[1]

1993. júniusának utolsó napjaiban egy tudományos szenzációtól voltak hangosak a napilapok világszerte: Andrew Wiles angol matematikus megoldotta a matematika egyik legnevezetesebb problémáját, bizonyítást adva a *Fermat-sejtésre.* A következő néhány oldalon erről a különös problémáról lesz szó.

Mi lehet az a matematikai kérdés, amiről többhasábos cikkek jelennek meg a nagy napilapokban? Nos, a Fermat-sejtés ártatlanul egyszerűnek hangzik:

Ha $n > 2$ egész szám, akkor nincsenek olyan nullától különböző x, y, z egészek, melyekre $x^n + y^n = z^n$ teljesül.

Egyszerű állítás, nem kell sok előismeret a megfogalmazásához. Valósággal csábítja az embert, hogy kezdjen el számolgatni, gondolkodni rajta. Hosszú története során sokakat megejtett különös varázsával. Többek számára jelentette azt a meghatározó élményt, ami a matematikusi pálya választásához vezette őket. Személyes ismerőseim között is van ilyen kolléga.

A kérdés eredetét kutatva i.e. 250-ig tekinthetünk vissza. Ezidőtájt született Diophantosz nagyhatású munkája, az *Aritmetika,* ami – ismereteink szerint – először adott közre valamelyes rendszerbe foglalva számelméleti és algebrai eredményeket. Íme egy jellegzetes feltevés a II. Könyvből: *osszunk fel egy adott négyzetet két négyzetre.* A probléma, és a Diophantosz által közölt megoldás a következő pontosabb „modern" megfogalmazást sugallja: *keressük az $x^2+y^2 = z^2$ egyenlet egész megoldásait,* szokásos nevükön a pitagoraszi számhármasokat.

Nem nehéz meghatározni az összes ilyen hármast. Az általánosság különösebb sérelme nélkül szorítkozhatunk arra az esetre, amikor mindhárom szám pozitív, semelyik kettőnek nincs közös prímosztója, és x páros (nevezzük ezeket primitív hármasoknak). Ekkor az $\frac{x^2}{4} = \frac{1}{2}(z+y) \cdot \frac{1}{2}(z-y)$ összefüggést használva kapjuk, hogy $\frac{1}{2}(z+y)$ és $\frac{1}{2}(z-y)$ egészek, sőt négyzetszámok:

$$\frac{1}{2}(z+y) = u^2, \qquad \frac{1}{2}(z-y) = v^2.$$

A gondolatmenetet folytatva könnyen adódik, hogy a primitív hármasok mind megkaphatók

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2$$

alakban, ahol $u > v$ pozitív, relatív prím egészek, és az egyikük páros.

Pierre Fermat (1601–1651) toulouse-i jogász kedvtelésből foglalkozott matematikával. Mégis olyan sok és fontos eredmény fűződik a nevéhez, hogy méltán tartják kora egyik legjelentősebb matematikusának. Fermat olvasta az *Aritmetikát,* mégpedig nagy figyelemmel, amire számos, a könyv margójára írt megjegyzéséből következtethetünk. A fenti, a négyzet felosztásával kapcsolatos részhez az alábbi széljegyzetet fűzte: *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.*

Magyarul – Bródy Ferenc míves fordításában – mindez így hangzik: *Nincsen mód viszont felosztani köböt két köbre, sem négyzetes négyzetet két négyzetes négyzetre, és általában a négyzeten túl a végtelenig semmiféle hatványt két ugyanolyan nevezetűre; mely dolognak igazán csudálatos bizonyítását találtam. Szűkebb a margó, semhogy befogadná.*

A Fermat-sejtést tehát egy olyan állításként fogalmazta meg, melyet bizonyítani tud. Azóta eltelt kb. 350 év, és egészen napjainkig senkinek nem sikerült bizonyítást találnia. Ezért általános a vélemény, hogy Fermat valószínűleg tévedett, elnézett valamit, és nem volt *igazán csudálatos bizonyítása.* Az 1800-as évek elejére minden más (levelekben és margójegyzetekben fennmaradt) állítását sikerült tisztázni, csak ez az egy állt ellen makacsul minden kísérletnek. Innen származik a sejtés másik gyakran használt elnevezése: Fermat Utolsó Tétele.

Pedig erőfeszítésben nem volt hiány. Az $n = 3$ és $n = 4$ esetekkel Fermat maga is foglalkozott, utóbbira adott gondolatmenete fennmaradt (szintén lapszéli jegyzetek formájában). Pontosabban azt igazolta, hogy az $x^4 + y^4 = z^2$ egyenletnek nincs csupa nem nulla egészekből álló megoldása.

Röviden bemutatjuk Fermat bizonyítását. Egy tanulságos módszerről van szó, mely több más problémára is alkalmazható, és amelynek a ma használt igen kifinomult változatait *Fermat-leszállásnak* nevezik.

Ha van az $x^4+y^4 = z^2$ egyenletnek csupa pozitív egészekből álló megoldása, akkor van olyan is, melyben z a lehető legkisebb. Ekkor (x és y esetleges felcserélése után) x^2, y^2 és z egy primitív pitagoraszi hármast alkot. Vannak tehát olyan u, v pozitív egészek, melyekre

$$x^2 = 2uv, \quad y^2 = u^2 - v^2, \quad z = u^2 + v^2.$$

A $v^2 + y^2 = u^2$ egyenlőség szerint v, y, u is egy pitagoraszi hármas, ami primitív is, mert különben x^2, y^2, z sem volna primitív. Ismét alkalmazhatjuk a primitív hármasok leírását. Alkalmas t és s pozitív egészekkel érvényesek a következők:

$$v = 2ts, \quad y = t^2 - s^2, \quad u = t^2 + s^2.$$

Az érvelés befejező részét feladatok formájában az olvasóra hagyjuk.

[1] Köszönetet mondok Bródy Ferencnek, Ivanyos Gábornak és Szabó Rékának a kézirattal kapcsolatos értékes észrevételeikért.

1. feladat. Mutassuk meg, hogy t, s és u is négyzetszámok.

A feladat állítása szerint $t = a^2, s = b^2$ és $u = c^2$, ahol a, b, c pozitív egész számok.

2. feladat. Igazoljuk, hogy $a^4 + b^4 = c^2$ és $c < z$.

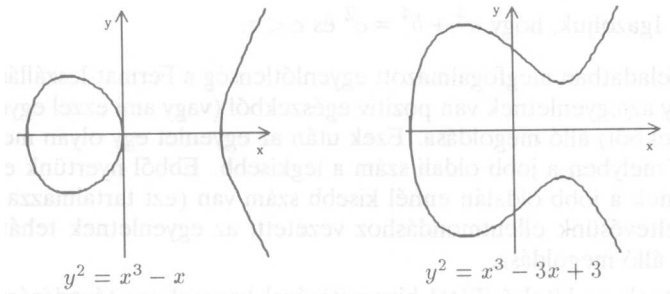
A 2. Feladatban megfogalmazott egyenlőtlenség a Fermat-leszállás lényege. Feltettük, hogy az egyenletnek van pozitív egészekből (vagy ami ezzel egyenértékű: nem nulla egészekből) álló megoldása. Ezek után az egyenlet egy olyan megoldásából indultunk ki, melyben a jobb oldali szám a legkisebb. Ebből nyertünk egy olyan megoldást, aminek a jobb oldalán ennél kisebb szám van (ezt tartalmazza a 2. Feladat). Kiinduló feltevésünk ellentmondáshoz vezetett, az egyenletnek tehát nincs pozitív egészekből álló megoldása.

Fermatnak az Utolsó Tétel bizonyításával kapcsolatos tévedéséről több elképzelés is van. Egy népszerű nézet szerint feltehetőleg arra gondolt, hogy a leszállás módszere könnyen átvihető tetszőleges n kitevőre. Ilyen általánosítást azonban senkinek sem sikerült kidolgozni.

Az $n = 4$ kitevő kizárása után elég a kérdést azokban az esetekben nézni, amikor $n > 2$ egy prímszám (miért?). Az $n = 3$ esetet *L. Euler* oldotta meg 1753-ban. *L. Dirichlet* és *A. M. Legendre* találtak bizonyítást $n = 5$-re 1825-ben. Ugyancsak Dirichlet nevéhez fűződik az $n = 14$ kitevő (1832-ben), az $n = 7$ esetet pedig *G. Lamé* tudta kezelni 1839-ben. Az 1847. év fontos volt a sejtés történetében. Ekkor született az első nevezetes hibás bizonyítás, méghozzá olyan neves matematikusok műveként, mint *A. Cauchy* és G. Lamé (avagy nem csak a matekórák dolgozataiba csúsznak be gyógyíthatatlan hibák). A másik – sokkal fontosabb – fejleményt *E. E. Kummer* eredményei jelentették. Kummer egy egészen más jellegű számelméleti probléma vizsgálata során dolgozott ki olyan eszközöket, melyekkel az Utolsó Tétel több kitevő esetére is igazolható. Módszere működik például a 37, 59 és 67 kivételével minden 100-nál kisebb n prímre. Kummer munkája tekinthető az *algebrai számelmélet* hajnalának. Kummer eredményeire építve *H. S. Vandiver* (1920 körül) igazolta a sejtést $n < 100$-ra. A nevek és az évszámok mutatják, hogy kiváló matematikusok foglalkoztak a problémával, de ennek ellenére a haladás meglehetősen lassú volt. Komoly előrelépést jelentettek az olyan feltételek, melyek révén számítógépek segítségével lehet vizsgálni a problémát nagyobb kitevőkre. Ezek segítségével 1992-re $n < 4\,000\,000$-ig igazolták a sejtést.

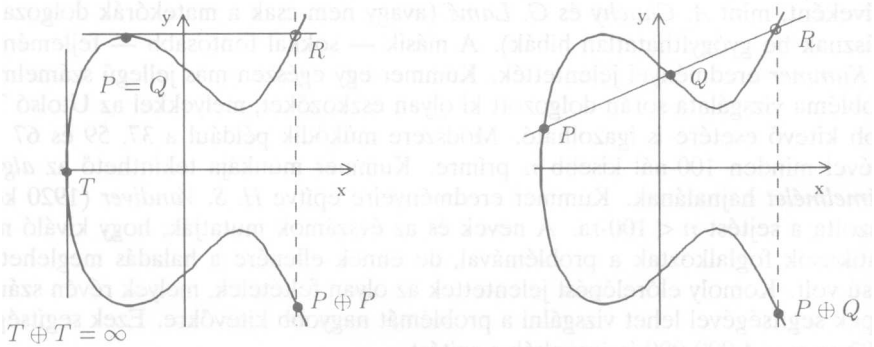
Fontos mérföldkő *Gerd Faltings* (1983) egy általános, sok egyenletre érvényes végességi tétele, melyből következik, hogy egy adott $n > 2$-re az $x^n + y^n = z^n$ egyenletnek csak véges sok primitív egész megoldása lehet.

A történet végén főszerep jutott az *elliptikus görbéknek*. Mielőtt az eseményekről beszélnénk, vessünk egy pillantást ezekre a rendkívül érdekes, gazdag struktúrájú objektumokra. Elliptikus görbén egy $y^2 = f(x)$ alakú egyenlettel definiált síkbeli görbét értünk, ahol $f(x)$ egy $ax^3 + bx^2 + cx + d$ alakú polinom, melynek három különböző gyöke van. A görbe *diszkriminánsa* a $\Delta = (a_1 - a_2)^2(a_1 - a_3)^2(a_2 - a_3)^2$ mennyiség, ahol a_1, a_2, a_3 az $f(x)$ polinom gyökei. A gyökök különbözősége egyenlő a $\Delta \neq 0$ feltétellel. A következő *ábra* két elliptikus görbe grafikonját mutatja.



1. ábra. Elliptikus görbék

Az elliptikus görbéknek sok szép geometriai és számelméleti tulajdonsága van. Egy ilyen érdekes tulajonság, hogy lehet egy az összeadásra emlékeztető műveletet definiálni a görbe pontjain. Ebből a célból még vegyünk a görbéhez egy ∞-nel jelölt „pontot”. Erről a mágikus pontról feltételezzük, hogy rajta van minden függőleges (az y-tengellyel párhuzamos) egyenesen, és hogy az x-tengelyre vonatkozó tükörképe önmaga. Ezután a görbe P és Q pontjainak $P \oplus Q$ összegét a következő eljárással határozhatjuk meg: legyen a P, Q pontokon átmenő egyenes és a görbe harmadik metszéspontja R; ennek az x-tengelyre való S tükörképe (ami szintén pontja a görbének) a $P \oplus Q$ összeg. Ha $P = Q$, akkor az összekötő egyenesükön a görbe P-beli érintőjét kell érteni. Előfordulhat az is, hogy R megegyezik a P, Q pontok valamelyikével, ekkor az egyenes R-ben érinti a görbét. Végül legyen $\infty \oplus \infty = \infty$.



2. ábra. Összeadás elliptikus görbe pontjain

A $\oplus$ műveletre teljesülnek az összeadás szokásos azonosságai, és a ∞ játssza a 0 szerepét: a görbe tetszőleges P, Q, R pontjaira $P \oplus Q = Q \oplus P$, $\infty \oplus P = P$, $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$. Ezek a tulajdonságok, kivéve az utolsót, az asszociatív szabályt, könnyen igazolhatók. Szintén egyszerű belátni, hogy a görbe tetszőleges P pontjához a P-nek az x-tengelyre való R tükörképe az egyetlen olyan pont, melyre $P \oplus R = \infty$ teljesül. Az összeadásnál megszokott értelemben használhatjuk tehát az $R = \ominus P$ jelölést. Jelöljük E-vel az $y^2 = x^3 - 2x$ görbét.

3. feladat. Határozzuk meg az E görbe $P \oplus P$, $P \oplus Q$ és $P \oplus R$ pontjait, ahol $P = (0,0)$, $Q = (\sqrt{2}, 0)$ és $R = (2,2)$.

Két pont összegének a koordinátái kifejezhetők az összeadandók koordinátáival és az elliptikus görbe a, b, c, d együtthatóival, mégpedig csak a $+, -, \cdot, /$ műveletek segítségével. Ebből két fontos következtetés vonható le. Egyik, hogy a $\oplus$ művelet definiálható algebrai úton, koordinátákkal. Másfelől, ha az a, b, c, d együtthatók mind racionális számok, akkor racionális koordnátájú pontok összege is racionális pont lesz (a ∞-t racionális pontnak tekintjük). Szemléltetésül nézzük, hogyan számíthatók ki az E görbe egy $P = (x, y)$ pontjára a $P \oplus P$ pont u, v koordinátái:

$$(*) \qquad u = -2x + \left(\frac{3x^2 - 2}{2y}\right)^2, \qquad v = -y + \frac{3x^2 - 2}{2y}(x - u).$$

A kifejezések nem értelmesek, ha $y = 0$. Ez azt a tényt tükrözi, hogy ekkor $P \oplus P = \infty$; másképpen fogalmazva, a görbe P-beli érintője függőleges.

Ha az a, b, c, d számok egészek, akkor tetszőleges p prímszámra tekinthetjük az $y^2 \equiv ax^3 + bx^2 + cx + d \pmod p$ kongruenciát. Ennek egy megoldásán egy egész számokból álló (u, v) párt értünk, melyre $v^2 - au^3 - bu^2 - cu - d$ osztható p-vel. Vegyük észre, hogy csak az u, v számok p-vel való osztási maradékán múlik, hogy az (u, v) pár megoldása-e. Ezért a megoldásokról teljes képünk marad, ha kikötjük még a $0 \le u, v < p$ egyenlőtlenségeket. Szokásos még ezeket a megoldásokat a görbe modulo p pontjainak is nevezni. Az E görbe modulo 5 pontjait rövid számolás után megkaphatjuk, észrevéve, hogy v^2 maradéka csak 0, 1 vagy 4 lehet: $(0,0)$, $(1,2)$, $(1,3)$, $(2,2)$, $(2,3)$, $(3,1)$, $(3,4)$, $(4,1)$, $(4,4)$.

Egy egész együtthatós F elliptikus görbe és egy p prímszám esetén jelölje $m_p(F)$ az F görbe modulo p pontjainak a számát. Ezzel a jelöléssel az előbbiek alapján $m_5(E) = 9$.

4. feladat. Mutassuk meg, hogy ha F egy egész együtthatós elliptikus görbe, és p egy prímszám, akkor $m_p(F) \le 2p$.

Néhány „rosszul viselkedő" prímszámot kivéve – ezek a prímek mind osztói a Δ diszkriminánsnak – értelmezhető a $\oplus$ összeadás az egész együtthatós görbék modulo p pontjain is. Itt is szükség van a ∞ pontra, és két pont összegét ugyanazokkal az algebrai kifejezésekkel számíthatjuk ki, amelyek a valós pontokra megadják az összeg koordinátáit. Például az E görbe modulo 5 pontjaira használhatók a $(*)$ formulák, ha a $P \oplus P$ összeget akarjuk meghatározni.

5. feladat. Adjuk meg az E görbe egy olyan $P \ne \infty$ modulo 5 pontját, melyre $P \oplus P \oplus P \oplus P \oplus P = \infty$.

Az elliptikus görbék számelméleti tulajdonságainak vizsgálata (egész koordinátájú pontok, modulo p pontok, a $\oplus$ művelet hatása ezeken) ebben a században vált intenzívvé. Érdekességként azért megemlítjük, hogy az egyik első ilyen jellegű állítást szintén Fermat margószéli feljegyzései között találták. Arról a tényről van szó, hogy az $y^2 = x^3 - 2$ egyenletnek csak két egész megoldása van, nevezetesen $(3, \pm 5)$. Igen szép és fontos „modern" eredmény *L. J. Mordell* tétele (1921): egy racionális együtthatós görbének van véges sok racionális koordinátájú pontja, melyekből az összes racionális pont megkapható a $\oplus$ művelet alkalmazásával. A modulo p pontokkal kapcsolatban *H. Hasse* (1934) bizonyította a $|p - m_p(F)| \le 2\sqrt{p}$ egyenlőtlenséget.

Az 50-es évek második felében *Taniyama Yutaka, Shimura Goro* japán, és *André Weil* francia matematikusok fogalmaztak meg egy nagy jelentőségű, egyebek között a racionális együtthatós elliptikus görbékre is vonatkozó sejtést (TSW-sejtés). Az ebben foglalt állítások kimondásához nagyon sok előkészület kellene, amire itt nem vállalkozhatunk. Érzékeltetésül csak annyit, hogy a TSW-sejtés szerint tetszőleges racionális együtthatós $y^2 = ax^3 + bx^2 + cx + d$ görbéhez vannak olyan *különleges* f és g függvények, melyekre $f(z)^2 = ag(z)^3 + bg(z)^2 + cg(z) + d$ teljesül. A sejtés lényege éppen ezeknek a különleges függvényeknek a tulajdonságaiban rejlik. A TSW-sejtésnek van egy (nem kevésbé bonyolult) számelméleti megfogalmazása is. Ennek érdekessége, hogy az állítás csupán a görbe modulo p tulajdonságain, sőt lényegében csak az m_p $(p = 2, 3, 5, \ldots)$ számokon múlik. A TSW-sejtéssel kapcsolatos első jelentős eredményt Shimura érte el 1971-ben, megmutatva, hogy teljesül görbék egy családjára.

A következő fontos esemény már összefűzi a két szálat, az Utolsó Tételt és az elliptikus görbéket. 1985-ben *Gerhard Frey* német matematikus a Fermat egyenlet tanulmányozása során meglepő kapcsolatot talált. Tegyük fel, hogy $n > 3$ prím és a páronként relatív prím a, b, c egészekre teljesül, hogy $a^n + b^n = c^n$, b páros, és $a + 1$ osztható 4-gyel. Könnyű meggondolni, hogy ha az Utolsó Tétel nem igaz, akkor ilyen n, a, b, c négyes létezik. Egy ilyen „megoldáshoz" Frey a következő egész együtthatós elliptikus görbét rendelte (ún. Frey-görbe):

$$y^2 = x(x - a^n)(x + b^n).$$

A görbe diszkriminánsa $\Delta = a^{2n}b^{2n}c^{2n}$ szép szimmetrikusan függ az a, b, c számoktól. A német kutatót számításai ahhoz a meggyőződéshez vezették, hogy a *Frey-görbékre nem teljesülhet a TSW-sejtés*. Volt elképzelése a bizonyításról is, de egy jelentős részkérdést nem tudott kezelni. Ez viszont sikerült *Kenneth A. Ribet* amerikai matematikusnak 1986-ban. Ribet munkája nyomán tehát világossá vált, hogy a TSW-sejtésből következik az Utolsó Tétel.

Talán nem teljesen túlzás azt mondani, hogy innentől *Andrew Wiles* asztalára került a kérdés. Wiles pályája kezdete óta foglalkozik elliptikus görbék aritmetikájával. Első, – tanárával, *J. Coates*-szal közösen elért – messzire mutató eredménye e tárgyban 24 esztendős korában, 1977-ben jelent meg. A princetoni egyetem professzoraként már régóta a kérdéskör egyik vezető szaktekintélyének számít. A hírek szerint Ribet eredményének közzététele óta dolgozott a TSW-sejtés igazolásán. Matematikai eredmények és módszerek félelmetes mennyiségű és mélységű arzenálját kellett bevetnie. Ezek között van annyira új és friss is, melyet csak 1992-ben publikáltak. Végül, ahogy azt 1993. június 23-án Cambridge-ben tartott előadásán bejelentette, igazolta a TSW-sejtést elliptikus görbék egy nagy osztályára, melybe, ha léteznének, beletartoznának a Frey-görbék is. Ez az osztály a *félig stabil* görbékből áll. A félig stabilitás feltétele a modulo p redukált görbékre vonatkozó kikötés, ahol $p|\Delta$. A feltételt nem nehéz megérteni $y^2 = (x - A)(x - B)(x - C)$ alakú görbék esetén, ha A, B, C egészek. A modulo p redukált görbe akkor tesz eleget a kikötésnek, ha az A, B, C számok p-vel osztva nem mind adják ugyanazt a maradékot ($p = 2$, 3-ra valamivel bonyolultabb a helyzet, ezt nem részletezzük). Felhasználva, hogy a, b, c páronként relatív prímek, a Frey-görbére $p > 3$ esetén egyszerű ellenőrizni a félig stabilitás feltételét.

Úgy tűnik tehát, hogy az Utolsó Tétel végre bizonyítást nyert. Wiles erőfeszítésének mértékét, az eredmény nehézségét esetleg érzékelteti, hogy a bizonyítás kézirata kb. 200 oldal terjedelmű. Becslések szerint több mint ezer oldal lenne az érvelés leírása, ha csak a szokásos egyetemi anyagban tárgyalt tényekből indulnánk ki.

Egy ilyen hosszú, bonyolult bizonyítás ellenőrzése sok időt igényel. Beletelik még egy időbe, mire a szakértők teljesen megbizonyosodnak a helyességéről. Nem teljesen elképzelhetetlen, hogy valahol hibát találnak a részletekben.[2] Az azonban már ma is világos, hogy óriási előrelépés történt a TSW-sejtéssel kapcsolatban. Nem véletlen tehát, hogy sokan – ezek közül e sorok írója sem kivétel – az emberi gondolkodás egyik csodálatos, fényes csúcsteljesítményének tartják Wiles munkáját.

Végezetül álljon itt egy derűs mozzanat az Utolsó Tétel bizonyítása körül világszerte megnyilvánuló érdeklődésről és izgalomról. San Francisco-ban a Szépművészetek Palotájában július végén volt egy rendezvény, ahol a szakértőknél szélesebb közönség számára mutatták be a problémát és Wiles eredményét. Az előadók között volt Ribet is. A több mint ezer fős befogadó képességű terem zsúfolásig megtelt, és legalább kétszáz érdeklődőt el kellett küldeni. Alighanem ez volt az első matematikai tárgyú rendezvény a történelemben, ahol a jegyüzérek is megjelentek. Az eredetileg 5 dolláros belépőjegyek 50 dollárért keltek el. Azóta is tűnődöm: honnan van ennyi érzékük a San Francisco-i jegyüzéreknek az aritmetika szépségeihez?

[2] A legutolsó hírek szerint valóban nem teljes a bizonyítás. A szerk.