# SZÁMELMÉLETI PROBLÉMÁK

Kurusa Árpád

Szeged, 1978.nov.o8.

hiba a 12. oldal, újra gépelni!

Ebben az értekezésben először a primekkel, aztán néhány érdekes problémával fogok foglalkozni.

1./ Primszámok és a hozzá kapcsolódó problémák:
-ezután prim= primszám-

Már a görögök ismerték a prim fogalmát, sőt Eratoszthenész bebizonyitotta; végtelen sok prim van.

Tegyük fel ugyanis, hogy véges $\underline{k}$ db. prim van. Ekkor ha $A=p_1 p_2 \dots p_k + 1$ akkor A nem osztható ezekközül a primek közül egyikkel sem /1 a maradék/ ami azt jelenti, hogy A-nak prim osztói különböznek $p_1 \dots p_k$ -tól. Ez ellentmondás, hisz feltettük, hogy $\underline{K}$ db. prim van; tehát a feltevésünk hibás; végtelensok prim van.

Ebből tudjuk, végtelen sok prim van, másrészt minden prim a 2-t kivéve, páratlan; tehát $4k\pm1$ alakú. Bizonyitható, hogy végtelen sok 4k-1 és 4k+1 alakú prim van.

Végtelen sok 4k-1 alakú prim van:
Tegyük fel, hogy véges $\underline{n}$ db. 4k-1 alakú prim van; képezzük a $A=4p_1 \dots p_n-1$ számot; A 4k-1 alakú.
A prim osztói nem lehetnek mind 4k+1 alakúak, mert $(4k+1)(4m+1)= 4(4km+k+m)+1$, azaz ekkor A 4k+1 alakú lenne, ami ellentmondás ; végtelen sok 4k-1 alakú prim van.

Végtelen sok 4k+1 alakú prim van:
Tegyük fel, hogy véges $\underline{n}$ db. 4k+1 alakú prim van; képezzük a $A=(p_1 \dots p_n)^2+1$ számot: A-nak nem osztója $p_1 \dots p_n$ /1 a maradék/; másrészt A 8k+2 alakú, hisz $(4k+1)^2+1=8(k+2k^2)+2$ ezért $A=2(4s+1)$.
Tegyük fel, hogy 2-n kivül A-nak csak 4k-1 alakú prim osztói vannak: $q_1 \dots q_m$

$$A=2q_1^{\alpha_1} \dots q_m^{\alpha_m}$$

Most bebizonyitom, hogy bármely $\alpha_i$ páros.
Legyen $\alpha_i = 2f+1$

$$A=(q_1^{2f+1})z_1=(p_1 \dots p_n)^2+1$$

Legyen $tq_1+r=p_1 \dots p_n \quad r<q_i$. Ekkor:

11111

Ekkor: $q_i z_2=(tq_i+r)^2+1$

$q_i z_2=q_i(t^2q_i+2tr)+r^2+1$

$q_i z_3=r^2+1$

Mivel $z_3<z_2$ ezért bármely egynél nagyobb $z_i$-t csökkenteni tudok, azaz ezzel az eljárással eljutok a következő egyenlőséghez.

$$q_i=z_j^2+1$$

Mivel $q_i=4k+3$, $z_j^2=2(2k+1)$ viszont a $2(2k+1)$ nem lehet négyzetszám, mert benne a 2 páratlan hatványon szerepel.

Ez ellentmondás; tehát bármely $q_i$ páros, akkor viszont $A=2x^2=(pp_1\ldots p_n)^2+1$. Azonban nincs olyan /az 1 kivételével/ négyzetszám, amelynek kétszerese előállna mint egy négyzetszám és 1 összege. Ez ujabb ellentmondás, tehát A-nak kell, hogy legyen $4k+1$ alakú prim osztója, ez azonban nem egyezhet meg $p_1\ldots p_n$-nel.
Ezzel bizonyitottuk állitásunkat.

Ezeknek a tételeknek messzemenő általánositása a Dirichlet tétel:

Ha $\underline{a}$ és $\underline{b}$ egymáshoz relativ primek, akkor az

$$ak+b \quad k=1;2;3;\ldots$$

végtelen számtani sorozatban végtelen sok prim van.

Ezt a tételt nem bizonyitom, mert, bár 1950-ben Selberg dán matematikus elemi úton bizonyitotta, ismert bizonyitásai a felsőbb matematika körébe tartoznak.
Régebben sokan próbálkoztak olyan képletek előállitásával amelyek megadják /sorban/ az összes primszámot.
Később azonban rájöttek, hogy ez /valószinüleg/ lehetetlen és elkezdték vizsgálni a primek eloszlását a számegyenesen.
Mint tudjuk az

$$A=1+\frac{1}{4}+\frac{1}{9}+\ldots+\frac{1}{n^2}$$

konvergens; másfelől Euler bebizonyitotta, hogy az

$$S=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p_k}$$

divergens, azaz minden határon túl nő /$p_i>0$/.

Először belátjuk a következő egyenlőtlenséget:

$$B = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} < \left(1 + \frac{1}{2} + \ldots + \frac{1}{2^k}\right)\left(1 + \frac{1}{3} + \ldots + \frac{1}{3^k}\right)\ldots\left(1 + \frac{1}{p_j} + \ldots + \frac{1}{p_j^k}\right)$$

ha $2^k < n < 2^{k+1}$ és $p_j$ a legnagyobb, $n$-nél kisebb prim.
A jobb oldal beszorzás után a következő tagokat fogja adni:

$$\frac{1}{2^{\alpha_1} \cdot 3^{\alpha_2} \cdot \ldots \cdot p_j^{\alpha_j}}$$

viszont mivel bármely $n$-nél kisebb pozitiv szám előáll $2^{\alpha_1} \cdot 3^{\alpha_2} \cdot \ldots \cdot p_j^{\alpha_j}$ alakban, ezért a jobboldalon szorzás után a B és más tagok /pl. $\frac{1}{p^k \cdot 3^k}$ / is; tehát az egyenlőtlenség valóban fennáll.

Most vegyük ennek az egyenlőtlenségnek a logaritmusát.

Ekkor azt kapjuk, hogy:

/1/ $$\lg B < \lg\left(1 + \frac{1}{2} + \ldots + \frac{1}{2^k}\right) + \lg\left(1 + \frac{1}{3} + \ldots + \frac{1}{3^k}\right) + \ldots + \lg\left(1 + \frac{1}{p_j} + \ldots + \frac{1}{p_j^k}\right)$$

Viszont:

$$1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^k} = \frac{1 - \frac{1}{p^{k+1}}}{1 - \frac{1}{p}} < \frac{1}{1 - \frac{1}{p}} = \frac{p}{p-1} = 1 + p^{\frac{1}{-1}}$$

másrészt

$$\left(1 + \frac{1}{p-1}\right)^{p-1} < 3 \quad ; \quad 1 + \frac{1}{p-1} < \sqrt[p-1]{3}$$

a kettőt összevetve azt kapom, hogy

$$1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^k} < \sqrt[p-1]{3} \underset{2<p}{<} \sqrt[p]{3^2}$$

azaz logaritmusát véve

$$\lg\left(1 + \frac{1}{p} + \ldots + \frac{1}{p^k}\right) < \frac{2 \cdot \lg 3}{p}$$

ezt /1/-be irva kapom, hogy

$$\lg B < 2 \cdot \lg 3 \cdot S \quad 2 \cdot S \cdot \lg 3$$

Mivel $B = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$ minden határon túl nő $\pm \frac{\lg B}{2 \cdot \lg 3}$ is minden határon túl nő, akkor pedig az $S = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p_k}$ is minden határon túl nő.

Ebből azt a következtetést vonhatjuk le, hogy a primek nem ritkulnak olyan nagyon, mint a négyzetszámok, vagyis elég „sürü" vannak a természetes számok közt. Másfelől azonban, ha $\Pi(n)$ jelöli az n-nél kisebb primek számát, akkor $\lim_{n\to\infty} \frac{\Pi(n)}{n} = 0$ tehát a primek a természetes számoknak csupán „0%"-át adják.

Először belátjuk, hogy ha $p_i$ az i-edik primet jelenti, akkor:

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_n}\right)\cdot\ldots = 0$$

Tudjuk, hogy /már beláttuk/

$$\left(1+\frac{1}{p_1}+\ldots+\frac{1}{p_1^n}+\ldots\right)\left(1+\frac{1}{p_2}+\ldots+\frac{1}{p_2^n}+\ldots\right)\cdot\ldots\left(1+\frac{1}{p_k}+\ldots+\frac{1}{p_k^n}+\ldots\right)$$

divergens, tart a $+\infty$ -be; viszont minden szorzó tényező a mértani sor összeg-képlete alapján $\frac{1}{1-\frac{1}{p_i}}$

ezért tudjuk, hogy:

$$\lim_{n\to\infty} \frac{1}{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_n}\right)} = +\infty$$

amiből:

$$\lim_{n\to\infty} \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_n}\right) = 0$$

ez viszont, definició alapján ekvivalens az

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_n}\right)\cdot\ldots = 0$$

egyenlőséggel. Ennek birtokában belátjuk, hogy $\lim_{n\to\infty} \frac{\Pi(n)}{n} = 0$. Legyen $n = m p_1 \ldots p_k$. Ekkor az n-nél $(m>0)$ kisebb hozzá relativ primek száma, +k nyilván nagyobb mint $\Pi(n)$. /~~$p_i$ Lehetnek az i-edik primek/

$$n\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) \geq \Pi(n) - k$$

$$\lim_{n\to\infty} \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) \geq \lim_{n\to\infty}\left(\frac{\Pi(n)}{n} - \frac{k}{n}\right)$$

~~mivel $k \leq \Pi(n)$~~

$$\lim_{n\to\infty} \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) \geq \lim_{n\to\infty} \frac{\Pi(n)}{n} - \lim_{n\to\infty} \frac{k}{2^k}$$

$$0 \geq \lim_{n\to\infty} \frac{\Pi(n)}{n} - 0$$

$\frac{\pi(n)}{n} > 0$ tehát $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$

Harmadfelől azonban két prim közt bármekkora különbség lehet.

Ha $N>2$ $N!$ soha nem prim.

Képezzük a következő számsort:

$N!+2\,;\ N!+3\,;\ N!+4\,;\ \ldots\,;\ N!+N\,;$

Ezek egyike sem lesz prim, mivel rendre oszthatók 2;3;...;N;-nel. Igy sikerült megadnunk N-1 db. egymásmellett lévő összetett számot, ami azt jelenti, hogy a primek közt bármekkora különbség lehet, hisz N bármekkora lehet.

Fölmerül a kérdés; vajon mi $\pi(x)$ nagyságrendje.
Legendre 1797-ben a következő sejtést mondta ki:

$\pi(x) \approx \frac{Ax}{\log x + B}$ $\quad A=1 \quad B \approx -1{,}0836$

C.F. Gauss 1792-93-ban azt találja, hogy

$\pi(x) \approx Li\, x \overset{def.}{=} \sum_{2\le n\le x} \frac{1}{\ln n}$

Észrevehetjük, hogy mindkét sejtésből következik:

$\frac{\pi(x)}{\frac{x}{\ln x}} \to 1$ ha $x \to +\infty$

Ők azonban még nem tudták bizonyitani állitásaikat. 1850-ben Csebisev nagy lépést tett ennek bizonyitása felé. Elemi uton bizonyitotta, hogy ha $\varepsilon > 0{,}08$ akkor ha x elég nagy /ha $x > N_{(\varepsilon)}$ /.

$$(1-\varepsilon)\cdot\frac{x}{\ln x} < \pi(x) < (1+\varepsilon)\frac{x}{\ln x}$$

$$0{,}92129\,\frac{x}{\ln x} < \pi(x) < 1{,}10556\,\frac{x}{\ln x}$$

Bár Csebisev bizonyitása elemi eszközökkel történt, elég bonyolult, igy annál egy gyengébb, de aránylag könyebben igazolható becslést igazolok.

A becslés két oldalból áll:

$$\ln 2 \frac{n}{\ln n} < \pi(x) < \ln 16 \frac{n}{\ln n}$$

Először a jobb aztán a baloldalt fogom igazolni.

/1. $\pi(x) < \ln 16 \frac{n}{\ln n}$

Először belátjuk a $\prod_{p \le n} p < 4^n$ egyenlőtlenséget.

Ez az egyenlőtlenség nyilvén igaz n= 1;2;3;4;5-re.

Most tegyük fel, hogy n=2m+1-re igaz, ekkor n+1=2/m+1/ ami páros szám, tehát nem prim /lévén $m>0$/ amiből következik, hogy:

$$\prod_{p \le n} p = \prod_{p \le n+1} p < 4^n < 4^{n+1}$$

Ha n=2m, akkor elég a $\prod_{m+2 < p \le 2m+1} p < 4^m$ becslést igazolni, hisz a feltevés szerint:

$$\prod_{p \le m+1} p < 4^{m+1}$$

A $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ binomiális együtthatóban fellép az összes m+2-nél nagyobb és 2m+1-nél kisebb prim, hisz a nevezőben, $m!(m+1)!$ -ben ezek a primek nem szerepelnek.

Ebből viszont állithatjuk:

$$\prod_{m+2 \le p \le 2m+1} p \le \frac{1}{2}\left[\binom{2m+1}{m} + \binom{2m+1}{m+1}\right] \le \frac{1}{2}\sum_{i=0}^{2m+1}\binom{2m+1}{i} = \frac{1}{2}\cdot 2^{2m+1} = 4^m$$

Ezzel beláttuk: $\prod_{p \le n} p < 4^n$

Most ez alapján belátjuk /1/.-et

$$4^n > \prod_{p \le n} p = \prod_{p \le \sqrt{n}} p \cdot \prod_{\sqrt{n} < p \le n} p > \prod_{\sqrt{n} < p \le n} p > \prod_{\sqrt{n} < p \le n} \sqrt{n} = \left(\sqrt{n}\right)^{\left(\pi(n) - \pi(\sqrt{n})\right)}$$

vagyis:

$$4^n > \left(\sqrt{n}\right)^{\left(\pi(n) - \pi(\sqrt{n})\right)}$$

Az egyenlőtlenség e alapu logaritmusát véve, majd átrendezve kapjuk:

$$\pi(n) < \frac{n}{\ln n} \ln 16 + \pi(\sqrt{n})$$

Durván becsülve $\pi(\sqrt{n}) < \sqrt{n}$

Ezért:

$$\pi(n) < \frac{n}{\ln n} \ln 16 + \sqrt{n}$$

(#)

Ha n elég nagy $\frac{\sqrt{n}}{\frac{n}{\ln n}} = \frac{\ln n}{\sqrt{n}} < \varepsilon$ ahol $\varepsilon > 0$

Elég nagy n-re $\pi(n) < \ln 16 \frac{n}{\ln n}$

/2/ $\ln 2 \frac{n}{\ln n} < \pi(n)$

Becsüljük először a $\binom{2n}{n}$ binomiális együtthatót.

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = 2^n \cdot \frac{3 \cdot 5 \cdot \ldots \cdot (2n-1)}{n!} > 2^n \frac{2 \cdot 4 \cdot \ldots \cdot (2n-2)}{n!} = \frac{2^{2n}}{2n}$$

Másrtészt mivel:

$$n! = \prod_{p \le n} p^{\alpha_p} \qquad \text{ahol} \qquad \alpha_p = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p \le 2n} p^{\beta_p} \qquad \text{ahol} \qquad \beta_p = \sum_{k=1}^{\infty} \left( \left[\frac{2n}{p^k}\right] - 2 \cdot \left[\frac{n}{p^k}\right] \right)$$

Ez utóbbi összegben nyilvánvalóan csak azok a tagok nem nullák, amelyekre $p^k \le 2n$

Ha a számban jövő tagok számát $m_p$-vel jelölöm akkor:

$$p^{m_p} \le 2n < p^{m_p+1}$$

Az egyes tagok azonban csak nulla vagy az egy értéket vehetik fel, hisz alakjuk $[2b] - 2[b]$

Tudjuk, hogy $x-1 < [x] < x$ , ezért:

$[2b] - 2[b] > 2b - 1 - 2b = -1$ ; $[2b] - 2[b] \ge 0$

$[2b] - 2[b] < 2b - 2(b-1) = 2$ ; $[2b] - 2[b] \le 1$

Márpedig ez azt jelenti, hogy:

$$0 \le \beta_p = \sum_{k=1}^{m} \left( \left[ \frac{2n}{p^k} \right] - 2 \left[ \frac{n}{p^k} \right] \right) \le m$$

Amiből /lévén $p^m \le 2n < p^{m+1}$ /

$$p^{\beta_p} \le p^{m_p} \le 2n$$

Ebből:

$$\frac{2^{2n}}{2n} < \binom{2n}{n} = \prod_{p \le 2n} p^{\beta_p} \le (2n)^{\pi(2n)}$$

$e$ alapu logaritmusát véve és átrendezve, adódik:

$$\pi_{(2n)} > \ln 2 \frac{2n}{\ln(2n)} - 1$$

mivel: $n \ge 2\left[\frac{n}{2}\right]$

$$\pi_{(n)} \ge \pi_{(2\left[\frac{n}{2}\right])} > \ln 2 \frac{2\left[\frac{n}{2}\right]}{\ln\left(2\left[\frac{n}{2}\right]\right)} - 1 > \ln 2 \frac{n}{\ln n} - \frac{2\ln 2}{\ln n} - 1$$

Tt+ a kivonandó korlátos $n \ge 2$ -re, ezért elég-

nagy n-re $\pi_{(n)} > \ln 2 \frac{n}{\ln n}$

Ennek egyenes következménye a Csebisev tétel, vagy másnéven „Bertrand féle posztulátum" amely kimondja:
Egyszám és kétszerese közt mindig van prim.

$$\pi_{(2n)} - \pi_{(n)} > 0{,}92 \cdot \frac{2n}{\ln 2n} - 1{,}11 \frac{n}{\ln n} > 0$$

$$n > e^{\frac{1{,}11 \cdot \ln 2}{0{,}73}}$$

~~Ha~~ $n < N_{(0{,}08)}$-re primszámtábla segitségével lehet ellenőrizni.

Csebisev másik eredménye, hogy: ha $\frac{\pi(x)}{\frac{x}{\ln x}}$ -nek létezik határértéke, akkor az 1.

Ennek bizonyitásához Euler ötletét használta fel, miszerint ha $u > 1$

$$\zeta(u) \overset{def.}{=} \sum_{n=1}^{\infty} \frac{1}{n^u}$$

akkor ennek a konvergens sornak u=1 közelében való viselkedéséből következtetéseket vonhatunk le a primek eloszlására. Ugyanis, a számelmélet alaptétele alapján:

$$\zeta(u) = \sum_{n=1}^{\infty} \frac{1}{n^u} = \prod_p \left(1 + \frac{1}{p^u} + \frac{1}{p^{2u}} + \dots\right)$$

$$\zeta(u) = \sum_{n=1}^{\infty} \frac{1}{n^u} = \prod_p \frac{1}{1 - \frac{1}{p^u}}$$

Mindebben az az érdekes dolog, hogy e szerint a primek eloszlása kapcsolatban van a $\zeta(u)$ folytonos valós függvény bizonyos tulajdonságaival. Megdöbbentő, hogy ennél még tovább menve, megengedve az értelmezési tartományban komplex számokat is, olyan komplex függvényt kapunk aminek tulajdonságaiból következik a primszámtétel:

$$\frac{\pi(x)}{\frac{x}{\ln x}} \to 1 \quad \text{ha} \quad x \to +\infty$$

Ez a kolosszális ötlet Riemanntól származik, aki mindezt 1859-ben az akadémiai székfoglaló előadásában adta közre. Kilenc oldalas értekezése tele van feltevésekkel, addig ismeretlen, nem megalapozott eljárásokkal, és mégis ez a dolgozat a matematika történet talán egyik legjobb dolgozata. Kilencvennyolc évvel Legendre és Gauss sejtése, 37-évvel Riemann értekezése után, 1896-ban J.Hadamard és De la Wallée Poussin egymástól függetlenül, nehéz analitikus problémák megoldása után bebizonyitotta a primszámtételt.

A következő kérdés az, vajon $\pi(x)$ és $\frac{x}{\ln x}$ közt mekkora lehet a különbség. Még Riemann rájött, hogy érdemesebb a Gauss által talált $Li\,x$ függvényt vizsgálni az $\frac{x}{\ln x}$ helyett. Riemann 1859-es székfoglalójában kimondott, egy azóta is „Riemann sejtés" néven emlegetett sejtést, mely szerint $\zeta(u)$ komplex függvény összes gyökének valósrésze 1/2. A sejtés döntő jelentősége, hogy ekvivalens a következő becsléssel:

$$|\pi(x) - Li\,x| < c \cdot \sqrt{x} \cdot \ln x$$

Ez azt jelenti, hogy a $Li\,x$ közelitő formula hibája legfeljebb $\sqrt{x}$ nagyságrendü /eltekintve az $\ln x$ faktortól./ Az eltelt 12o év alatt még nem sikerült a Riemann sejtést bizonyitani, de több részeredmény született:

Erhardt Schmidt bebizonyitotta, hogy a Riemann sejtés a lehető legjobb becslést biztositja, ha igaz. Korobov és Vinográdov 1958-ban bizonyitotta, hogy

$$|\pi(x) - Li\,x| < \frac{x}{e^{(\log x)^{3/5}}}$$

A kérdés a továbbiakban nyitott, egyelőre senki sem tudott ezekre a kérdésekre jobb feleletet adni.
A primekkel kapcsolatban azonban vannak más problémák is. Goldbach 1742-ben Eulernek irt levelében említést tesz egy illetve két sejtésről:

1/ bármely kettőnél nagyobb páros szám előáll mint két prim összege /binér Goldbach sejtés/

2/ bármely ötnél nagyobb páratlan szám előáll mint három prim összege /ternér Goldbach sejtés/

Érdemes megjegyezni, hogy a kettes sejtés az egyes következménye, hisz ha a páratlan számból pl. 3-at levonva, páros számot kapunk és ha ez két prim összege, akkor nyilván igaz a kettes sejtés.
Másik érdekes probléma az iker-primek problémája.
A kérdés az: vajon végtelen sok ikerprim van-e.
/ikerprim: olyan számpár amelyben p és p+2 is prim/

A Goldbach sejtésekkel kapcsolatban az első eredményt G.H.Hardy, Littlewood és Ramanujan érte el. Sikerült levezetniük ternär Goldbach sejtést, de bizonyitásuk renégegeteg függvénytani sejtést tartalmazott. 1930-ban Snyirelmannak elemi módszerekkel sikerült bebizonyitani, hogy bármely elegendően nagy szám előáll, legfeljebb 800000 prim összegeként. Módszerének javitásával Ricci 1936-ban ezt a számot 67-re csökkentette. 1937-ben T.M.Vinogradovnak, az általa bevezetett trigonometrikus összegek elméletével sikerült Hardy Littlewood és Ramanujan bizonyitásából kiküszöbölni a sejtéseket, és ezzel bebizonyitani a ternär Goldbach sejtést elegendően nagy számokra. Bizonyitásában, az volt az érdekes, hogy nem adhatott alsó korlátot.
Ma már sikerült ezt az alsó korlátot megtalálni / $10^{100}$ / de ez még mindig túl nagy ahhoz, hogy az ennél kisebb számokra, akár gépekkel is igazolni lehetne a sejtést.
A bizonyitás másik érdekessége, hogy következik belőle; ha $A(n)$ azon számok száma melyek kisebbek $n$-nél és nem állithatók elő két prim összegeként, akkor:

$$\lim_{n\to\infty} \frac{A(n)}{n} = 0$$

Az ikerprim probléma első eredményét Vigo Brun érte el, bebizonyitván, hogy az ikerprimekből képzett sorozat reciprok összege konvergens, vagyis számuk „elenyésző" a primek közt. A további kutatásokban szinte együtt haladt a Goldbach sejtés az ikerprim problémával, ugyanis 1947-ben Rényi Alfréd igazolta, hogy minden elegendően nagy páros szám előáll $P_1+P_k$ alakban, ahol $P_i$ olyan szám aminek $i$ 1-nél nagyobb prim osztója van.
Módszere az ikerprim problémára is hasonló eredményt szolgáltatott. 1950-ben Selberg kimutatta: Ha $m$ elég nagy $2m=P_2+P_3$ és, hogy végtelen sok olyan $p$ prim van, melyre $p+2$-nek legfeljebb 3 prim osztója van. Végül

1966-ban J.Chon bebizonyitta, ha m elég nagy $2m=P_1+P_2$ ehhez hasonló ereményt kapott az ikerprim problémára is.
Érdekes, hogy a Goldbach sejtés és az ikerprim probléma azon ritka problémákközé tartozik a számelméletben, melyek nem következnek a Riemann hipotézisből.

Természetesen a primek körül még rengeteg probléma van és valószinüleg lesz is. Csak példa képpen, érdekes sejtés a következő kettő:

1/ A

$3;\ 2^3-1=7;\ 2^{2^3-1}-1=127;\ 2^{2^{2^3-1}}-1=2^{127}-1;\ \ldots$

sorozatban csak primek fordulnak elő. Az eddig kiszámolt értékek mind ezt támasztják alá, de eddig még nem sikerült bizonyitani.

2/ Ezt a problémát én találtam, de eddig bizonyitanom nem sikerült:
Irjuk fel a természetes számok sorozatát, aztán alá a primek sorozatát és vonjuk ki a primekből a felettük levő számot /tulajdonképpen képezzük a $p_n$-n különbségek sorozatát/. Ezután képezzük az igy kapott sorozat elemei közti különbség abszolut értékét, majd az igy kapott sorozattal tegyük ugyanezt. Igy kapunk egy táblázatot:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
| 1 | 0 | 0 | 1 | 2 | 4 | 6 | 8 | 10 | 14 | 18 | 20 |
| 1 | 0 | 1 | 1 | 2 | 2 | 2 | 2 | 4 | 4 | 2 | |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 2 | 0 | 0 | | |
| 0 | 1 | 1 | 1 | 0 | 0 | 2 | 2 | 0 | | | |
| 1 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | | | | |
| 1 | 0 | 1 | 1 | 2 | 2 | 0 | | | | | |
| 1 | 1 | 0 | 1 | 0 | 2 | | | | | | |
| 0 | 1 | 1 | 1 | 2 | | | | | | | |
| 1 | 0 | 0 | 1 | | | | | | | | |
| 1 | 0 | 1 | | | | | | | | | |
| 1 | 1 | | | | | | | | | | |
| 0 | 1 | | | | | | | | | | |
| 1 | | | | | | | | | | | |

A

Nézzük meg a A-val jelölt „átlót". Állitásaim:

1/ a A átló minden eleme az első kettőt kivéve, egyes

2/ ha $a_n$ sorozat ugyan-ilyen táblázatának A átlójára fennáll /1/, akkor ha $p_n$ jelöli az n-edik primet $p_n \leq a_n$

Ezzel elérkeztünk a primszámok eddigi történetének végére.

2./ Érdekes problémák.

1. Wilson tétele: /p-1/!+1 akkor és csak akkor osztható p-vel, ha p prim.

Legyen a 2;3;...;p-2; számok valamelyike.

Nézzük az a;2a;3a;...;/p-2/a; számokat.

Bármely kettő p-vel való osztási maradéka különböző, ezért p-vel való osztásukkor maradékul az 1;2;...;p-1 számokat pontosan egyszer adják. Az 1;2;...;p-1; számok közt található b melyre ba maradéka p-re 1. Ekkor nyilván $b \neq 1$ $b \neq p-1$, hisz $2 \leq a \leq p-2$ , másrészt $b \neq a$, mert ha b=a és ba maradéka p-re 1, akkor $a^2-1=/a-1//a+1/$ osztható lenne p-vel ami csak akkor volna lehetséges, ha a=1 vagy a=p-1. Ezért $2 \leq b \leq p-2$ és $b \neq a$ ;tehát a 2;3;...;p-2;számok olyan számpárokra osztható, melyek szorzatának maradéka p-re 1. Következésképpen a $2 \cdot 3 \cdot \ldots \cdot (p-2)$ szorzat, amely p-3/2 ilyen számpárt tartalmaz, p-vel osztva 1-et ad maradékul, vagyis a

$$(p-1)! = [1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2)] \cdot (p-1) \qquad \text{maradéka } p-1$$

azaz/p-1/!+1 osztható p-vel, ha p-nek csak az egy és önmaga osztója.

Ha p nem prim, akkor van $q < p-1$ osztója, viszont ekkor $q \mid (p-1)!$ amiből $q \nmid (p-1)!+1$, vagyis

$$p \nmid (p-1)! + 1$$

2. Bármely $n \geq 7$ természetes szám felirható legfeljebb n/3 db. különböző primszám összegeként.

Az állitás nyilván igaz n=8;9 esetben. Tegyük fel, hogy az állitás n=8;9;...;k;-ra igaz. Tekintsük a $n+1-p_{\pi(n+1)}$ számot. Ez nyilván előáll /indukciós feltevés/ $\frac{n+1-p_{\pi(n+1)}}{3}$ db. különböző prim összegeként.

Állitásunk igaz, ha:

$$1+\frac{n+1-p_{\pi(n+1)}}{3} < \frac{\frac{n}{2}+1}{3}+1 < \frac{n+1}{3} \quad \text{és} \quad 2p_{\pi(n+1)} > n+1$$

Mint látjuk ez igaz, tehát bármely $n \geq 7$ szám felirható legfeljebb n/3 db. különböző prim összegeként.

3. A görögök a számok osztóit, annak részeinek tekintették igy érthetően különös érdekességet tulajdonitottak azoknak a számoknak, amelyeknek a számnál kisebb osztóinak, részeinek összege éppen magát a számot adták. Ezeket a számokat tökéletes számoknak nevezték.
Ilyen pl. 1+2+3=6; 1+2+4+7+14=28

Már Eukliédesz észrevette, hogy a $2^{p-1}\cdot(2^p-1)$ számok, ahol $2^p-1$ primszám, tökéletes szám. Euler azonban azt is bebizonyitotta, hogy a páros számok közül csakis ezek lehetnek tökéletes számok.

Legyen $S(n)$ az $n$ osztóinak összege.

Tudjuk, hogy $S(n)$ multiplikativ, azaz ha $/n;m/=1$ akkor $S(n\cdot m) = S(n)\cdot S(m)$

Ekkor állitásunk a következőt jelenti;: $S(n) = 2n$

Legyen $n = 2^t\cdot m$ ahol m páratlan; ekkor $(2^t; m) = 1$

ezért $S(n) = S(2^t)\cdot S(m) = (2^{t+1}-1)\cdot S(m)$

másrészt $S(n) = 2n = 2^{t+1}\cdot m = (2^{t+1}-1)\cdot m + m$

Ebből következik, hogy: $(2^{t+1}-1)(S(m)-m) = m$

Ha $S(m)-m = d^{**}$ $d/m$ ~~másrészt~~ $S_m = m + d^{**}$

Ez azt jelenti, hogy m-nek csak m és d az osztója, mert ha lenne még osztója, azt hozzáadva m+d-hez, nagyobb lenne $S(m)$-nél; ebből azonban d=1, azaz m primszám és $2^{t+1}-1$ -gyel egyenlő.

Ezzel beláttuk Euler állitását.

Ha $n = 2^{p-1}\cdot(2^p-1)$ akkor;

$S(n) = S_{(2^{p-1})}\cdot S_{(2^p-1)} = (2^p-1)\cdot\left((2^p-1)+1\right) = 2\cdot 2^{p-1}\cdot(2^p-1)$

Ezzel beláttuk Eukliedész állitását. Ezek tehát páros tökéletes számok voltak. A páratlan tökéletes számokról ~~ezt~~ máig sem tudunk semmit, még azt sem, hogy egyáltalán létezik e.

3. Meg kell emliteni az ugy-nevezett diofantoszi egyenleteket. Nevüket onnan kapták, hogy i.e.3.sz.-ban egy Diophantos nevü görög foglalkozott a következő egyenlet megoldhatóságával az egész számok körében.

$$ax+by=c$$

Mint tudjuk, ennek az egyenletnek akkor és csak akkor van megoldása, ha $(a;b)\nmid c$. Adiofantoszi egyenletek azonban nem csak elsőfokuak és nem csak két ismeretlenesek lehetnek. Mig az előbb emlitett problémát lezártnak tekinthetjük, addig a másodfoku diofantoszi egyenleteket korántsem. Vannak ugyan megoldott részek, de nem mind. Igy pl. megoldottnak tekinthető a Phitagórászi számhármasok problémája, a Pell féle egyenletek / $x^2-dy^2=1$ $d>1$ $d\neq a^2$ /. Megoldottnak tekinthető az

$$x^2+y^2=u$$

egyenlet is, mióta Euler bebizonyitotta; pontosan azok a számok bonthatók fel két négyzetszám összegére, amelyek, primfelbontásában a 4k-1 alaku prim nem fordul elő páratlan hatványon. Lagrange bizonyitotta, hogy az

$$x^2+y^2+z^2+t^2=u$$

diofantoszi egyenlet mindig megoldható. Bebizonyitható az is, hogy minden n természetes szám felosztható 9 köbszám, 21 negyedik hatvány összegére. Ezek általánositása a Waring tétel: Minden természetesszám felirható, legfeljebb $M(k)$/k-tól függő mennyiség/ db. k hatvány összegeként. A legutóbbi időkig csak olyan bizonyitásait ismerte a világ, melyek a felsőbb matematika eszközeit használták. Ma már ismert J.V.Linnyik elemi bizonyitása, de az még mindig bonyolult.

Másik érdekes diofantoszi probléma, a Fermat-féle sejtés. Fermat azt sejtette, hogy az

$$x^n+y^n=z^n$$

egyenletnek, a triviális megoldásoktól eltekintve, nincs megoldása, ha $n>2$. Egy könyve szélére a következőket irta:

„Az $n>2$ esetben nincsenek olyan zérustól különböző számok, amelyek azt az egyenletet kielégitenék. Ennek egy csodálatosan szép bizonyitását találtam, azonban a lap széle kevésnek bizonyul, hogy azt befogadja." Sajnos bizonyitása nem maradt fenn és igy azóta is igen sokan dolgoznak azon, hogy bebizonyitsák sejtését.

A számelméletben persze még sok probléma van, és még több lesz - szinte kimerithetetlen tára a problémáknak. Remélem sikerült közelebb hoznom az olvasóhoz a számelmélet nagy problémáit, vagy hajdanában nagy problémáit, sikerült egy kis bepillantást adnom abba is, hogyan fejlődik a matematika e régi, de még mindig sok ujat rejtegető fejezete.

Irodalom jegyzék:

1/ Dr.Szendrei János:
Algebra és számelmélet. Tankönyvkiadó 1978.

2/ D.O.Skljarszkij-N.N.Csencov-I.M.Jaglom:
Válogatott feladatok és tételek az elemi matematika köréből 1. Aritmetika és algebra. Tankönyvkiadó 1976.

3/ Erdős Pál - Surányi János:
Válogatott fejezetek a számelméletből. Tankönyvkiadó 196o.

4/ Középiskolai Matematikai Lapok 1977.1o.szám.