelvén már megfogalmazták, és a legmagasabb szintű módszerekkel be is bizonyították - tétellé vált! Ami tehát nem valamely történet, hanem történelem.

Amelyet A. Wiles úr írt, s így leghitelesebben az Ő művéből ismerhető meg.

Vagy az arról szóló, a szélesebb olvasói kör részére készült, részben szintén történeti, részben ismeretterjesztő művekből.

Idézek egy kapcsolódó magyar nyelvű kiadványból:

„...Az új kérdéseket már nem értené meg egy tízéves gyerek. A műkedvelők ideje lejárt...”

Mert Fermat ideje óta több száz év telt el. A matematika nagy léptekkel haladt útján előre, hogy máig az átlagos emberi gondolkodással ellenőrizhetetlenül nagy távolságba jusson.

Baj ez, vagy nem? Nem baj, de azért elgondolkoztató!

Mert érteni akarunk, és sok minden mást értünk is, egyre jobban. És próbálunk továbbra is a magunk szintjén mindent megérteni.

De az, hogy valaki a csúcsot már meghódította, nem ok arra, hogy mások annak a közelébe se merészkedjenek! Sőt - hadd gyakoroljanak - egyiküket tán új csúcsok eléréséhez segítheti!

Emiatt a FERMAT sejtés története sem kell, hogy befejeződjön, hanem tovább kereshetők, újabb megoldások, hogy az Ő története is folytatódhasson.

Pontosan emiatt **nem tehető** még most sem **pont a végére**

Lám - az előző mondat végén is szinte kiáltóan hiányzik a pont (vagy bármely más írásjel), de mégsem szeretném, hogy azt valaki kijavítsa! Mert most paradox módon éppen ennek - a (kivételesen szándékosan tett) - hiánynak a pótlása okozna információvesztést!

1.1 A Fermat sejtés felírásai

A Fermat sejtésnek ugyanis számtalan sok eltérő interpretációja létezik, a világ minden nyelvére lefordítva.

(1) Az **EREDETIT** Fermat egy könyv - Diofantosz: Aritmetika - szélére jegyezte le.

Érdekes, sőt feltételezhetően fontos is lenne olvasni a sajátkezű bejegyzését, amely azonban sajnálatos módon már nem található.

Számunkra azonban mégsem érdektelen, ha célunk valóban pontosan azt bizonyítani! Ez indokolja a próbálkozásokat, hogy azt rekonstruáljuk.

(2) Az eredetiben ugyanis sejthetően legalább egy **mondatvégi ponttal kevesebb volt**, mint az első, kiadott **másolatéban.** Mert annak utolsó mondata eléggé ráutalóan a *nem befejezhető*, a *vég nélküli* **végtelenről** szólhatott, ami a sejtés egy lehetséges, éppen Fermat „felírásából" következő megoldása. És egy olyan „játékos" utalás a befejezetlenség, a „végtelenség" jelzésére, mint a **mondatvégi pont elhagyása -** a szerző hisz abban, hogy éppen mint neki, másnak is eszébe juthatott! Mert ugyanakkor, mint a korábbi példájából is kitűnik, az ilyen hiány roppant feltűnő, sőt nyugtalanító! Persze ez nem fontos - de mégis a lényeget illető feltevés. Ami tudományos műben le sem írható, de történetben...

Idézzük tehát a latin nyelvű másolatot az eredeti nyomtatott műből, majd egy internetes forrásból is.

Az eredeti (nyomtatott másolat):[1]

„Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet(,)"

Vagy egy másik, amely csak kicsit más...

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caparet.

Nem hibáztatható a másoló, hogy kötőjellel szétválasztott túl hosszú szavakat - az újabb nyelvi szabályok különféle szempontból előírhatnak efféle tagolást? Vagy a régiek is előírták, csak éppen FERMAT nem tartotta be a szabályokat? Nahát...tanult ember, éppen jogász létére hogy nem félt a büntetéstől? Az viszont már eléggé feltűnő, hogy az „...est dividere; cujus..." közé pontosvesszőt tett - Fermat nyilván itt is tévedett, úgy tűnik, eléggé „felületes" volt a mondattagolásnál! (Mert ha nem Ő, akkor talán mi?) Vagy éppen azzal is jelezni szándékozott valamit? Hiszen tényleg, eléggé „zavartnak" tűnik úgy, legalább egy vessző nélkül!

De nézzünk más, az interneten, és az irodalomban is gyakran szereplő, még jobban eltérő változatot is:

„Cubem autemin duos cubos, aut quadratoquadrum in duos quadratoquadros, et generaliter nullam in infinitum ultra quadrantum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet."

Mint látható, elvétve még találhatók bennük azonos latin szavak, ám a mondatrészek tagolása, s ezáltal hangsúlyozásuk - alapvetően eltérő! Egyébként az utóbbi változat igen elterjedt. Mikor keletkezett, kinek vált ezáltal érthetőbbé a leírás, ami így viszont alapvetően megváltoztatja az értelmezést? Mert vegyük észre, hogy Fermat talán nem véletlenül választhatta a saját, meglehetősen logikátlannak tűnő mondat-tagolását, ami másoknak később joggal bánthatta is a „jó ízlését". Valószínűsíthető, hogy ő az első mondatban csupán a sejtést szándékozhatott ismertetni, jelezve még, hogy talált rá egy csodálatos bizonyítást is, amelyet viszont a második mondatban ismertetett. Teljesen logikus, és „rávezető elképzelése volt ez, amelyet azonban alapvetően felborított a mondatrend későbbi „jószándékú kiigazítása".

[1] Simon Singh: „A nagy FERMAT sejtés" könyvében szereplő másolatot tekintjük az első ismert nyomtatott leírásnak.

Ami azért is érdekes, mert az eredeti, és az eltérő, módosított felírások az adott esetben ugyanazon könyvben is, egymástól néhány oldalra szerepelnek, ráadásul mind a kettő latinul... Mi igazolhatja ezt a latinból -latinra fordítást?

De nemcsak ebben fedezhetők fel a későbbi jószándékú javítások nyomai. Mert az is feltűnő, hogy amíg az „eredeti másolat" végén lévő, igencsak bizonytalan, mondatvégi jel alig hasonlít a „Hanc" szót megelőző, karakteres pontra, addig az internetes változat végén már egyértelműen „pont" látszódik. Határozott, megingathatatlan pont, ahogyan annak a nyelvtan, a helyesírás szabályai szerint lennie kell! Mert egyetlen lektor, szerkesztő vagy szedő sem engedélyezné a mű kinyomtatását anélkül a pont nélkül (ezt a szerző egyszer ki is próbálta), holott pontosan ez az eset volt az, amikor a szabályt ignorálniuk kellett volna!

Megjegyezhető, hogy amíg például az „egypont" (.) a befejezettséget, addig a „hárompont" (...), vagy egy vesző is (,) éppen a befejezetlenséget jelöli, amely azonban lehet valamely véges dolog befejezetlensége is.

Ám mivel jelezhető szintaktikailag a befejezhetetlen „végtelenség"?

Talán magának az írásjelnek, a pontnak az elhagyásával? Ami voltaképpen nagyon meglepő, és figyelemfelkeltő! Szinte elképzelhetetlen, hogy Fermat a habitusának megfelelően az eredeti bejegyzésében ezt a „közlési lehetőséget" ne használta volna ki, hiszen a végrendelete végén sincs pont...Feltehetően tudatosan cselekedett így, hiszen ha nincs mondatvégi pont, akkor annak mondanivalója a végtelen! Legyen az valamely szám, vagy az élete? Mi már persze tudhatjuk, Fermat a végrendeletében sem tévedett - az Ő szelleme és neve már múlhatatlanul létező.

Nehéz persze összeszedni azokat a kis múlt-szilánkokat, amelyek mindezt hitelesen igazolhatnák.

A bemutatott változtatások azonban így is meglehetősen szabados értelmezését bizonyítják egy nagy matematikus szellemi örökségének, sejtetve, hogy azoknak lehetett közük az elmúlt százévek sikertelen kereséseihez. Továbbá egy még annál is sokkal fontosabb információvesztéshez, amelyről majd később lesz szó.

Ám maguk a fordítások túltesznek az előbbieken is.

Internetes (a könyvi fordítással azonos) változat:

Lehetetlen egy köbszámot felírni két köbszám összegeként, vagy egy negyedik hatványt felírni két negyedik hatvány összegeként; általában lehetetlen bármely magasabb hatványt felírni két ugyanolyan hatvány összegeként. Igazán csodálatos bizonyítást találtam erre a tételre, de ez a margó túlságosan keskeny, semhogy ideírhatnám.

Nagyon lendületes a fordítás, ám kevés köze van a latin eredetihez. Mert ebben a fordításban meg sem jelenik a végtelen (infinitum szó), a marginis pedig egyáltalán nem biztos, hogy margót, hanem korlátozó lapszélt, határt is jelenthet - átvitt értelemben annak a határtalanságnak a jelzését, amely nem helyezhető ott el, ami a bizonyítása lényege.

Mert az eredeti szöveg fordítása szerkezetileg helyesen két részből kellene hogy álljon (szintén nem szó szerint):

- A tétel felvezető részéből (első mondat): *...amelyre igazán csodálatos bizonyítást készítettem.*

- A tétel bizonyításából (második mondat): *a rendelkezésre álló hely kicsi a megoldás felírására,*

LEHETETLEN (LEÍRNI) ... MERT ... A HELY TÚLSÁGOSAN KESKENY!

Szándékosan nem használom a képiesebb „margó” szót, mert az megvezetné a gondolkodást, és elrejtené a szó másodlagos jelentést, amely pedig eléggé nyilvánvaló utalás arra - hogy olyan bizonyítást kell keresni, amely:

BEFEJEZHETETLEN, vagyis **VÉGTELEN**!

(A végtelen efféle értelmezése nem lehetett korszak-idegen!)

Mindenesetre túl sok „véletlen” történt a sejtés körül - Fermat eredeti bejegyzése eltűnt, a nyomdai változatban bizonytalan írásjelet tettek oda, ahol feltehetően nem volt - majd mindez saját életet élve a mondatrenddel együtt később is megváltozott - nagy csoda lenne mindezek után, ha valóban azt keresték, és találták volna meg, amire Fermat valójában gondolt.

Másfelől az efféle „nyomozások” valahogy nem illenének egy tudományos műbe, azonban ez (szerencsére?) - nem az! És mint a továbbiakban érzékeltetni szándékozunk, a hasonló, szinte észrevehetetlen módosítások fokozták le századokon keresztül Fermat tételét „sejtéssé”, illetve hoztak létre egy másik sejtést, amit bár másképpen ugyan, de végül bizonyítani lehetett.

(3) Fermat tehát szövegesen fogalmazott, képlet nélkül. Ráadásul az eredeti felírás sem őrződött meg, s így az ismertetett feltevés „pontja” már soha nem igazolható - másféle, logikai bizonyítás szükséges.

Persze a problémát minden érdeklődő valahogyan, legfeljebb kicsit másképpen „megértette”, újrafogalmazva felírta, és vizsgálta.

Nincs tehát abban sem kivetnivaló, hogy a szerző is másképpen megpróbálta. Legfeljebb vitatható az állítása, hogy az eredetihez jobban igazodóan.

A hatványösszegek **oszthatóságának** vizsgálatakor merült fel ugyanis az a „formula”, amelyet Fermat eredeti-másolati megfogalmazásához leginkább közelinek talált, és amelynek a bizonyítását a továbbiakban ismerteti:

„Lehetetlen felírni az $a^p + b^p - c^p = 0$ ***azonosságot p>2 prímszám kitevő esetén nullától eltérő természetes összetett relatív prímszám változókkal, mert azok minden osztójához igazolható lenne további, náluk nagyobb prímszámosztó.”***

Itt láthatólag együtt van a vélt „eredeti felírás”:

„LEHETETLEN FELÍRNI - MERT VÉGTELEN SOK SZÁMBÓL ÁLL”

Ez tehát olyan, mintha azt mondanánk „nem fér el a lapszél korlátolt helyén, röviden a margón.

Ennek bizonyítását próbálja a szerző bemutatni, a matematikai-logika eszközeivel is.

(Megjegyzendő, hogy a „mondatvégi pont” történeti szerepe csak e bizonyítás után merült fel - mint érdekesség - és nem megfordítva - hogy „generálta azt...)

(4) Végül a Fermat sejtés bármely úton történő bizonyításának sokféle következménye van, és közülük bármelyik szolgálhatna valamely új változata felírásának alapjául.

Például a hatványösszegek elmélete alapján is könnyen belátható, hogy a tétel létezése esetén:

„Nem írható fel természetes számok ($x_1;x_2;x_3$) p>2 prímszám hatványából ($X= x^p$) a következő harmadfokú egyenlet":

$\mathbf{X}^3+q_{2*}\mathbf{X}-q_3=0$

Hiszen $q_1=X_1+X_2 - X_3= x_1^p + x_2^p - x_3^p$ nem lehetne nullával egyenlő!

Nyilvánvaló tehát, hogy az adott esetben a harmadfokú egyenlet megoldó képletének sem lehetnének ilyen, természetes szám megoldásai!

Vagyis, hogy erre az esetre a harmadfokú egyenlet ebben az alakban fel sem írható, és meg sem oldható. Amire jelenleg nincs semmiféle tiltó szabály, pedig a ma már bizonyított képletből következik! Valami nincs rendben már a matematika alapjainál, csak nehezen észlelhető, vagy talán nem szívesen látnánk meg?

Mindenesetre a sejtés az előző módon is megfogalmazható, és lám - egészen más következtetést is eredményez!

Létezhetnek tehát ugyanazon problémára eltérő megfogalmazások - egyfajta különálló „bizonyítási formulák". Mintha különféle irányokból szeretnénk valamely hegyre feljutni, vagy mást keresnénk ott. Van aki a látványt, van aki egy követ... Így azután hiába azonos a csúcs, az élmény: egészen más!

Ha tehát valamely probléma „általánosan" lett megfogalmazva vagy értelmezve, akkor azt elvileg sokféleképpen lehet bizonyítani. Hiszen csak az úticélt szabják meg, az elérési utat nem. Erre példaként akár a tévesen értelmezett Fermat sejtés is szolgálhatna, amelyre eltérő parciális bizonyítások sora született, amelyek között bármiféle kapcsolat nehezen lenne fellelhető.

Azonban fel lehet írni a sejtést úgy is, hogy az a megoldások körét - a megközelítés irányát korlátozza! Az olyan felírás, amely utal a megoldás elvárt útjára is, nevezhető „bizonyítási formulának". És Fermat eredeti felírása minden bizonnyal *nem általános* volt, hanem megoldási útjában korlátozott, *bizonyítási formula*. Hiszen olyan úton való közelítést „sejtetett", amelynek végén a befejezetlenség, a végtelen, a megismerhetetlenség várakoztak.

Azonban a számok, az egyenletek, a problémák felírásának sokféle *szempontja, és korlátja* lehetséges még, amelyről a mai ismereteink nem szólnak.

Amiről egy másik „történetben" szintén lenne mit mondani...

1.2 A „Fermat sejtés" vizsgálatának elvei

A Fermat sejtés elsődlegesen korának (XVII. század) ismeretei és felfogása szerint vizsgálható!

Tekintsük tehát a vélhetően a korabeli ismeretszinten is értelmezhető következő (kicsit részletesebb) felírást:

„Lehetetlen az $a^p+b^p-c^p=0$ ***azonosságot p>2 prímszám hatvány esetén nullától eltérő természetes (összetett, relatív prímszám) változókkal felírni, mert azok minden osztójához igazolható valamely nagyobb*** d_n ***prímszámosztó, s így NEM FELÍRHATÓ!"***

Valamelyest persze eltér az előbbi lefordított másolatétól, de tartalmilag eléggé jól közelíti! Mert Fermat egyértelműen utalt arra, hogy milyen megoldásra gondol, sőt a szerző szerint tulajdonképpen le is írta azt.

Felmerülhet a kérdés, hogy vajon Fermat miért pont ezt a bizonyítási utat választotta?

Csupán találgatható (mint itt minden...) hogy azért, mert az irracionális számok már régóta ismertek voltak! És így tudható volt az is, hogy a kérdéses azonosság **irracionális** számokkal könnyen kielégíthető. Például felírható:

$2^3+3^3-(\sqrt[3]{35})^3=0$ **1./**

Ahol $\sqrt[3]{35}$ természetesen irracionális szám, amelyet ha le szeretnénk számjegyekkel írni, szintén „**nem férne el a margón**”. De ez egyfajta „triviálisnak” mondható bizonyítás csupán.

Fermat kezdetben természetes egészekkel felírhatót szándékozhatott bizonyítani, de nem talált ilyeneket. Vizsgálatai során viszont azt tapasztalhatta (ahogyan szerző is), hogy csakis olyan, természetes egészekből álló megoldások lehetségesek, amelyek ugyanolyan végtelenül „nagyok”, és rendezetlenek, mint a végtelen nem szakaszos törtek. Vagyis hogy azok sem írhatók le, vagy jelezhetők csupán számokkal, s így nem férnének el a lapszélen!

Ekkortájt feltételezhetően még a VÉGTELEN másfajta, köznapibb értelmezése is elfogadott lehetett. Ezért, ha valamely növekvő számsorozat számjegyekkel nem volt befejezhető, nem volt vége - pontosabban a ***végére nem lehetett pontot tenni*** *(aminek eredeti „jelölésében”, vagyis a pont elhagyásában nagyon hiszek)* akkor az „befejezetlen, végnélküli-végtelen” volt, és nyilvánvalóan nem férhetett el valamely szokásos könyv margóján, szokásosan felírva.

Így Fermat voltaképpen csak az azonosság korábban is ismert irracionális törtszám megoldásainak már létező **felírási ellehetetlenülését** egészítette ki valamely egész számokéval.

Sőt tovább gondolva - valójában azt ismerhette fel, hogy **irracionális számok értelemszerűen nemcsak végtelen nem szakaszos törtek, hanem végtelen nem rendezett (=nem szakaszos) egész számok is lehetnek**!

Mert a vizsgálatai során megmutatkozott, hogy a **nem rendezhető,** vagy **szakaszosan nem ismétlődő egész számok végtelen sokaságának** felírása is éppen olyan **irracionális (=ésszerűtlen, kivitelezhetetlen)**, mint a végtelen törteké.

Így hát most már bármennyire is furcsának, és szükségtelennek tűnik a megállapítás**, de az *irracionalitás* nemcsak a tizedesvessző jobb, hanem a bal oldalán is jelen lehet!** Mert e tekintetben nem azt a tulajdonságot tartjuk igazán irracionálisnak, hogy valami végtelen. Pedig önmagában az is annak tekinthető, de valahogy azzal mégis inkább kibékülünk, hiszen a végtelen szakaszos törteket is racionálisnak tekintjük.

Hanem irracionálisnak úgy tűnik, főképpen azt tartjuk, ami **nem rendezett**! És az egész számok sorozata éppen ugyanúgy lehet rendezett, pld, szakaszosan ismétlődő: a=123123123..., mint rendezetlen. (A továbbiakban a számsor végén: **...** az egészek szakaszos végtelen ismétlődését jelenti.) S egy ilyen ismétlődéses szám e tekintetben csupán annyiban különbözik egy végtelen szakaszos törtszámtól, hogy nem tört, hanem egész. De mert e körülménynek láthatólag ma nincs semmilyen elméleti, vagy gyakorlati jelentősége, nem is tárgya a számok osztályozásának. ***Irracionális egész szám***? Igen, ráadásul többféle formában. Hiszen az előző példa még olyan esetre vonatkozott, amikor a számsor első ismétlődése ismert volt. De mint bizonyítjuk majd, a Fermat sejtés „megoldásainál” az első rendezett számcsoport sem leírható.

Íme egy szám (a=...), amely ugyan létezik, azonban helyiértékkel egyetlen számjegye sem jegyezhető le, vagyis nem megismerhető! Olyan, mint egy láthatatlan emberről készült fénykép!

Pedig a **véges-végtelen**, úgy is mint **zárt-nyitott, korlátlan, vagy korlátozott (határolt)** szinte minden természeti tudományágban problémaként megjelennek. Azonban most nem is ez a fő kérdés, hanem az, hogy **rendezett,** vagy **rendezetlen**, vannak e **ismétlődő mintázatai,** vagy **nincsenek**, vagyis hogy **racionális,** vagy **irracionális, megismerhető**, vagy **nem**?

Hol válik el a rész, és az egész? Hiszen ha rendezettek, sokszor nehéz szétválasztani őket.

Tekintsük például a következő, egyszerű példát:

...12,12...

Itt egy olyan „racionális”(?) számot írtunk fel (a 10-es számrendszerben), amely nemcsak a tört, hanem az egész számok irányába is ismétlődve halad. És ezt annak ellenére tudtuk így felírni, hogy mindkét irányba végtelen! De mert **szakaszosan rendezett**, elég volt valahogyan jelölni hogy ezek a szakaszok végtelenszer ismétlődőek.

Mi történik most, ha ezt a számot 100-nak valamely hatványával szorozzák, vagy osztják? Láthatóan semmi. Mert az **egész** pont olyan, mint a **rész**... És nem változna semmit a „mintázata”, (csak értéke) akkor sem, ha 2-vel, sőt 4-gyel szoroznánk.

Ha viszont 10, vagy 11-gyel? Akkor milyen „mintázatot” adna?

Vagy egy még szélsőségesebb kérdés - hogy valamely értelemben - talán nem is szorozható?

A tizedes vesző jobb oldala utáni végtelen nem szakaszos tizedes törteknek van osztályba sorolása: irracionálisak.

Ha azonban a bal oldala áll ilyen végtelen, nem szakaszos egész számokból, akkor azt ne különböztessük meg?

Ha valamely tudományág „fősodorvonalán” kívül hasonló kérdés felmerül, általában gyorsan felejtődik is. Hiszen a terminológia csak másodlagos kérdés, amelynek gyakorlati fontossága gyakran eltörpülhet például akár egyetlen szükséges százalékszámítás elvégzése mögött is...

Másfelől a tudományágak fejlődését terminológiájuk általában követi, mintegy reprezentálva annak tartalmát, és közvetve megmutatva még azt is, hogy mely irány nincs a „fősodorban”...

Fermat feltehetően **sejtésével** és **tételével** túllépett a fenti „terminológiai kérdésen”, meglátva a két bizonyítási út (**irracionális tört**, és **irracionális egész**) azonosságát. Hogy tételét ezt követően kidolgozhassa, nem kellett többszáz évnyi „fejlődést megsejtenie”.

Szerző is belátja, hogy vitatható feltevések ezek, amelyeket magának kell megmagyaráznia, bizonyítania...

Mert a későbbi korok matematikusai új úton indultak el, és az ismeretek „ollója egyre nyílt”.

És a végtelen, rendezetlen egészek problematikája - úgy tűnik - nem vált eléggé hangsúlyossá ahhoz, hogy a terminológiában is tükröződjön. Így idővel mind nagyobb nehézséget okozott már nemcsak a bizonyításnak, de magának a sejtésnek is a kor nyelvére való „lefordítása” is.

Következésképpen - ha most a Fermat sejtés vélt bizonyítási formuláját szándékozunk vizsgálni, akkor visszalépve korába azt kellene bizonyítanunk, hogy *ha az azonosságot bármely p >2 prímre próbálnánk felírni, akkor az csak olyan egész értékű relatív prímszám változókkal történhetne meg, amelyek nem befejezhető, végtelen hosszú rendezetlen „irracionális” egészszámokból állnának*, sorrendjük se ismert, s így valamely szokásos könyv szokványos szövegeként **nem lehetnének felírhatók**.

Szokatlan, és nehezen megválaszolható „formula”, bizonyítási út ez.

A hatványösszegek elmélete azonban a Fermat sejtés újszerű vizsgálatát teszi lehetővé azáltal, hogy az algoritmussal bármely fokszámú hatványösszegek között összehasonlítás, osztható-sági vizsgálat, a közös osztó meghatározása könnyebben és áttekinthetőbben elvégezhető.

A következőkben az I-III kötetekben bemutatott és bizonyított jelöléseket, és összefüggéseket alkalmazzuk.

Fermat sok időt töltött hasonló vizsgálatokkal, lehetetlen, hogy elment ilyen összefüggések mellett!

1.2.1 A Fermat azonosság vizsgálata

A bizonyítási formulának megfelelően a vizsgálat során arra kell törekedjünk, hogy olyan összefüggéseket találjunk, és bizonyítsunk, amelyek vagy a hatványösszeget, vagy annak összetevőit, elsősorban magukat a változókat közvetlenül, vagy közvetve növelik!

Így nyilván oszthatósági vizsgálatokat kell majd végezzünk, amire a hatványösszeg elmélet algoritmusai igen alkalmasak.

1.1 Tételezzük fel, hogy a következő azonosság természetes relatív prím számokkal felírható:

$$Q_3^p = a^p + b^p - c^p = 0 \qquad \textbf{2./}$$

Csak emlékeztetőül:

- a felső index (p, és később m) a hatványösszeg fokszáma
- az alsó index: 3 (később 3’) a változók száma az alap, és a módosított (3’) felírások esetén.

1.2. Most képezzünk egy **módosított**, látszólag elsőfokú azonosságot az

$A = a^p$, $B = b^p$; $C = c^p$ szintén módosított változókkal:

$$Q_{'3}^1 = A+B-C=0 \qquad \textbf{3./}$$

1.3. A továbbiakban ezt véve alapul, képezzünk az A;B;C változókból m=2n+1 fokszámú hatványösszegeket, ahol $2<m<\infty$ páratlan szám.

$$Q_{'3}^m = A^m + B^m - C^m = g * q_3^{'} * q_2^{'z} * P_m \qquad \textbf{4./}$$

Ahol:

$q_1^{'} = A+B-C=0$ (elsőfokú módosított paraméter, itt nulla) **5./**

$q_2^{'} = A*B-C*A-C*A$ (másodfokú módosított paraméter) **6./**

$q_3^{'}$ =A*B*C (harmadfokú módosított paraméter) **7./**

z =0;1;2 kitevő, a $q_2^{'}$ paraméter ismétlődési száma

(3-nál z=0; 5-nél z=1; 7-nél z=2, és így tovább, ciklikusan ismétlődve.

P_m= f(m; $q_2^{'}$; $q_3^{'}$) polinom, (m-2*z-3), 6-tal osztható fokszámú **8./**

g = együttható, hatványösszeg tagokból triviálisan kiemelhető egész szám

Nyilvánvaló, hogy mert $q_1^{'} = Q_{'3}^{1}$ =0, a $Q_{'3}^{m}$ m>1 fokszámú azonosságok egyike sem fordulhat nullába.

1.4. Képezzük most két azonosság különbségét!

$$Q_{'3}^{m} - Q_{'3}^{1} = Q_{'3}^{m} = g * q_3^{'} * q_2^{'z} * P_m \qquad \textbf{9./}$$

1.5. Hozzuk az azonosság bal oldalát változó páronként rendezve a kis Fermat képlet alakjára, majd a módosított formából az alapváltozókra visszafordítva is írjuk fel.

$$(A^m - A) + (B^m - B) - (C^m - C) = A*(A^{m-1} - 1) + B*(B^{m-1} - 1) - C*(C^{m-1} - 1) = \qquad \textbf{10./}$$

$$= a^p * [a^{p*(m-1)} - 1] + b^p * [b^{p*(m-1)} - 1] - c^p * [c^{p*(m-1)} - 1] \qquad \textbf{11./}$$

Látható, hogy az **AZONOSSÁG BAL OLDALA m**-el, vagy **d**=p*(m-1)+1-el, amennyiben azok prímszámok, vagy az a;b;c változókban, vagy pedig a kis Fermat tétel alapján az összegekben **OSZTHATÓ** kell, hogy legyen!

1.6. Belátható, és a kis Fermat tétel segítségével **bizonyítható, hogy nemcsak az m fokszámú hatványösszegek, hanem végtelen m'=1+r*(m-1) fokszámú számú további hatványösszeg bal oldala is ismétlődően m, és d-vel oszthatóak kell, hogy legyenek!**

Ahol r tetszőleges egész szám (a p kitevőt a módosított változók, A;B;C tartalmazzák.)

Ezek a d-vel szükségszerűen osztható azonosságok e= (m-1) fokszám különbségre rendezett r= 0-∞ tagú végtelen **hatványösszeg-sorozatokat** alkotnak.

1.7. Az előző esetben viszont szükségszerű, hogy az **AZONOSSÁG JOBB OLDAL**A is, amely több tényezőre bontható, m; d-vel osztható legyen.

$$m;\ d \mid g * q_3^{'} * q_2^{'z} * P_m \qquad \textbf{12./}$$

1.8. Mint látható, az **m** prímszám (kitevő) a változóktól függetlenül, a binomiális együtthatók képlete alapján mindenkor a **g** együttható triviális osztója, sőt, azzal egyenlő is (g=m) kell, hogy legyen. Így az **m** prím **megfelel** a sejtés bizonyítása formulájának, reá vonatkozóan más vizsgálatok nem szükségesek.

A továbbiak során elegendő csupán a d osztók oszthatósága feltételeinek vizsgálatára szorítkoznunk...

1.9. Elsőként bizonyítsuk, hogy a vizsgálandó d=p*(m-1)+1 **osztók száma végtelen!**

Legyen D valamennyi lehetséges ismert d prím szorzata. Akkor a kis Fermat tétel (!) segítségével mindig találhatunk olyan d_n számosztót, amely D-nek nem osztója, s így annak osztóinál nagyobb kell, hogy legyen.

$d_n \; I \; (D^{p*(m-1)} - 1) = (D-1)* (D+1)* [d_n...]$ **13./**

Vagyis végtelen számú d_n osztó elhelyezkedésének feltételeit kell, hogy vizsgáljuk!

1.10. A d_n osztók, ha nem **g** triviális, a változóktól független számosztói, akkor a másik három, a változóktól függő tényezőké lehetnek csak:

$d_n \; I \; q_3^{'} * q_2^{'z} * P_m$ **14./**

Ezek közül:

- ha d I $q_3^{'}$, akkor tulajdonképpen az egyik változó osztója, közvetlenül annak értékét növeli, s így a sejtés bizonyítási formulájának eleve megfelel.
- ha d I, $q_2^{'z}$ akkor nem lehet közvetlenül magának a változónak az osztója, mert $q_3^{'}; q_2^{'z}$-nek csak egyetlen közös osztója lehet: d=1. Végül is azonban a $q_2^{'z}$-t növelő ilyen osztók is közvetve, más osztókkal is ugyanúgy növelik a változók értékét, mert $q_2^{'}$ és $q_3^{'}$ csak egyszerre növekedhetnek. A sejtés bizonyítási formulája szempontjából pedig érdektelen a változók osztóinak milyensége, így $q_2^{'}$ osztói a sejtés igazolására hasonlóképpen megfelelnek, mint a $q_3^{'}$.
- A P_m polinomnak is lehetnek olyan, csupán együtthatóitól és műveleti struktúrájától függő **„funkcionális" számosztói**, amelyek, bár belőle tagonként nem kiemelhetők, azonban a **változóktól mégis független számosztók**. Ezek **közvetlenül** növelik a hatványösszeget, s így a sejtés bizonyítási formulájának szintén **megfelelnek**. Más, polinom osztók viszont a **változóktól is függhetnek**. Ezek oszthatósága nem általános, hanem **változó-specifikus**. Emiatt a sejtés bizonyítási formulájának általánosságban **nem felelnek meg**.

A P_m polinom adott fokszámon bármely nagy, a változóktól függő d osztót is tartalmazhatna, illetve kell, hogy tartalmazzon.

Ezért a P_m polinom d-vel való oszthatósága a bizonyítás kulcskérdése.

További vizsgálataink célját az kell, hogy képezze, hogy megmutassuk: a Fermat tétel esetén végtelen számosságú prímszám (d és egyéb alakú) nem lehetne P_m, csakis a g; $q_3^{'}$*; vagy* $q_2^{'z}$ *tényezők osztója.* Vagyis hogy emiatt a változók végtelen nagyok kellene, hogy legyenek. És hogy emiatt állíthatta Fermat joggal, hogy a felírás nem férne el a margón!

Minthogy pedig a polinomok oszthatóságáról, két polinom közös osztójának megtalálásáról van szó, d oszthatóságát kell a témához illeszkedő, egyedi módszerekkel vizsgálnunk!

1.2.2 Polinom oszthatósági példák.

A hatványösszeg képző algoritmussal végtelen sok olyan különböző fokszámú, vagy adott fokszám-különbségű (e) hatványösszeg-sorozat képezhető, amelyek P_m polinomjai d-vel oszthatók kell, hogy legyenek.

Ezeket a polinomokat a hivatkozott elmélet eszköztára, algoritmusai segítségével, egymással végtelen változatban párosítva megvizsgálható, hogy vajon létezhet-e közös osztójuk, és hogy milyenek azok?

Mert ha bármely ilyen hatványösszeg-párnak közülük az azonosság bal oldalán van közös d osztója, ame**ly azonban a jobb oldalon nem lehetne közös osztója P_m polinomjaiknak, akkor az *csak a g;* $q_3^{'}$*;* $q_2^{'z}$ *együttható és paraméterek osztója lehetne.***

Első lépésként legcélszerűbb mindezt példákkal demonstrálni.

Példaképpen vizsgáljuk a p=3, $Q_{'3}^{1}$ =0 hatványösszeg lehetséges d osztóit

$Q_{'3}^{1}$ =A+B-C=0

Tekintsük a d=3(m-1)+1 alakú összes lehetséges prímek oszthatóságát, ha m végigfut a páratlan számok során.

Az azonosság bal oldalát már nem vizsgáljuk külön, mert az a kis Fermat tétel szerint d prímmel mindig osztható. Csak az azonosság jobb oldalán lévő $g^* q_3^{'} * q_2^{'z} * P_m$ szorzat oszthatósága érdekes, amely a hatványösszeg algoritmussal képezhető.

A változatok, m=1-el kezdődően:

1. m=1; d=3(1-1)+1 = 1 **15./**

$Q_{'3}^{1}$ =A+B-C=0

Triviális megoldás, az osztó az egység d=1.

2. m=3; d=3(3-1)+1 = 7 **16./**

$$Q_{'3}^{3} = 3\,q_3^{'}$$

Mint látható, d=7 a jobboldalon triviálisan nem osztható. Így ez az első olyan prímszámosztó, amely csak $q_3^{'}$, vagyis valamelyik változó osztója kell, hogy legyen!

„Általánosan is kimondható, hogy az m=2p+1 alakú prímek csakis a változók osztói kell, hogy legyenek."

3. m=5; d=3(5-1)+1 = 13 **17./**

$$Q_{'3}^{5} = 5\,q_3^{'} * q_2^{'}$$

Mint látható, d=13 triviálisan szintén nem osztható, s így vagy $q_3^{'}$, vagy $q_2^{'}$ osztója kell, hogy legyen.

4. m=7; d=3(7-1)+1 = 19 **18./**

$$Q_{'3}^{7} = 7\,q_3^{'} * q_2^{'2}$$

Az előzővel azonos az oszthatósága.

„Általánosan is kimondható, hogy az m=4p+1; és m=6p+1 alakú prímek csakis a $q_3^{'}; q_2^{'}$ paraméterek osztói kell, hogy legyenek, s így közvetve vagy közvetlenül a változók értékét növelik."

5. m=9; d=3(9-1)+1 = 25 **19./**

d=25 Nem prímszám, baloldalon nem igazolható.

Megjegyzendő azonban, hogy az eddigi egyszerű vizsgálati menet a továbbiakban bonyolultabbá válik, mert megjelenik a $q_3^{'}; q_2^{'}$ paraméter-változókat egyszerre tartalmazó P_m polinom.

6. m=11; d=3(11-1)+1 = 31 **20./**

$$Q_{'3}^{11} = q_3^{'} * q_2^{'}(11\,q_2^{'3} - 11\,q_3^{'2})$$

ahol, a P_{11} polinom:

$P_{11}=(q_2^{'3} - q_3^{'2})$ és g=11 **21./**

Módszert kell tehát találnunk arra (egyelőre csak egyedit), hogy a $P_{11}=(q_2^{'3} - q_3^{'2})$ polinom d=31-el való, változó-függő oszthatóságát kizárhassuk.

Vegyük észre, hogy d-vel a sorozat következő, m=21 hatványösszeg baloldala, s így a P_{21} polinom is 31-el osztható kell, hogy legyen. Ezáltal összehasonlításra, közös osztó keresésre alkalmas polinom párja lehet az előzőnek.

Maga a képlet a Newton binomról szóló II. kötet táblázatából írható ki.

$$Q_{3}^{21} = q_3^{'}(21\,q_2^{'9} - 196\,q_2^{'6}\,q_3^{'2} + 147\,q_2^{'3}\,q_3^{'4} - 3\,q_3^{'6}) \qquad \textbf{22./}$$

Ahol

$$P_{21} = \quad (21\,q_2^{'9} - 196\,q_2^{'6}\,q_3^{'2} + 147\,q_2^{'3}\,q_3^{'4} - 3\,q_3^{'6}) \quad \text{és } g=1 \qquad \textbf{23./}$$

Látható, hogy ez a képlet d=31-el triviálisan szintén nem osztható, sőt az is, hogy egyébként csak $q_3^{'}$, vagyis közvetlenül a változók osztója lehetne.

Ami általános szabályként is, bármely p kitevő esetére felírható:

„Az m=3+6*r fokszámú módosított hatványösszegekben a d osztók vagy $q_3^{'}$, vagy a P_m polinom osztói lehetnének csak!"

Sőt, az is látható, a polinom tagjaiból triviálisan más osztó sem emelhető ki.

Ez is általános szabályként felírható:

„Ha m nem prímszám, hanem két különböző prímszám szorzata, akkor triviálisan egyikük sem emelhető g osztójaként ki."

Hasonlítsuk össze a két polinomot, több lépésben csökkentve fokszámukat:

1. lépés: $P_{21} - 21*P_{11}\,q_2^{'6} = (21\,q_2^{'9} - 196\,q_2^{'6}\,q_3^{'2} + 147\,q_2^{'3}\,q_3^{'4} - 3\,q_3^{'6}) - (21\,q_2^{'9} - 21\,q_2^{'6}\,q_3^{'2}) =$

$$= q_3^{'2}(-175\,q_2^{'6} + 147\,q_2^{'3}\,q_3^{'2} - 3\,q_3^{'4}) \qquad \textbf{24./}$$

2. lépésben a csökkentett polinomot ismét a kisebbel kell, hogy összehasonlítsuk.

$$(-175\,q_2^{'6} + 147\,q_2^{'3}\,q_3^{'2} - 3\,q_3^{'4}) + (175\,q_2^{'6} - 175\,q_2^{'3}\,q_3^{'2}) = q_3^{'2}(-28\,q_2^{'3} - 3\,q_3^{'2}) \qquad \textbf{25./}$$

3. *Ha az előző lépésben azt tapasztaltuk volna, hogy az eredmény P_{11}-el egyező, vagy csak egy számosztóval tér el attól, akkor a vizsgálat megállt volna, és P_{11}-et, mint legkisebb közös polinom osztót azonosíthattuk volna. Minthogy azonban ilyen egyenlőség nem állt fenn, a fokszám csökkentés tovább folytatható*.

$$(-28\,q_2^{'3} - 3\,q_3^{'2}) + (28\,q_2^{'3} - 28\,q_3^{'2}) = -31\,q_3^{'2} \qquad \textbf{26./}$$

Ebből az összehasonlításból tehát az derül ki, hogy az m=11;21 hatványösszeg párok között d=31 a P_{21};P_{11} polinomoknak **funkcionálisan közös számosztója**, és mert a változóktól független, a sejtés bizonyítási formulájának így is **megfelel**.

Ugyanakkor ez a részeredmény nem zárja ki, hogy további számpárok összehasonlításakor esetleg találhatók még szigorúbb kritériumok, akár közvetlenül a változók oszthatóságának bizonyítására is.

Hiszen elegendő lenne csak egy ilyent találni...az kizárná a teljes hatványösszeg sorra, hogy d a P_m polinom osztója lehessen.

Például m=31 esetén is látható, hogy d=31 a Q_{3}^{31} hatványösszeget nem funkcionálisan, hanem g-ben, triviálisan osztja!

Erre kell általánosabb bizonyítást bemutatnunk!

Most azonban még két próbát végzünk:

7. m=13, d=3*(13-1)+1=37

$$Q_{r3}^{13} = q_3' * q_2'^2 (13 q_2'^3 - 26 q_3'^2) \qquad \textbf{27./}$$

ahol $P_{13}=(q_2'^3 - 2 q_3'^2)$ és g=13 **28./**

A kontrol polinom pedig, m=25 esetén

$$Q_{r3}^{25} = q_3' * q_2'^2 (25 q_2'^9 - 375 q_2'^6 q_3'^2 + 630 q_2'^3 q_3'^4 - 100 q_3'^6) \qquad \textbf{29./}$$

ahol $P_{25}=(5 q_2'^9 - 75 q_2'^6 q_3'^2 + 126 q_2'^3 q_3'^4 - 20 q_3'^6)$ és g=5 **30./**

Hasonlítsuk össze a két polinomot, több lépésben csökkentve fokszámukat:

1. lépés: $P_{25} - 5*P_{13} q_2'^6 = (5 q_2'^9 - 75 q_2'^6 q_3'^2 + 126 q_2'^3 q_3'^4 - 20 q_3'^6) - (5 q_2'^9 - 10 q_2'^6 q_3'^2) =$

$= q_3'^2 (-65 q_2'^6 + 126 q_2'^3 q_3'^2 - 20 q_3'^4)$ **31./**

2. lépés: a csökkentett polinomot ismét a kisebbel kell, hogy összehasonlítsuk.

$(-65 q_2'^6 + 126 q_2'^3 q_3'^2 - 20 q_3'^4) + (65 q_2'^6 - 130 q_2'^3 q_3'^2) = 4 q_3'^2 (- q_2'^3 - 5 q_3'^2)$ **32./**

3. lépés: a csökkentett polinom kisebbel való összehasonlítása.

$(q_2'^3 + 5 q_3'^2) - (q_2'^3 - 2 q_3'^2) = 7 q_3'^2$ **33./**

Következésképpen m=13 esetén d=37 ismét a $q_3'; q_2'^2$ paraméterek osztója kell, hogy legyen, vagyis a változókat kell, hogy növelje.

8. m=15, d=3*(15-1)+1=43

$$Q_{r3}^{15} = q_3' * (15 q_2'^6 - 50 q_2'^3 q_2'^2 + 3 q_3'^4) \qquad \textbf{34./}$$

ahol $P_{15=}(15 q_2'^6 - 50 q_2'^3 q_2'^2 + 3 q_3'^4)$ és g=1 **35./**

A korábban megfogalmazott szabálynak megfelelően ez is csak a változók vagy a P_m polinom osztója lehetne, és a tagokból számosztó nem emelhető ki.

A kontrol polinom pedig, **m**=29 esetén

$$Q_{r3}^{29} = q_3' * q_2' (29 q_2'^{12} - 638 q_2'^9 q_3'^2 + 1914 q_2'^6 q_3'^4 - 870 q_2'^3 q_3'^6 + 29 q_3'^8) \qquad \textbf{36./}$$

ahol $P_{29}=(q_2'^{12} - 22 q_2'^9 q_3'^2 + 66 q_2'^6 q_3'^4 - 30 q_2'^3 q_3'^6 + q_3'^8)$ és g=29 **37./**

Hasonlítsuk össze a most már öttagú polinomot a kisebbel, több lépésben csökkentve a fokszámot:

1. lépés: $15*P_{29} - P_{15} q_2'^6 = (15 q_2'^{12} - 330 q_2'^9 q_3'^2 + 990 q_2'^6 q_3'^4 - 450 q_2'^3 q_3'^6 + 15 q_3'^8) -$

$(15 q_2'^{12} - 50 q_2'^9 q_3'^2 + 3 q_2'^6 q_3'^4) = q_3'^2 (-280 q_2'^9 + 987 q_2'^6 q_3'^2 - 450 q_2'^3 q_3'^4 + 15 q_3'^6)$ **38./**

2. lépés: a csökkentett polinomot ismét a kisebbel kell, hogy összehasonlítsuk (most a q_3'-t csökkentjük, ami mindegy).

$$(-280\,q_2'^9+987\,q_2'^6\,q_3'^2-450\,q_2'^3\,q_3'^4+15\,q_3'^6)-5\,q_3'^2*(15\,q_2'^9-50\,q_3'^2\,q_2'^6+3\,q_3'^4)=$$

$$=8\,q_2'^3*(-35\,q_2'^6+114\,q_2'^3\,q_3'^2-25\,q_3'^4) \qquad \textbf{39./}$$

Mint látható, nem adódott saját polinom osztó, így a vizsgálatot folytatni kell.

Ettől kezdődően azonban a „kisebb" osztó alatt mindig az eredményül kapott értendő.

3. lépés: a csökkentett polinom kisebbel való összehasonlítása.

$$3*(-35\,q_2'^6+114\,q_2'^3\,q_3'^2-25\,q_3'^4)+7*(15\,q_2'^6-50\,q_2'^3\,q_2'^2+3\,q_3'^4)=$$

$$=2*(-4\,q_2'^3\,q_3'^2-27\,q_3'^4) \qquad \textbf{40./}$$

4. lépés: a kiinduló polinom „kisebbel" való összehasonlítása.

$$9*(15\,q_2'^6-50\,q_2'^3\,q_2'^2+3\,q_3'^4)-q_3'^2(4\,q_2'^3\,q_3'^2+27\,q_3'^4)=q_2'^3(135\,q_2'^3-454\,q_3'^2) \qquad \textbf{41./}$$

Most sem adódott saját polinom osztó, s így a vizsgálat tovább folytatható.

5. lépés: Összehasonlítás

$$4*(135\,q_2'^3-454\,q_3'^2)-135*(4\,q_2'^3+27\,q_3'^2)=-5461\,q_3'^2 \qquad \textbf{42./}$$

ami 43-mal ismét csak funkcionálisan osztható (127*43=5461).

Ami a lényeg, hogy ez sem változófüggő polinom, hanem csak számosztó, s így a hatványösszeget, közvetve a változókat növelnie kell!

9. Összegzés

A végzett számpéldák csaknem minden vizsgálati lehetőséget felmutattak már. Az eddigi eredmények mindegyike azonban a **sejtés bizonyítási formulájának megfelelt!**

Mert valamennyi vizsgált osztóról bebizonyosodott, hogy vagy triviálisan, vagy funkcionálisan, közvetve vagy közvetlenül a hatványösszeget, és a változókat növeli.

(m=3; d=7;13;19;31;37,43 ...).

Természetesen mindez nem biztosítéka annak, hogy minden d osztó ilyen, de eléggé biztató arra nézve, hogy valamely szabály mégiscsak létezhet!

Továbbá már az eddigi példákkal is bizonyítást nyert az a feltevés, hogy a triviálisan nem osztható d osztók legalább egy része csakis a g; $q_3'; q_2'^2$ tényezők osztója lehet!

Másfelől, *nincs szükség annak a kizárására, hogy létezhetnek olyanok is, amelyek a P_m polinomot polinom osztóval, a változóktól függően osztják!*

A sejtés bizonyítási formulája ugyanis nem azt igényli, hogy minden d osztó a változók része legyen. Az igény csak az, hogy **számuk végtelen** legyen. Ez pedig akkor is teljesülhet, ha egy részük a P_m-t a változóktól függően is osztja.

Előző példák szemléltetően mutatják a sejtés bizonyítási formulájának sajátosságait.

Az így végzett egyedi vizsgálat azonban a továbbiak során egyre bonyolultabb lenne. **Általános bizonyítás** kidolgozására van szükség.

1.2.3 Polinomok közös osztói

Különféle fokszámú polinomok közös **természetes szám osztóit a következők elemei tartalmazhatják** (sajátos megfogalmazásom):

- Az **egység** =1
- **Triviális számosztó** (vagyis m=0 fokszámú polinom), amely a P_m polinom tagjainak együtthatóiból **külön-külön** mindegyikből kiemelhető, s így a **változóktól független**. Ilyenek például a binomiális együtthatókból kiemelhetők, köztük az m= prímszám kitevők.
- **Funkcionális számosztó**, (szintén m=0 fokszámú polinom), amely azonban a P_m polinom tagjaiból nem külön, hanem **azok összességéből** valamely műveleti szabály alapján emelhető ki, és a **változók értékétől szintén független**. Ilyenek képződhetnek bizonyos azonosságok, pld. a kis Fermat tétel alkalmazásakor, mivel ha a változó maga d-vel nem, az a^{d-1}-1 azonosság d-vel mindig osztható.
- **polinom osztó** - a vizsgált két polinomnál kisebb, vagy a kisebbel azonos („saját"), de legalább m=1 fokszámú, a **változók közötti függvénykapcsolatot** biztosító polinom.

1.2.4 Polinom párok közös osztóit vizsgáló algoritmus

A következő, (a példákkal már részben demonstrált) általános algoritmus ajánlható két azonos, vagy különböző fokszámú polinom **legkisebb közös polinom-osztója** megtalálására.

- A két polinom közül a kisebb fokszámút az egyik **változóval** (adott esetben az egyik paraméterrel) történő szorzása útján a nagyobbal azonos fokszámra kell hozni.
- Mindkét polinomot alkalmasan megválasztott **számmal** szorozva, bármely két azonos változó-összetételű (célszerűen csak az egyik változót tartalmazó) tagja egyenlővé tehető.
- Egymásból kivonva ezeket az azonos tagok kiesnek. A megmaradó összeg a másik változóval egyszerűsíthető, és ezáltal a polinom fokszáma (és tagszáma) eggyel csökkenthető.
- A jelzett művelet megismételhető a kisebb, és a csökkentett fokszámú polinomok között, mindaddig, amíg a nagyobb polinom a kisebbel azonos fokszámú nem lesz.
- Ha ekkor a két polinom azonossága, vagy csak számszorzó különbsége tapasztalható, akkor a kiinduló polinomok közös osztója maga a kisebb polinom („**sajátosztó"**).
- Ha a két polinom nem azonos, akkor ez az algoritmus ismételten, minden lépésnél fokszám csökkentéssel addig végezhető, amíg eredményül vagy valamely m=0 fokszámú közös számosztót, vagy egy m>0 közös polinomosztót nem kapunk.
- **Számosztó** a változótól nem függ, triviálisnak, vagy funkcionálisnak tekinthető.
- **Polinomosztó** számosztója a változóktól is függ.

A további vizsgálatok célja, hogy megmutassuk, hogy a d számosztók közül végtelen számú, határesetben valamennyi - a Fermat sejtés esetén maguknak a változóknak az osztója kellene, hogy legyen!

1.2.5 Hatványösszegek közös osztói

A továbbiakban a hatványösszeg algoritmusnak megfelelő hatványösszeg (polinom) sorozatok speciális oszthatósági szabályait vizsgáljuk, amelyeknek a Fermat sejtés is megfelel.

Az azonosságok bal oldalán azok d-vel való oszthatóságát a kis Fermat tétellel vezettük le.

Az azonosságok jobb oldalán a közös osztó összehasonlító vizsgálatára a hatványösszeg elmélet szerinti algoritmus használható (lásd I. kötet).

$$Q_{3}^{r+3} = q_1^{'}\, Q_{3}^{r+2} - q_2^{'}\, Q_{3}^{r+1} + q_3^{'}\, Q_{3}^{r} \qquad \textbf{43./}$$

Az algoritmusból következik, hogy bármely hatványösszeg a nála kisebb három, egymás után következő hatványösszegből a $q_1 ; q_2 ; q_3$ paraméterek segítségével képezhető.

Továbbá egy fontos oszthatósági szabály:

„Ha három egymás után következő hatványösszegnek, amelyekből nagyobb fokszámút képezünk, bármely közös szám, vagy polinom osztója van, akkor az eredményként kapott hatványösszegnek is változatlan formában (polinom, vagy szám) ezt az osztót tartalmaznia kell!”

Átrendezve az előző, növekvő algoritmust csökkenőre, belátható, hogy bármely kisebb fokszámú hatványösszeg a nála nagyobb, három egymás után következő hatványösszegből a paraméterek segítségével szintén kiszámolható, azonban azzal a korlátozással, hogy az eredmény a változók osztóit nem biztos, hogy tartalmazhatja.

$$Q_{3}^{r} = (Q_{3}^{r+3} - q_1^{'}\, Q_{3}^{r+2} + q_2^{'}\, Q_{3}^{r+1}) / q_3^{'} \qquad \textbf{44./}$$

„Ha három egymás után következő hatványösszegnek, amelyekből kisebb fokszámút képzünk, bármely közös szám, vagy polinom osztója van, akkor az eredményként kapott hatványösszegnek is változatlan formában (polinom, vagy szám) ezt az osztót tartalmaznia kell, kivéve a változókat!”

A két szabály (növekvő és csökkenő) alapján egy következő, általánosabb, a teljes fokszám intervallumra vonatkozó is feltételesen körvonalazható:

„Ha bármely három egymás után következő hatványösszegnek, valamely közös szám (kivéve a változókat), vagy polinom osztója van, akkor az összes 0 - ∞ hatványösszegnek azt változatlan formában (polinom, vagy szám) tartalmaznia kell!”

Másfelől azonban ez a $Q_{3}^{0} = 3$ hatványösszegre is vonatkoztatható, amiből újabb általános szabályok következnek:

„A teljes hatványösszeg-sor, vagy annak legalább három egymás után következő hatványösszegének közös osztója, ha a változókat nem osztja, csakis d=3 lehet.”

„Nem létezhet tehát olyan három egymás után következő hatványösszeg sem, amelyeknek azonos polinomosztója lenne!”

Ezek, és még számos más következtetés a hatványösszeg algoritmusból adódnak.

1.3 A Fermat sejtés bizonyítása.

Bizonyos szempontból az előzőhöz hasonló a helyzet a Fermat sejtés esetén is, ahol az a feladat, hogy bizonyítsuk: a hatványösszeg sorozatban e=m-1 különbséggel periodikusan ismétlődő P polinomoknak nem lehet közös d_n szám vagy más polinom osztója.

Hiszen, mint láttuk a példákban, $Q_3^3=0$ esetén az m=3; (5; 7;11;13;15) fokszámú hatványösszegeknek d=7;(13;19;31;37;43) értékű közös osztói kellene, hogy legyenek, az e=(m-1)-el nagyobb fokszámú m’=5;(9;13;21;25;29); m”=7;(13;19;31;37;43)....m”’, s így tovább, végtelen hatványösszeg sorozatok bármely tagjával történő összehasonlításuk esetén.

Vagyis ez esetben is végtelen hatványösszeg sorozat oszthatóságáról van szó, azonban **nem egyenkénti**, hanem e=(m-1) **páros fokszám eltérésű** fokozatokkal, csupa páratlan hatványösszeggel.

Bizonyítható azonban, hogy a hatványösszeg-algoritmus alkalmazható ilyen esetben, is azonban módosított felírással:

$$Q_{'3}^{1+(r+3)*e} = q_1^{''} Q_{'3}^{1+(r+2)*e} - q_2^{''} Q_{'3}^{1+(r+1)*e} + q_3^{''} Q_{'3}^{1+r*e} \qquad \textbf{45./}$$

$$q_1^{''} = A^e + B^e - C^e \qquad \textbf{46./}$$

$$q_2^{''} = A^e B^e + A^e C^e + B^e C^e \qquad \textbf{47./}$$

$$q_3^{''} = A^e B^e C^e \qquad \textbf{48./}$$

Fenti, „**e”** fokszámkülönbségű módosított algoritmus egyébként egyszerű próbával bizonyítható.

Ezzel az algoritmussal bármely e=m-1 fokszám eltérésű hatványösszeg sor tagjai, függetlenül annak kezdő fokszámától leírhatók!

És az algoritmus jelentése is ugyanaz, mint korábban:

„Ha a hatványösszeg sorozat bármely három egymás után következő, e=(m-1) fokszám különbségű hatványösszegének valamely közös, szám, vagy polinom osztója van (kivéve a változókat), akkor azt az ilyen hatványösszeg sorozat összes hatványösszegének változatlan formában (polinom, vagy szám) tartalmaznia kell!”

A közös osztó kereső algoritmussal megtalált közös szám, vagy polinom osztók csupán lehetőségek, amelyekből még nem következik, hogy azok ténylegesen létező osztók.

A Fermat sejtés esetén azonban szükségszerű, hogy a létező közös osztónak minden hatványösszeg párban mindig azonos formában realizálódnia kell!

- Mert ha csak az egyiknél is hiányozna, azt jelentené, hogy mindegyikben csak a változók osztója lehetne.
- Ha csak az egyik párnál is eltérő alakú osztója lenne, akkor az összes többinél is annak ismétlődnie kellene...
- Ha viszont realizálódik, mint osztó, akkor az algoritmus alapján a változóktól függetlenül a szám és a polinom osztókra minden szituációban érvényes oszthatóságot kell, hogy kapjunk.

Beleértve természetesen a legkisebbet, az induló hatványösszeget is, vagyis r=0, és $Q^{1}_{,3}$ =0

Amelynek jobb oldalán p=1, Q^{1}_{3} **=0** esetén egyszerűen nulla érték lenne, nem pedig polinom, s így ellentmondásmentesen **minden számmal és polinommal oszthatóan!**

Ha azonban p>1, $Q^{1}_{,3}$ **=0**, akkor a jobb oldalon nem nulla áll, csak egy, az adott esetben nulla-értékű polinom.

A $Q^{1}_{,3}$ polinom viszont egészében nem tekinthető „sajátosztó”-nak, mert akkor a nagyobb fokszámúak a nullaértékűvel lennének oszthatók, s így ismétlődően más hatványösszegek is periodikusan nullába kellene, hogy forduljanak. Ez pedig csak a triviális megoldásnál, mikor a változók nullaértékűek, fordulhatna elő.

Ugyanakkor ezt a polinomot valamennyi, a kereső algoritmussal megtalált polinom osztónak is osztania kellene! Vagyis a $Q^{1}_{,3}$ jobb oldali polinomjának egyetlen nullaértékű, és végtelen sok nem nulla polinom osztó szorzatából kellene állnia. Ezek az osztók ugyanis attól függetlenül kell, hogy létezzenek, hogy az adott változó kombináció esetén a $Q^{1}_{,3}$ polinom éppen nullaértékű, vagy nem.

Így más esetekben, mikor nem nullaértékű, a $Q^{1}_{,3}$ hatványösszeg végtelen nagy lenne.

Ezért a d_n osztók nem lehetnének P_m 0>m fokszámú osztó polinomjainak változóktól függő osztói, csakis a paramétereké!

1.4 Befejező gondolatok

Bizonyítást nyert tehát, hogy az adott feltételek mellett valamennyi lehetséges d prím osztó közvetlenül, vagy közvetve a változókat növelné, „túlcsordítva” őket bármely könyv margóján...

A bizonyításhoz csupán Fermat munkásságának eredményei (pld. a kis Fermat tétel), valamint a hatványösszegek elmélete (szimmetrikus polinomok szerkesztési elvei) lettek felhasználva, amelyeket minden bizonnyal már Ő is kellő szinten ismerhetett.

Csodálatra méltó, ahogyan a bemutatott ellentmondást századokkal előbb meglátta, és lejegyezte. Másfelől nála ez természetes volt, hiszen ebben a gondolati körben élt! És akkortájt nem volt ritka, vagy tőle idegen a feltételezett „talányos” közlési forma. Sőt az is lehet, hogy később többeknek is elmondta a bizonyítást, de senki sem jegyezte le, hiszen így is szinte kiáltó:

Nem lehet felírni.... mert VÉGTELEN!

Korát megelőzve, sajátosan eltérő módon, de helyesen, így fogalmazta meg, hogy a sejtés megoldása a természetes számok halmazában nem kereshető, nem része annak!

Ha létezett volna a terminológia, azt mondhatta volna, hogy a megoldás **„irracionális (=nem szakaszosan ismétlődő, (rendezetlen) végtelen egész szám, vagy törtszám)** lehet csak!

De végül is mindegy, miért - hogy túl nagy, irracionális, vagy komplex szám - ezek csupán a sokféleképpen megfogalmazható sejtés **eltérő, de egyenlő fontosságú megoldásai**, amelyek jelentése mégis hasonló: hogy **a változók nem kereshetők a természetes számok között...**

Megmutatkozik, hogy, **ugyanazon „sejtésnek" sokféle, egymással kapcsolatba nehezen hozható felírása és bizonyítása lehetséges!**

Ugyanakkor előzőek alapján biztosra vehető, hogy Fermat a sajátját részletesen is felírta, és bizonyította is. És több évszázados, sikertelen keresése nyomatékosíthatja, hogy az nem volt egyszerű. Hanem talán éppen a legnehezebb...

Amit tehát Fermat sejtésnek gondoltunk, az valójában - TÉTEL.

Befejezésül megemlékeznék arról, hogy észrevételeikkel, bírálatukkal sokan segítették a munkámat, amit most megköszönök. De aktív közreműködésükre nem számíthattam, és sejtem, hogy azt opponálva - jó szándékkal is - a közlését sem ajánlották volna!

Így van okom tartani attól, hogy hibázhattam. És mert ilyen bizonytalanságban vagyok, sem állíthatom, hogy ez tudományos igényű mű! Csupán régies történet, kommentárokkal. Talán egyező, talán nem egyező másokéval, amelyeket alig ismerek...

Ha pedig már úgyis csak történet - akkor legyen is az - nem fogtam vissza a fantáziámat!

S így sok mindenről írhattam, amelyeknek tudományos igényű műben nem lehetne helye.

És még sok mindenről, főképpen magukról a SZÁMOKRÓL szeretnék írni ugyanígy...

Mindezeket mérlegelve is bízom abban, hogy e gondolatok érdekesek, sőt hasznosak lehetnek, és hogy még messze nem tehető pont a végükre
(Bárhogy is kívánkozna a különféle szabályok, és a gépi hibajavító program szerint oda!)

Most is, kétséggel és bizakodással útjukra bocsátva őket - erre gondolok!

Forrai György

Budapest. 2009. június. (2. javított kiadás)
2007. január 22. (Eredeti kiadás)

2 Elliptikus egyenletek vizsgálata hatványösszeg módszerrel (Fermat sejtés)

Ez a fejezet nem újabb Fermat sejtés bizonyítás, csupán kíváncsi próbálkozás az elliptikus egyenletek vizsgálatára a hatványösszeg elmélet alkalmazásával, ami nagyon kínálkozó lehetőség.

2.1 Elliptikus egyenletek felírási formái

A témakör a Fermat sejtéshez, annak bizonyítása történetéhez kapcsolódik.

- Elsőként Taniyama és Shimura fedezték fel az elliptikus egyenletek, és a moduláris formák közötti kapcsolatot.

- Majd G. Frey ismerte fel, hogy az bebizonyítva elvezethet a Fermat sejtés eldöntéséhez is.

- Ezt a „sejtését" Ken Ribet igazolta.

- Végül pedig A. Wiles bizonyította a kiinduló Taniyama-Shimura sejtést, és általa közvetve a Nagy Fermat sejtést is.

A Wiles tehát a legnehezebb, a befejező lépést tette meg a Fermat sejtés bizonyítására, amelyet azonban Frey alapozott meg azzal, hogy a Fermat azonosságot elliptikus egyenletté alakítva a következő döntési sémát (bizonyítási formulát) vetette fel.:

Ha bizonyítható Taniyama-Shimura sejtése, hogy valamennyi elliptikus egyenletnek rendelkeznie kell moduláris párral, akkor Fermat sejtése is igaz kell, hogy legyen, mert a Fermat azonosságból képzett elliptikus egyenlet(ek) különleges struktúrája („különcsége") miatt azok feltételezhetően nem lehetnek modulárisak, tehát nem létezhetnek!

A Frey általa levezetett elliptikus egyenlet(ek) egy változata („Frey görbe") a következő:

$$y^2 = x^3 + (a^n - b^n)\, x^2 - a^n b^n \qquad 1./$$

ahol :

x;y az elliptikus egyenlet változói

a;b;n a Fermat azonosság változói és kitevője

A felvázolt „bizonyítási formula" egyfelől reménykeltő, másfelől meglehetősen bizakodó volt, hiszen beteljesüléséhez még két igazán nehéz sejtést kellett igazolni:

- hogy a Fermat sejtés elliptikus alakjához nem tartózhatnak moduláris párok - ami Frey sejtése, és amit végül Ken Ribet bizonyított.

- hogy minden elliptikus egyenletnek kell, hogy moduláris párja legyen - ez lett később A. Wiles hozzájárulása.

G. Frey arra hivatkozott, hogy az általa levezetett képlet valójában elliptikus egyenlet, hiszen illeszkedik annak ***általános*** alakjához:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4\, x + a_5 \qquad 2./$$

ahol a_1, a_2, a_3, a_4, a_5, x, y valamely K test elemei. x, y a változók, a_1, a_2, a_3, a_4, a_5, adott paraméterek.

Ugyanakkor felismerte, hogy az mégis „különc” abban a tekintetben, hogy valószínűleg nem elégítené ki a Taniyama-Shimura sejtést, ha az bizonyított lenne. Vagyis a Fermat azonosság sem létezhetne, s ezáltal Fermat sejtése igazolható lenne.

Fontos lenne tehát tudni, hogy miben áll az a különbség, amely miatt az 1. képlet mégsem egyenértékű más hasonló elliptikus egyenlet felírásokkal.

Összehasonlítás céljából álljon itt az ellipszis egyenlete is, egységes paraméter jelölésekkel:

$$a_3x^2 + a_1xy + y^2 + a_4x + a_2y + a_5 = 0 \qquad 3./$$

Összehasonlítva a 2./ képlettel, szemléletesen megmutatkoznak az elliptikus, és az ellipszis egyenletek kisebb-nagyobb hasonlóságai, és különbségei, amelyek közül a legfontosabb, hogy az elliptikus egyenlet tartalmaz egy harmadfokú tagot, az x^3-t is, amely alaposan felkavarja tulajdonságait. Ami megnyilvánul a görbe alakzatában is, mert amíg az ellipszis egyetlen egységes, bezáródó alakzat, és az őt metsző egyenes csak két pontját érintheti, addig az elliptikus görbék két részből is állhatnak, és a metsző egyenesükkel három metszéspontjuk lehet (az érintési pont is kettőnek számít).

Megjegyzendő, hogy a valós számtest feletti ($a_1=a_2=0$) elliptikus görbék az x tengelyre szimmetrikusak, és hogy esetükre felírható a sokkal egyszerűbb *Weierstrass-féle normálalak is*:

$$y^2 = x^3 + a_4x + a_5 \qquad 4./$$

A továbbiakban a vizsgálni ajánlott hatványösszeg-algoritmusok képzése az I. kötetben szereplő alapösszefüggésekkel, és jelölésekkel történik.

Elsőként az y=0 helyen érvényes, a továbbiakban **„elliptikus bázisegyenlet”-**ként említett képlet lesz felírva. Ami tulajdonképpen egy harmadfokú algebrai egyenlet, amely később a független változóval (ez esetben „y”) még bővítendő.

A kiinduló lépés a harmadfokú, három ismeretlenes ($x_1;x_2;x_3$), egyenlet gyöktényezős alakja:

$$(x-x_1)*(x-x_2)*(x-x_3)=0 \qquad 5./$$

Kanonikus polinomja:

$$0 = x3 - q_1x^2 + q_2x - q_3 \qquad 6./$$

Az itt alkalmazott jelölések a korábbiaknak (1./) a következőképpen feleltethetők meg:

$$q_1=-a_3 = x_1+ x_2 + x_3$$

$$q_2=a_4 = x_1 x_2+ x_1 x_3 + x_2 x_3 \qquad 7./$$

$$q_3=-a_5= x_1 x_2 x_3$$

A három gyök, illetve paraméter alapján felírható a harmadfokú teljes hatványösszeg (bizonyítás I. kötetben):

$$Q_3^3 = x_1^3 + x_2^3 + x_3^3 = q_1^3 - 3q_1q_2 + 3q_3 \qquad 8./$$

A fenti felírási alakkal bármely, a paraméterekkel kapcsolatos feltétel változása szemléletesen bemutatható.

Például, $q_1 = 0$ esetén :

$$Q_3^3 = x_1^3 + x_2^3 + x_3^3 = 3\, x_1 x_2 x_3 = 3\, q_3 = -3\, a_5 \qquad 9./$$

Megjegyzendő, hogy ez esetben több új feltétel is keletkezik:

- A gyökök egymással relatív prím alakra hozhatók $(x_1; x_2; x_3) = 1$.

- Relatív prímként csak egyikük lehet páros.

- Nem lehet mindhárom gyök azonos előjelű. Értéktől és előjeltől függően a hatványösszeg (Q_3^3) pozitív, vagy negatív lehet, aminek az elliptikus környezetben jelentősége van.

Maga a q_3 paraméter pedig vagy adott, vagy kiszámítható.

Mint látható, bármely elliptikus „bázisegyenlet” (y=0 helyen) mindig visszavezethető valamely harmadfokú egyenlet három gyökéhez, mint megoldásához.

Az elliptikus egyenlet általános alakját (2./) vizsgálva, annak minden tagját x hatványa szerint egy oldalra átrendezve a másik oldal nullával egyenlő.

$$0 = x^3 + a_3 x^2 + (a_4 - a_1 y)\, x + (a_5 - y^2) = x^3 - q_1' x^2 + q_2' x - q_3' \qquad 10./$$

Ebből (fordított szemlélettel) kitűnik az is, hogy az elliptikus egyenlet általános alakja voltaképpen egy szokásos harmadfokú egyenlet speciálisan átrendezett alakjával egyenértékű. Amikor a két oldalon eltérő fokszámú változók (x;y) találhatók, s így valamely, kétismeretlenes határozatlan, harmadfokú egyenlet alakul ki.

Az átrendezés következtében a független változó hozzáadása miatt módosulnak a paraméterek is:

$q_1' = a_3$ (változatlan) 11./

$q_2' = a_4' = (a_4 - a_1 y)$ (y első hatványán szerepel) 12./

$q_3' = a_5' = (-a_5 - y^2)$ (y második hatványán szerepel) 13./

Az **x** változó tekintetében harmadfokú egyenletnek két paramétere is az **y** változótól függ. Ami azt jelenti, hogy y-nak értéket adva a harmadfokú egyenletnek újabb és újabb x változói (gyökei) határozhatók meg.

Hasonló módon kiszámítható az új változókhoz tartozó hatványösszeg ($Q_3'^3$) is:

$$Q_3'^3 = x_1'^3 + x_2'^3 + x_3'^3 = q_1'^3 - 3q_1'q_2' + 3q_3' \qquad 14./$$

Továbbra is fenntartva a feltételt, hogy **y** bármely értékénél $q_1, =0$ kell, hogy legyen:

$$Q_3,^3= x_1,^3 + x_2,^3 + x_3,^3= 3\, q_3, = 3\, x_1, x_2, x_3,= - (a_5 + y^2) \qquad 15./$$

Vagyis, hogy y^2 most a q_3 paraméterhez kapcsolódik.

Behelyettesítve a_5 -nek a bázis egyenletnél korábban már kiszámított értékét, kapjuk:

$$y^2= -Q_3,^3 -a_5= -3(x_1, x_2, x_3,+a_5)= - 3(x_1 x_2 x_3 + x_1, x_2, x_3,) \qquad 16./$$

Megjegyzendő, hogy a valós számokra érvényes Weierstrass-féle normálalakból is ugyanilyen alakú hatványösszeg lenne képezhető. A hatványösszeg azonban kevesebb tagot (paramétert) tartalmazna, és a gyökök lehetséges viszonyát a vizsgált $q_1=0$ esetre áttekinthetőbben mutatná meg. Ugyanis ebben az esetben az a_4 paraméter figyelembevételére azért nincs szükség, mert azt a $q_1=0$ feltétel szükségtelenné teszi. Vagyis sokkal tömörebben, átláthatóbban, és kevesebb paraméterrel fejezi ki a független változó és a gyökök kapcsolatát, mint a kanonikus polinom alakúak, s így vizsgálathoz inkább alkalmas.

A továbbiakban hangsúlyosan az egész számokra, és a Fermat azonosságra vonatkozó elemzés történik majd. Hogy annak feltételei ($x_1,^p+ x_2,^p+ x_3,^p=0$) hatványösszeg alakban is teljesüljenek, a gyököket $x_1,^p$; $x_2,^p$;$x_3,^p$ vagyis p hatványúnak kell felvenni:

$$y^2= Q_3^3 -Q_3,^3=3(x_1^p x_2^p x_3^p - x_1,^p x_2,^p x_3,^p) \qquad 17./$$

Megjegyzendő, hogy a szokásos szemlélet szerint ebben a behelyettesítésben nincs semmi kivetnivaló, hiszen hasonló felírás bármely összetett számmal már a kiinduló gyöktényezős alaktól (4./) kezdve jelenleg minden korlátozás nélkül megtehető. Vagyis a (17./) képlet akár a gyöktényezős alakjától így is levezethető.

A már említett „számvektoralgebra” egyik feladata megmutatni, hogy *ez nem egészen így van!* Hogy még valamely azonos végeredmény is a számok *valódi* jelentéséhez igazodóan, „szabályosan”, csak olyan eltérő úton lenne elérhető, amelynél a hatványozás abban a formájában, ahogyan most ismerjük - nem is létezik!

2.2 Az elliptikus egyenletek felírási formáinak elemző összehasonlítása

Felhasználva az elliptikus egyenletek hatványösszeg alakú felírásának újabb lehetőségét, a továbbiakban általános, és speciálisan a $q_1=0$ esetre vonatkozó elemzések történnek majd.

Következtetések a *hatványösszeg* (15./ 16./17./) képletekből

1.) **y=0** feltétel hatványösszeg esetén általánosságban csak úgy teljesülhet, ha

$x_1,x_2,x_3,= -a_5$

Amelyek különleges pontjai az elliptikus görbének: metszékei az x tengelyen, az y=0 helyen.

2.) **y** egész értékénél a gyökök szorzatkülönbsége 2 páros, és 3 páratlan hatványával osztható, kell, hogy legyen, vagyis hogy y legalább 6-al osztható

$2^{2m};3^{2m+1}$ **I y;** $(x_1\, x_2\, x_3 - x_{1'}\, x_{2'}\, x_{3'})$

3.) Fentiekből következik, hogy **y** változó csak összetett szám lehetne, amelynek állandó (2*3), és kiegészítő osztói vannak Amiből következik, hogy az (y) változó értékkészlete nem lehetne folyamatos, például nem állhatna csupán egyetlen prímszámból.

4.) $\mathbf{y} = \pm\ (-3a_5 - 3x_{1'}x_{2'}x_{3'})^{0,5}$, ezért valós szám eredményhez $(-3a_5 - 3x_{1'}x_{2'}x_{3'})>0$

Ez a feltétel a gyökök előjel-elosztásától, és értékétől (vagyis implicit y-tól is) függően többféleképpen realizálódhat. Ha mindkét egyenlet gyökeiből kettő-kettő pozitív előjelű, y biztosan valós értékű lehet.

5. $y=\pm(-3a_5)^{0,5}$ esetén $3x_{1'}x_{2'}x_3=0$ adódik, ami azt jelenti, hogy x=0 helyen $y=\pm(-3a_5)^{0,5}$,

Ezek szintén különleges pontjai az elliptikus egyenletnek: szimmetrikus metszékei az x=0 helyen, az y tengelyen. Azonban bizonyos, hogy egész megoldást nem képezhetnek.

6.) A Fermat sejtés esetén $-a_5=a^pb^pc^p$. Vagyis x=0 helyen $y=\pm(-3a_5)^{0,5}=\pm\ (3a^pb^pc^p)^{0,5}$, amelyek bizonyosan szintén nem egészek, megoldást nem képezhetnek.

Természetesen még sok hasonló következtetés lenne tehető az elliptikus görbék más pontjaira is, amelyek a kanonikus alakban kevésbé észlelhetők. Ám közülük az a legfontosabb, hogy ***$q_1=0$*** esetén az ismertetett sajátosságok ***bármely páratlan hatványra,*** **beleértve a p=1 esetet is, érvényesek**, és hogy azok előállításuk módja és strukturális adottságaik révén valamennyien egy csoportot alkotnak!

Tekintsünk valamely koordinátarendszert, amelynek vízszintes tengelye a három x gyök szorzata (q_3), a függőleges pedig: y.

A 2.) következtetés alapján y lehetséges egész megoldásai csak az x tengelytől legalább 6 egységnyi távolságra lévő egyeneseken helyezkedhetnek el, közbenső pontok nélkül.

Ami persze nem zárja ki, hogy egy másik hasonló diagramon, amelyen csupán maguk az x gyökök külön vannak feltüntetve, nem lehetnének találhatók olyan pontok, ahol az x változó szintén egész. Sajnos azonban, olyan közbenső pontok, amelyek az y koordináta mentén a folytonosságot biztosíthatnák, nem lennének rajta! Olyan lenne tehát, mint valamely „diszkrét" fonalakból lazán szőtt ruha - ugyan felvehető, ám mintha nem is lenne! Persze lehetséges, hogy mindez csak a ma már feleslegesnek tartott „hatványösszeg-elmélet" szemszögéből látszódik így?

Vagyis, hogy $q_1=0$ feltétel. p>0 esetén x;y egész gyökpárjai ugyan lehetségesek, azonban sehol **nem alkothatnak folytonos elliptikus függvényt?** Akkor viszont talán nem is valódi, hanem csak valamiféle különc (kvázi, pszeudó vagy bármilyen más) elliptikus függvények ezek? Ha pedig nem azok, akkor milyen értelemben lehetne reájuk is vonatkoztatni bármely, csak elliptikus egyenletekre érvényes feltételrendszert - pld. akár a Taniyama-Shimura-Wiles tételt is? Milyen alapon mondható a Fermat azonosságból képzett „pszeudo-elliptikus" egyenletre, hogy moduláris formai kapcsolata kellene, hogy legyen, mert ha nincs, akkor nem is létezhet?

Hiszen akkor talán - az előzőek szerint - nem létezhetne a $q_1=a+b-c=0$ azonosság sem? De azt már **nem**! Mert legalább az hadd létezhessen! Hiszen a Fermat sejtés is az 1. fejezetben adott bizonyítási formulájával úgy igazolható csupán, hogy közben mégsem igaz, mert vannak megoldásai - a **megismerhetetlen, „irracionális, egészek**". Furcsa paradoxon ez, amelyhez a „mindenható logikán" túl egy kis filozófia sem nélkülözhető.

A végzett elemzés alapján még számos érdekes kérdés lenne feltehető, és megválaszolható...

A fentiek ismeretében azonban a kívülálló már nem gondolhatja túl meggyőzőnek egy olyan bizonyítási formula létezését, hogy „...ha a Taniyama-Shimura sejtés: *igen*, akkor a Fermat sejtés is: *igen*!”

Ám ha a tudományok országának királynője, a *Matematika* már rábólintott, akkor egy „átutazó” a kíváncsi szemlélődésen túl milyen okkal-joggal merészelne kételkedni benne?

Mindez egyébként sem változtathat semmit azon a tényen, hogy A. Wiles, és Alkotótársai munkája nyomán a Matematika is jelentős, méltán ünnepelhető lépést tett előre.

Ami azonban nem ok arra, hogy továbblépés ne történjen! Akár úgy is, hogy előbb kicsit - visszalépünk. Hátha onnan jobb út indítható?

Budapest. 2009.07 (Javított kiadás)

3 A Fermat sejtés számvektor-algebrai bizonyítása (sejtése)

Mi az, hogy számvektor-algebra? Most csak annyi mondható róla, hogy talán Fermat gondolkodása folytatódik benne, aki már akkor meglátta, (vagy még láthatta) hogy az algebrának, a matematikának más útjai is lehetségesek, mint amelyen a XVII. században meglódult és szétágazódva a mai napig töretlenül halad.

Továbbá még az, hogy a számok egy valódi, a tudatos létezés gondolatköréhez illeszkedő, mégoly egyszerű „filozófiai" definíciója nélkül lehetetlen megismerni, vagy létrehozni valamely egységes matematikát! Márpedig ilyen meghatározás - bármennyire is hihetetlennek tűnik - jelenleg nem ismert! Emiatt pedig nemcsak a felső, hanem az általános matematikai ismeretek között is gyakran nehéz fellelni összefüggést.

Hogy egészen egyszerű kérdések nemcsak hogy megválaszolásra, hanem még felvetésre sem kerülnek. Például, hogy ha lehetséges, hogy x^3 =1*1*1, akkor az x^3-1=0 egyenlet megoldása miért nem 1*1*1, hanem az egységgyökök szorzata?

Szóval, a matematika elindult, és a kívülállók szemszögéből hihetetlen távolságra jutott egy olyan úton, amely talán a XVII. században ágazott el. Nem lehet, hogy ez a hatalmas ugrás már maguknak a matematikusoknak is kicsit sok, csak talán nem szólnak róla?

Szólnak, persze.... R. Langlands (Princetoni professzor) már évtizedekkel korábban a matematika egységesítését igényelte! Az első eredmény ebben éppen A. Wiles munkája volt!

Fermat akkori gondolat-csíráit azonban belepte az idő pora, és a matematika mások által másképpen kiszélesített diadalútja. Így most rossz érzés elismerni, hogy annak vélt folyamodványa: a **számvektor-algebra** ma még messze nem befejezett, sőt alig elkezdett tudomány, s így talán helytelen beszélni is róla...

Vagy talán mégsem? Hiszen alkalmazásai szükségesek és fontosak lehetnek?

Valamennyi keveset tehát mégis kellene már szólni róla...

Legalább annyit, hogy a „**számok, a tudatos létezés megismerhető (nem megismerhető) elemi „egyedei"**, éppen úgy, mint bármi más: dolog vagy fogalom, élő vagy élettelen.

És mert így van, ugyanazon törvények érvényesek reájuk, mint bármi másra.

Egyebek között az **„Egyediség Törvénye"** is, amelyet a jelenlegi matematika hírből sem ismer.

Amelynek legelső megnyilvánulása az a kérdés, hogy „Ki vagy?" (s nem pedig, hogy „mi vagy", mert az a rendeltetésről szól). Kérdés, amit csak közvetlenül, *(elsőfokon)*, és csupán egyetlen, jól körülhatárolt, tulajdonságokkal és névvel rendelkező „egyedhez" lehet intézni, a matematikában például így: $(x-x_1)=0$. Mert az egyed azonosítására egyedül ez a kérdés szolgálhat, ami pontosan emiatt az algebrai egyenletek gyöktényezős alakjának nélkülözhetetlen eleme. Mert minden, ami megismerhető, valahol erre a kérdésfeltevésre visszavezethető, mert minden ilyen elemi egyedekből építkezik. Ami miatt nem mindegy az sem, hogy a kérdést $(x-a)=0$, vagy pedig $(x-a^p)=0$ alakban tesszük fel. Vagyis hogy megkérdőjelezhető annak a műveletnek a jogossága is, amelyet pedig a szerző is alkalmazott, a Fermat azonosságot az elliptikus egyenletbe helyettesítve. Holott tudja, hogy ily módon néhány vizsgálati lépcsőfokot „megtakarítva" számos információt (elegendőt akár a Fermat sejtés bizonyítására is) elveszített, vagy összemosott! Mert az „egyediséggel" rendelkező számokkal végzett műveletek sokban el kellene, hogy térjenek attól a gyakorlattól, amelyet a matematika ma megenged, látszólag egyszerűsítve, valójában pedig egyre átláthatatlanabbá téve a feladatát.

Azonban e tanulmány keretében még reménytelen és hibás szándék lenne a számvektor algebra alapjait tovább részletezni.

Inkább valamiféle példa lenne hasznosabb - akár a Fermat sejtés megoldása is!

Szerző azonban kéri a tisztelt Olvasó megértését, hogy azzal kapcsolatos állásfoglalását most még szintén csak egyfajta „sejtésnek" tekintse.

Mentségéül szolgáljon, hogy valamely sejtéssel szembeni bizonyítás amúgy sem kérhető a szerzőjétől számon, mert azt önmagának vagy másoknak csak később kell cáfolnia, vagy bizonyítania.

Álljon tehát a következő, új problémafelvetés a már megoldott Fermat sejtés helyébe:

Sejtés (Tétel?):

„A Nagy Fermat sejtés Fermat, és más szerzők által adott leírásai eleve nem voltak megfogalmazhatók, mivel a „számvektor-algebrában" maguk a számok, a szorzás, hatványozás és fordított műveleteik az algebrában ismert módon nem értelmezhetők."

Vagyis hogy maga a Fermat sejtés is voltaképpen felírhatatlan, tehát „irracionális".

Korai még a válasz, hogy a fenti állítás hogyan értelmezhető, azonban mindez már úgy is az új sejtés részét képezi, amely még hosszú időre „munkát" adhat a szerzőnek és másoknak is - amennyiben érdekli őket...

Ugyanakkor belátható, hogy a fentinél „rövidebb" megoldása a Fermat sejtésnek szinte elképzelhetetlen lenne, hiszen csupán egyetlen mondat. Feltéve persze, hogy a tisztelt Olvasó el tud tekinteni attól, hogy Fermat még ennél is rövidebb megoldást adott: „...nem fér el... (mert pont nélküli végtelen?)". Tehát, hogy a megoldás *nem megismerhető, irracionális*.

Továbbá magának a számvektor-algebrának a létezése hiányától is el kellene tekintenie, mert annak még sokáig, és sokak által fejlődnie kell.

Hiszen el kell ismerni, hogy az „majdnem a semminél" tart még! Vajon az kevés, vagy sok?

Azonban a formálódó „**számvektor algebra**" oly mértékben eltér mindattól, amit ma **algebrának**, illetve összefoglalóan **matematikának** gondolunk, hogy talán nem is nevezhető annak. Ezért a legközelebb megjelentetni tervezett kötet talán ezt a címet viselné:

„NEM - MATEMATIKAI MÓDSZEREK.
BEVEZETÉS A SZÁMVEKTOR-ALGEBRÁBA"

Persze, csak ha megjelenik. Mert ha valamiről bebizonyosodik, hogy érdektelen, vagyis hogy haszontalan, akkor meggondolandó hogy további időt, munkát fordítsanak reá.

Ám nem lenne helyes ilyen gondolattal befejezni-

Forrai György

2009-07-26 (I. javítás)