

Leonhard Euler (1707–1783)

EULER LEONARD a matematika egyik fejedelmének nevét minden olvasónk ismeri. Az idén van születésének kétszázötvenedik évfordulója. Ez igen nagy idő, mégis az évfordulóról az egész civilizált világon megemlékeznek, ami világosan mutatja Euler nagy jelentőségét a matematika történetében, sőt jelenére kiható kimagasló fontosságát. (Rendkívüli nagysága indokolja, hogy lapunk is megemlékezzék az évfordulóról.)

Euler 1707. április 15-én született egy Basel melletti kis faluban, ahol atyja kálvinista lelkész volt, aki fiát is papnak szánta. A baseli egyetem, ahova Euler került, volt akkor a matematikában a világ legnevezetesebb egyeteme, ahová messze földről gyülekeztek a tehetséges tanítványok, magyarok is. Tanáruk a világhírű BERNOULLI¹ (ejtsd: bernujji) János nagy matematikus és lelkes tanár, akinek két fia akkor szintén az egyetem hallgatója volt. Euler meleg barátságot kötött velük. Az ifjú Euler tehát nem lett pap, hanem azt az utat követte, amelyet tehetsége számára kijelölt. Matematikus lett. Az ifjú Bernoulli rábeszélésére 20 éves korában Pétervárra, a mai Leningrádba ment, ahol a Tudományos Akadémia főtitkára lett. 1741-ben II. Frigyes porosz király meghívására a berlini Tudományos Akadémiához került, de 25 év múlva visszament Pétervárra, ahol haláláig maradt. Fiatalon, 28 éves korában, elvesztette egyik szemét, 64 éves kora, 1771 óta, teljesen vak. Tudományos munkásságát mégsem hagyta abba. Egyik inasának, aki azelőtt szabólegény volt, tollba mondotta híres Algebráját, amely nemcsak a mai középiskolai anyagot tartalmazza, hanem jóval többet. A könyv annyira világos és oly könnyen érthető, hogy belőle a szabólegény alaposan megtanulta az algebra elemeit, úgy, hogy Euler diktálása alapján le tudta írni Euler gondolatait. Euler matematikai irodalmi tevékenysége tehát vaksága alatt sem szűnt meg, sőt talán még bővebben ömlött. A könyvet ma is nagyon ajánljuk németül vagy franciául tudó olvasóinknak.

Euler, ámbár a kor legnevezetesebb uralkodóinak udvartartásában élt, értéke tudatában sohasem süllyedt udvaroncá, mindig megmaradt büszke svájci polgárnak. II. Katalin cárnőnél – aki maga is jelentékeny személyiség – egy tábornok szavára tette, miért Euler, a civil az Akadémia elnöke és nem ő, a tábornok. A cárnő azt felelte: „Tábornok, Bátyuskám, mindenki lehet, akit ÉN annak kinevezek, de Eulerré még én sem nevezhetek ki senkit.”

Euler a legtermékenyebb matematikus. Nyomatott munkáinak száma 862, köztük több remek vastag kötet. Munkássága a matematika minden ágában korszakalkotó. Egyetlen más matematikus sem volt oly sokoldalú, mint ő, joggal elmondható, hogy egész más matematikát hagyott hátra, mint aminőt talált. A legfelsőbb matematikában messze kitolta tudásunk határait, de a legelemibb kérdésekbe is döntően szólt bele. Az iskolai matematika mai egyszerű alakja Eulernek köszönhető. Ha bárki ma háromszögről beszél, általában csúcsait A , B , C -vel, szembenfekvő oldalait a , b , c -vel jelöli. Ez a természetes és áttekinthető jelölési mód Eulertől ered. A $\sin$, $\cos$, $\tan$, $\cot$ jelölések is Eulertől valók. Az $f(x)$, e , π jelöléseket is Euler vezette be. A 16. századbeli RHATICUS a derékszögű háromszög meghatározását 2 adatból 140 fóló oldalon tárgyalja, az az oly egyszerű mód, amelyet ma a II. osztályban tanulnak, Eulertől ered. Általában a trigonometria mai oly könnyű alakja Eulertől származik, a goniometria majdnem minden formuláját Euler vezette le, a gömbháromszögtan (ez ma nem iskolai anyag, de mindenkinek szüksége van rá, aki pl. csillagászattal foglalkozik) is mai alakját Eulertől nyerte, legtöbb formuláját Eulernek köszöni. A trigonometriai függvényeket dimenzió nélküli számértékeknek fogja fel, és a körön mind a négy síknegyedben ábrázolja, az előjeleket az egyes negyedekben először Euler állapítja meg helyesen. Az *analitikus geometria* feltalálói a 17. századbeli FERMAT (ejtsd: fermá) és DESCARTES (ejtsd: dékárt, az á rövid) csak egy tengelyt és a kezdőpontot használják, az ordinátatengelyt Euler vezette be.

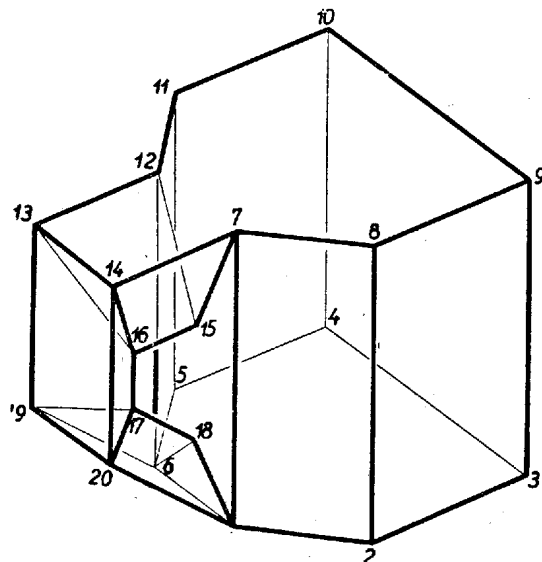
Kötetekre lenne szükség, ha Eulernek csak legfőbb eredményeiről be akarnánk számolni, hiszen 862 dolgozatának legtöbbje fontos és érdekes kérdésekre ad választ, gyakran többre is. Éppen azért csak néhány egyszerűen elérhető oly eredményének bemutatására szorítkozom, amelyek ifjú olvasóinkat érdekelhetik. A logaritmusnak mint a hatvány megfordításának, így tehát 7. alpművelet gyanánt való felfogása Eulertől származik. A 18. század elejének tudósai sokat vitatkoztak arról, mit kell a negatív szám logaritmusán érteni? A vitát Euler döntötte el, amikor megmutatta, hogy a logaritmus fogalmát célszerűen át lehet vinni a komplex számok körére is, de itt már a logaritmus végtelen sok értékű függvény, és a negatív szám logaritmusaként komplex szám.

A háromszög Euler-féle egyeneséről az iskolában tanultatok. A háromszög magassági pontja M , súlypontja S , és a körülírt kör középpontja O ebben a sorrendben egy egyenesen, az Euler-féle egyenesen fekszik, és $MS = 2 \cdot SO$. Az affinitás geometriai rokonságát is Euler vezette be. A Feuerbach-féle kört a francia szerzők Euler-féle körnek nevezik, mert ő ismerte fel először, hogy a háromszög oldalfelező pontjai, a magasságok talppontjai és a magasságok felső részeinek felezőpontjai ugyanazon körön fekszenek. (A FEUERBACH-kör elnevezés mégis jogos, mert az a tétel, hogy a Feuerbach-kör érinti a háromszög mind a négy érintő körét, Feuerbachtól származik.)

„Euler poliéder tétele” is iskolai anyag. Ez a tétel tulajdonképp régibb, már Descartes leveleiben is előfordul, de Euler önállóan fedezte fel, Descartes levelét ugyanis csak 80 évvel Euler halála után publikálták. Ez a tétel úgy szól, ha egy szögletes test lapjainak száma l , csúcsainak száma c , és éleinek száma e , akkor általában $l + c = e + 2$.

Mint ismeretes, ez az összefüggés *konvex* szögletes testekre mindig igaz, de *konkáv* egyenes vonalú testekre nem mindig áll fenn. Pl., ha a hasábhöz síklapokból álló fogantyút ragasztunk, a keletkezett testre (1. ábra) már nem áll a tétel.

¹A BERNOULLI család nevezetes a tudomány történetében, mert benne jóval 100 éven túl, több nemzedéken át öröklődött a kivételes matematikai tehetség.



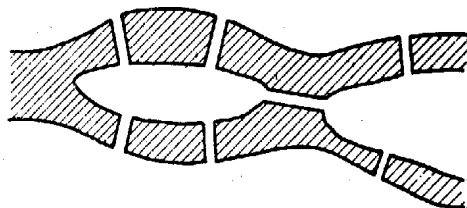
1. ábra

(Ábránkon $l = 16$, $c = 20$ és $e = 35$, tehát $l + c = e + 1$.) Újabban felteszik, hogy már az ógörög ARCHIMEDES is ismerte a poliéder tételt.

Most néhány, az iskola anyagában nem szereplő elemi természetű eredményét vagy bizonyítását fogom bemutatni.

Képzeljünk egy $6 \cdot 6 = 36$ mezű sakktáblát. Az Euler-féle „36 tiszt problémája” a következő: 6 ezredbeli 6 különböző rendfokozatú tiszt helyezkedjék el úgy, hogy az ugyanazon sorban vagy oszlopban elhelyezkedő tisztek között ne legyen két azonos ezredbeli vagy azonos rendfokozatú. Euler – ennél általánosabban – kimutatta, hogy ez lehetetlen, ha $4n + 2$ különböző ezredbeli, $4n + 2$ számú különböző rendfokozatú tisztet akarnánk így elhelyezni.

Egy másik ily egyszerű Euler-féle probléma a „Königsbergi hidak” problémája. Königsberg városát átszelő Pregel folyón átvezető hét híd helyzetét vázlatosan a 2. ábra mutatja.



2. ábra

A feladat, hogy kell a sétát berendezni, ha valamennyi hídon át akarunk menni, de mindegyiken csak egyszer, hogy kiinduló pontunkra visszatérjünk. Ha a kérdést a budapesti hidakra vonatkozólag akarnám feltenni, azonnal láthatnók, hogy a feltétel teljesíthetetlen, mert a Margitszigetre vezető mind a két híd három ágú, tehát sétánknál egy ág vagy kimarad, vagy kétszer kell útba ejteni. A königsbergi hidakhoz visszatérve, hasonlóképpen nézzük azokat a területeket, amelyekre három híd vezet, pl. a folyó deltáját jobb oldalt. Nyilván csak két eshetőség lehetséges, ha mindhárom hidat útba akarjuk ejteni, vagy kétszer bemegyünk a deltába, és egyszer távozzunk, vagy fordítva egyszer be, kétszer ki. A második esetben a séta a deltában kezdődött, különben nem távozhatnánk kétszer a deltából, ahová csak egyszer mentünk be, az első esetben hasonló okból a séta a deltában végződik. Amit a deltáról mondtunk, áll a folyó két pontjáról is, mert oda is három híd vezet, ahol tehát a sétának kezdődnie vagy végződnie kell. Ezek szerint (mint az ábra is mutatja) három oly terület van, ahol a sétának kezdődnie vagy végződnie kellene. Márpedig ez lehetetlen, a feladat tehát nem teljesíthető. Ez a probléma ugyebár játéknak, afféle matematikai mulatságnak tetszik, a valóságban azonban elvezet a mai matematika egyik fontos ágához, a topológiához.

A megokolás ugyan csak felsőbb matematikai megfontolásokkal lehetséges, de az eredmény egyszerű alakja és az iskola anyagával való összefüggése miatt bizonyítás nélkül megemlítem Euler fontos eredményeit az exponenciális és trigonometrikus függvények összefüggéséről. Az

$$e^{ix} = \cos x + i \sin x$$

Euler-féle formula ($i = \sqrt{-1}$, $e = 2,7172\dots$, a természetes logaritmus alapszáma) a legnagyobb matematikai felfedezések egyike. nx -re való alkalmazása adja az

$$e^{inx} = (\cos x + i \sin x)^n = \cos nx + i \sin nx$$

ún. MOIVRE-féle formulát, amelynek ez az egyszerű, ma használt alakja Eulertól való, és amely sok trigonometriai felfedezésének nyitja. Ugyaninnen erednek a logaritmusra vonatkozó már említett felfedezései. Alkalmazásként zárt alakban fogjuk írni a fenti összefüggés segítségével az

$$1 + \cos x + \cos 2x + \dots + \cos nx$$

és a

$$\sin x + \sin 2x + \dots + \sin nx$$

összegeket a

$$q = e^{ix} = \cos x + i \sin x$$

hányadosú

$$\begin{aligned} Q &= 1 + q + q^2 + \dots + q^n = \\ &= 1 + (\cos x + i \sin x) + (\cos 2x + i \sin 2x) + \dots + (\cos nx + i \sin nx) \end{aligned}$$

mértani sorban. Az első összeg a valós (i -t nem tartalmazó) rész, a második pedig a képzetes rész (i szorzója). Ha $q \neq 1$, azaz $x \neq 0$, akkor a mértani sort összegezve (és $q^{-\frac{1}{2}}$ -nel bővítve)

$$\begin{aligned} Q &= \frac{1 - q^{n+1}}{1 - q} = \frac{q^{-\frac{1}{2}} - q^{n+\frac{1}{2}}}{q^{-\frac{1}{2}} - q^{\frac{1}{2}}} = \\ &= \frac{\cos(-\frac{1}{2}x) + i \sin(-\frac{1}{2}x) - [\cos(n + \frac{1}{2})x + i \sin(n + \frac{1}{2})x]}{\cos(-\frac{1}{2}x) + i \sin(-\frac{1}{2}x) - [\cos(\frac{1}{2}x) + i \sin(\frac{1}{2}x)]} = \\ &= \frac{\cos \frac{x}{2} - \cos(n + \frac{1}{2})x - i [\sin \frac{x}{2} + \sin(n + \frac{1}{2})x]}{-2i \sin \frac{x}{2}} = \\ &= \frac{\sin \frac{x}{2} + \sin(n + \frac{1}{2})x + i [\cos \frac{x}{2} - \cos(n + \frac{1}{2})x]}{2 \sin \frac{x}{2}}. \end{aligned}$$

[Az utolsó lépésben i -vel bővítettünk, és felhasználtuk, hogy $i(-i) = -i^2 = -(-1) = 1$]. Összehasonlítva Q két alakját, azt kapjuk, hogy

$$\begin{aligned} 1 + \cos x + \cos 2x + \dots + \cos nx &= \frac{\sin \frac{x}{2} + \sin(n + \frac{1}{2})x}{2 \sin \frac{x}{2}} \\ \sin x + \sin 2x + \dots + \sin nx &= \frac{\cos \frac{x}{2} - \cos(n + \frac{1}{2})x}{2 \sin \frac{x}{2}}. \end{aligned}$$

A kapott összefüggések könnyen igazolhatók komplex számok használata nélkül teljes indukcióval, vagy a bal oldalakat $2 \sin \frac{x}{2}$ -vel szorozva, és a trigonometrikus szorzatokat különbséggé alakítva.

Áttérek Euler néhány számelméleti felfedezésének ismertetésére. *Számelmélet*-nek a matematika azon ágát nevezik, amely elsősorban az egész számok sajátságainak felderítésével foglalkozik. Száz évvel Euler előtt is élt már egy nagy matematikus, a már említett Fermat, aki fontos eredményeket ért el a számelméletben; de Fermat csak tételeit közölte, a módszert, amellyel eredményeihez jutott, elhallgatta. Euler életcéljának tekintette, hogy Fermat bizonyítás nélkül fennmaradt tételeire bizonyítást keressen. Ez a legtöbb esetben sikerült is neki, sőt sokszor lényegesen általánosította Fermat tételeit. Néhány ilyen vizsgálatáról beszámolok.

Ezek között a legnevezetesebb az, melyet ma röviden „Fermat tételé”-nek vagy „Fermat kis tételé”-nek neveznek. („*Kis* tételnek nevezett *nagy* tétel” – mondja szellemesen egy magyar matematikus.)

Először Euler bizonyította be, három bizonyítást adott rá, szépségük és érdekességük miatt mindhármat bemutatom. Maga a tétel így szól:

Legyen p valamely tetszőleges prímszám, és a nem osztható p -vel, akkor

$$a^{p-1} \equiv 1$$

osztható p -vel vagy mai nyelven a kongruencia² jelével

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

²A kongruencia fogalmát és műveleti szabályát ismertettem lapunk idei évfolyamában: K. M. L. XIV, 1957. 34. és 35. o., ismeretüket tehát feltételezem. Lásd még Faragó László: *A számelmélet elemei*, 48–57. o. vagy *Matematikai Versenykérdések* I. rész, 45–47. o.

Az állítás $p = 2$ -re magától értetődő, így a bizonyításban elég páratlan prímszámokra szorítkozni.

Euler első bizonyítása azt adja, hogy $a^p - a$ minden a -ra osztható p -vel. A bizonyítás a binomiális együtthatók egy egyszerű sajátosságát használja fel és teljes indukcióval történik.

Ha $k = 1, 2, \dots, p-1$, akkor a

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!}$$

binomiális együttható (amelyről tudjuk, hogy egész szám) osztható p -vel, mert a számláló osztható vele, viszont a nevező p -nél kisebb számok szorzata, és így nem lehet p -vel osztható, hiszen p törzsszám.

A binomiális tétel értelmében

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \dots + \binom{p}{p-1} + 1,$$

tehát

$$2^p - 2 = \binom{p}{1} + \dots + \binom{p}{p-1} = p \equiv 0 \pmod{p},$$

azaz osztható p -vel. A tétel $a = 2$ -re tehát helyes.

Tegyük most fel, hogy valamilyen $a (\geq 2)$ értékre már tudjuk az állítás helyességét:

$$a^p - a = pA.$$

Ekkor belátjuk, hogy helyes a helyett $(a+1)$ -re is.

$$\begin{aligned} (a+1)^p - (a+1) &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a + \\ &+ 1 - a - 1 = (a^p - a) + \left\{ \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a \right\} = \\ &pA + pB \equiv 0 \pmod{p}. \end{aligned}$$

Az első zárójelben levő kifejezésről az indukciós feltevésből, a másodiktól pedig a binomiális együttható fent belátott tulajdonságából tudjuk, hogy osztható p -vel.

Ezzel igazoltuk a fent kimondott tételt. Ha a osztható p -vel, akkor mind a két tag külön osztható p -vel. Ha a nem osztható p -vel, akkor $-p$ prímszám lévén $-a^p - a = a(a^{p-1} - 1)$ csak úgy lehet p -vel osztható, ha a második tényező osztható vele, vagyis

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

Ezzel igazoltuk az állítást eredeti alakjában is.

Második bizonyításában Euler a tételt általánosítja, mert kimutatja, hogy a tétel úgy fogalmazható, hogy összetett modulusokra is érvényes. A p -nél kisebb, hozzá relatív prímszámok száma $p-1$, amint Euler megmutatta, ez a Fermat-féle kongruenciában a $p-1$ kitevő jelentősége. Ha tehát n egy tetszőleges egész szám (n lehet tehát prímszám és lehet összetett), akkor, ha a nála kisebb és hozzá relatív prím pozitív egész számok számát, amint szokás $\varphi(n)$ -nel jelöljük³, ha a valamely n -hez relatív prímszám, akkor

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

a Fermat-féle kongruencia Euler-féle általánosítása.

Írjunk a rövideg kedvéért $\varphi(n) = m$ -t. Legyenek az n -nél kisebb n -hez relatív prímszámok (valamilyen sorrendben)

$$r_1, r_2, \dots, r_m.$$

Azt állítjuk, hogyha a és n egymáshoz relatív prímek, akkor az

$$ar_1, ar_2, \dots, ar_m.$$

számokat p -vel osztva, azok $r'_1, r'_2, \dots, r'_m$, maradékai újra az $r_1, r_2, \dots, r_m$ számok valamilyen sorrendben.

A maradék jelentése szerint $ar_i - r'_i$ osztható n -nel ($i = 1, 2, \dots, m$). Itt r'_i is relatív prím n -hez, mert különben n és r'_i legnagyobb közös osztója lenne ar_i -nek is, de ez nem lehet, mert a és r_i relatív prím n -hez, és így a szorzatuk is az.

Az $r'_1, r'_2, \dots, r'_m$ számok tehát minden esetre az $r_1, r_2, \dots, r_m$ számok közül kerülnek ki. Mivel mind a két sorozatnak ugyanannyi eleme van, így annak megmutatásához, hogy az előbbiben szerepel az utóbbi minden eleme, elég

³Lásd K. M. L. XIV., 1957. 67. o., vagy Faragó L.: *A számelmélet elemel* 42,-44. o.

megmutatni, hogy az előbbi sorozat különböző indexekhez tartozó elemei nem lehetnek egyenlők. Valóban, ha $r'_i = r'_j$ volna ($i \neq j$), vagyis ar_i és ar_j ugyanazt a maradékot adná n -nel osztva, akkor

$$ar_i - ar_j = a(r_i - r_j)$$

osztható volna n -nel. Mivel a és n relatív prímek, így ez csak úgy lehetne, ha $r_i - r_j$ osztható volna n -nel. Ez azonban lehetetlen, mert r_i és r_j különböző, n -nél kisebb pozitív számok, s így különbségük abszolút értéke n -nél kisebb, és nem 0.

Ezzel igazoltuk a fent kimondott állításunkat. A maradékokra a kongruencia jelét használva, fennáll:

$$\begin{aligned} ar_1 &\equiv r'_1 \pmod{n}, \\ ar_2 &\equiv r'_2 \pmod{n}, \\ &\dots\dots\dots \\ ar_m &\equiv r'_m \pmod{n}. \end{aligned}$$

Szorozzuk össze ezt az m kongruenciát:

$$a^m r_1 r_2 \dots r_m \equiv r'_1 r'_2 \dots r'_m \pmod{n},$$

de az r -ek sorozata azonos (más sorrendben) az r' -k sorozatával, tehát szorzataik azonosak. Az r -ek s az r' -k is egyenként relatív prímek n -hez, tehát szorzatuk is az, ezért ezzel a szorzattal a kongruencia mindkét oldalán egyszerűsíthetünk, s marad

$$a^m \equiv 1 \pmod{n}.$$

vagy m helyébe az értékét beírva

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{q. e. d.}$$

Euler harmadik bizonyítása is közvetlenül ezt az utóbbi kongruenciát bizonyítja, sőt még több derül ki belőle. Azt mutatja meg ugyanis, hogyha δ a legkisebb kitevő, amelyre az

$$a^\delta \equiv 1 \pmod{n}.$$

kongruencia teljesül, akkor δ osztója $\varphi(n)$ -nek.

Tekintsük ugyanis a -nak egymás után következő hatványait:

$$(1) \quad a, a^2, a^3, \dots$$

Ezeknek az n osztóra vett maradékai csak véges sok értéket vehetnek fel (legfeljebb n -et), így elég messze menve a sorozatban található két hatvány a^i és a^j ($i > j$), amely ugyanazt a maradékot adja, vagyis amelyek különbsége osztható n -nel. De a , s így a^j is relatív prím n -hez, $a^i - a^j = a^j(a^{i-j} - 1)$ pedig osztható n -nel, tehát $a^{i-j} - 1$ is osztható n -nel. Van tehát olyan k kitevő (pl. $k = i - j$), amelyre $a^k - 1$ osztható n -nel, vagy a kongruenciák nyelvén

$$a^k \equiv 1 \pmod{n}.$$

Legyen δ a legkisebb kitevő, melyre az

$$a^\delta \equiv 1 \pmod{n}.$$

kongruencia teljesül. Most lehetséges, hogy az (1) sorozat kimeríti az összes a -nál kisebb és a -hoz relatív prím számokat. Ekkor $\delta = \varphi(n)$, és így az állítás bizonyítást nyert. Ha nem, akkor van olyan n -hez relatív prím b szám, amelynek az n osztóra vett maradéka különbözik az

$$(1') \quad a, a^2, \dots, a^\delta$$

sorozat minden elemének maradékától. Szorozzuk meg az (1') sorozat minden tagját b -vel, így kapjuk az

$$(2) \quad ab, a^2b, a^3b, \dots, a^\delta b$$

sorozatot, amelyben nincs két egymással mod n kongruens szám, és amelynek minden tagja különbözik az (1') sorozat minden tagjától. Valóban, ha valamilyen $1 < j < i < \delta$ kitevőkre

$$a^i b \equiv a^j b \pmod{n}$$

lenne, akkor

$$a^{i-j} \equiv 1 \pmod{n}.$$

lenne, és itt $0 < i - j < \delta$, holott δ a legkisebb pozitív kitevő, amelyre a kongruencia teljesül.

Ha pedig

$$a^j b \equiv a^i b \pmod{n}$$

lenne, akkor

$$b \equiv a^{i-j} \pmod{n}.$$

volna, azaz b maradéka előfordulna az (1') sorozat maradékai közt, holott ennek az ellenkezőjét tettük fel.

Ha az (1') és (2) sorozatok együtt sem merítenék ki az n -nél kisebb és hozzá relatív prímszámok sorát, akkor volna oly c szám, mely maradéka egyik sorozat maradékai közt sem foglaltatnék, és ugyanúgy kimutathatnók, hogy az

$$(3) \quad ac, a^2, \dots, a^\delta c$$

sorozat mindenikének maradéka $\pmod{n}$ különböző, és az (1') és (2) sorozat bármely tagjától is különbözik, és így tovább, a különböző maradékok száma mindenesetre, osztható δ -val. Q. e. d.

Ez a bizonyítás – amint SPEISER baseli professzor⁴ matematikai antológiájában mondja, a 18. század egyik alapvető teljesítménye. Vele kezdődik – amint ugyancsak Speiser mondja – a matematikában az elegancia, mert a számolás elkerülésével vezet nagy jelentőségű eredményhez. A bizonyításban a matematika egy fontos új ágának az alap gondolata rejlik, mely a mai matematikában uralkodó. Nem csoda tehát, hogy minden matematikai antológiának nélkülözhetetlen alkatrésze ez a csodálatos bizonyítás.

Euler további számelméleti felfedezéseinek felsorolásában is felhasználom a kongruencia fogalmát, mert így rövidebben mondhatom el őket.

Euler igen sokat foglalkozott a kvadratikussal kongruenciákkal. Ezalatt ezt értjük: Legyen D oly egész szám, mely nem osztható a p törzsszámmal. Akkor az

$$x^2 \equiv D \pmod{p}$$

kongruencia megoldható, ha

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

és megoldhatatlan (azaz nincs oly x szám; melynek négyzetéből D -t kivonva, p -vel osztható számot kapunk), ha

$$D^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Rögtön látni, hogy ebből az „Euler-féle kritériumból” a Fermat-tétel újabb – negyedik – bizonyítása következik, mert négyzetre emelés minden esetben

$$D^{p-1} \equiv 1 \pmod{p}$$

kongruenciát szolgáltatja.

A kvadratikussal kongruenciákkal való állandó foglalkozásának eredményeit összefoglalva élete utolsó évében egy igen nagy jelentőségű tételt talált, az elemi számelmélet egyik legmélyebb tételét. Legyen p és q két prímszám. Ha p és q valamelyike $4k+1$ alakú, akkor az

$$x^2 \equiv p \pmod{q}$$

és

$$x^2 \equiv q \pmod{p}$$

kongruenciáknak vagy mindkettője megoldható vagy egyikük sem; ha pedig p is, q is $4k+3$ alakú, akkor a két kongruencia közül mindig megoldható az egyik, de csak az egyik. A két kongruencia fennállása, ill. lehetetlensége között összefüggést talált, azért a tételt ma *reciprocitási tételnek* nevezik. Tételét Euler nem tudta bebizonyítani, ez csak jóval később a 19 éves GAUSSnak sikerült, aki Eulertól függetlenül szintén felfedezte.⁵

Mondtam már, hogy Euler életproblémájának tekintette Fermat bizonyítás nélkül fennmaradt tételeinek bebizonyítását. Ezek közül néhányat felsorolok.

Minden $4k+1$ alakú prímszám két négyzetszám összege.

Minden természetes egész szám előállítható, mint 4 négyzetszám összege. Ezen tétel bizonyítási kísérletei közben találta a következő csodálatos azonosságot:

$$\begin{aligned} & (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ & (x_1 y_2 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 + (x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3)^2 + \\ & + (x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4)^2 + (x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2)^2 \end{aligned}$$

(bizonyítását az olvasóra bízom), melynek folytán elég a tételt prímszámokra bizonyítani.

⁴ A. SPEISER: Klassische Stücke der Mathematik, Zurich und Leipzig 1925. Orell Fössl
110. o.

⁵ Lásd K. M. L. X. kötet, 1955. ápr. 98. o.

A *diofantoszi egyenletek* elmélete is igen nagy eredményeket köszönhet Euler-nek. Említett algebrai könyvének második része a diofantoszi egyenletekkel foglalkozik. Bebizonyította, hogy az

$$x^2 + 2 = y^3$$

egyenlet egyetlen megoldása $x = 5$, $y = 3$, és az

$$x^2 + 4 = y^3$$

egyenletnek csak két megoldása van $x = 2$, $y = 2$ és $x = 11$, $y = 5$. Fermat ezekre a tételeire igen büszke volt, de csak Euler bizonyítása maradt fenn. Bebizonyította továbbá az ún. Fermat-féle sejtés következő speciális eseteit, hogy az

$$x^3 \pm y^3 = z^3 \quad \text{és az} \quad x^4 \pm y^4 = z^2$$

egyenletek 0-tól különböző egész számokban lehetetlenek. Felemlítem továbbá a következő (Fermat-tól független) eredményét. Az

$$x^3 + 1 = y^2$$

határozatlan egyenlet összes megoldásai $x = -1, 0, 2$; $y = 0, 1, 3$, vagyis két egymásra következő szám közül – a $-1, 0$; $0, 1$; $8, 9$ pároktól eltekintve – nem lehet az egyik köb, a másik négyzet.

Lapunkban egyik régebbi cikkemben⁶ ismertettem a biztosítási matematika elemeit. A biztosítási matematika is Eulertól származik.

Euler fő érdeme a felsőbb matematika részletes kidolgozása, hogy a természet vizsgálatára alkalmas legyen. Minderről a sok bámulatos eredményről nem szólhattam, de egyik könnyen érthető, ámbar igen magas segédeszközöket igénylő problémájáról megemlékezem egy-két szóval. Keresendők azon görbék, amelyek valamely kívánt sajátsággal a legnagyobb vagy a legkisebb mértékben rendelkeznek. Pl. az egyenlő kerületű zárt görbék közül melyeknek a területe a legnagyobb.

Nem hagyom szó nélkül, hogy akadtak matematikusok, akik kifogásolták, hogy Euler a matematika filozófiai alapjait elhanyagolta, és csak a matematikával (és alkalmazásaival) törődött, ebben pedig a legnagyobb mesterek közé tartozik, a logikai alapokkal szemben pedig közömbös. Ezért egy-két eredménye hibás, de egyébként csodálatos matematikai érzéke megóvta azoktól a hibáktól, amelyekre a régi idők nem elég precíz fogalomalkotása több kortársát csábította. A nagy alkotó korszakokban visszaszorul a kritika, amely meddőbb korszakokban virul. Euler pedig a legnagyobb stílusú alkotók közül való. Csak igen kevés alkotását soroltam fel – és mégis micsoda gazdagság!

A matematikának nagyon sok kedvelője van napjainkban, különösen hazánkban. Ezeket fogva tartja a matematika szépségének varázsa. Már pedig Euler levezetései – amint a bemutatott ízelítők is – a bennük rejlő szépség folytán sok-sok nemzedéknek okoztak gyönyörűséget, és a „*mathematica delectans*” nagy művészenek megszerezték sok-sok ezer olvasójának bámulatát és tiszteletét. A magyar ifjúság is örömmel hódol a zseniális matematikus emlékének.

⁶Lásd K. M. L. IX., 1954. nov. 68–70. o.