

6. AZ ANALITIKUS SZÁMELMÉLET NÉHÁNY KÉRDÉSE.

6.1. Az e transzcendens szám.

Analízisbeli segédeszközök.

6.1.A Tétel. Legyenek $h_1, h_2, \dots, h_n$ az $[a, b]$ intervallumon integrálható függvények, továbbá $d_1, d_2, \dots, d_n \in \mathbb{R}$. Ekkor

$$\int_a^b \left(\sum_{i=1}^n d_i h_i(x) \right) dx = \sum_{i=1}^n d_i \int_a^b h_i(x) dx.$$

6.1.B Tétel. Ha az f, g függvények differenciálhatók az $[a, b]$ intervallumon, akkor

$$\int_a^b f(x)g'(x)dx = f(b)g(b) - f(a)g(a) - \int_a^b f'(x)g(x)dx.$$

6.1.C Lemma. Legyen $g, h \in \mathbb{R}[x]$. Ha $g(x) = h(x)e^{-x}$ minden $x \in \mathbb{R}$ -re, akkor g, h a zéró polinom.

6.1.D Lemma. Tetszőleges $c \geq 0$ valós számra $\lim_{n \rightarrow \infty} \frac{c^n}{n!} = 0$.

Bizonyítás. Legyen $m > 1$, $m > 2c$. Ekkor

$$\begin{aligned} \frac{c^n}{n!} &= \frac{c}{1} \cdot \frac{c}{2} \cdots \frac{c}{m-1} \cdot \frac{c}{m} \cdot \frac{c}{m+1} \cdots \frac{c}{n} \\ &\leq \underbrace{\frac{c}{1} \cdot \frac{c}{2} \cdots \frac{c}{m-1}}_d \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} = \frac{d}{2^{n-m+1}} \end{aligned}$$

Az állítás ezek után nyilvánvaló.

A valós számok egy speciális közelítése racionális számokkal

Fölhasználjuk, hogy a racionális számok halmaza a valós számok halmazának egy sűrű részhalmaza, azaz, ha $\alpha \in \mathbb{R}$, akkor bármely α -t tartalmazó intervallumban van racionális szám. Formálisan ez azt jelenti, hogy

bármely $\alpha \in \mathbb{R}$ és $\varepsilon > 0$ -hoz van olyan $m, m_1 \in \mathbb{Z}$ és $\varepsilon_1 \in \mathbb{R}$ úgy, hogy $|\varepsilon_1| < \varepsilon$ és

$$\alpha = \frac{m_1}{m} + \varepsilon_1.$$

Számunkra egy ennél jobb, élesebb approximáció lesz szükséges. Általában egy közelítésnél az eltérés abszolút értékét kell csökkenteni, ill. kicsinek választani. Ilyen az előbbi közelítés is. Ennél jobbnak tekinthetők bizonyos esetekben azok a racionális approximációk, amelyeknél nemcsak az eltérés, hanem annak egy számszorosa (s gyakran ez a szám nagy) is kicsi. Pontosabban fogalmazva egy ilyen közelítés a következő.

Definíció. Legyen $a \in \mathbb{R}$ és $\varepsilon > 0$. Ha van olyan $|\varepsilon_1| < \varepsilon$ valós szám és m, m_1 egészek, hogy

$$a = \frac{m_1 + \varepsilon_1}{m},$$

akkor azt mondjuk, hogy a *erősen approximálható* racionális számokkal.

E fogalom lényegében Liouville-től ered. Ő vette észre először (1844-ben), hogy az algebrai számok a „rosszak”, míg a transzcendensek a „jók” a racionális számokkal való approximációkor. Erre utalt a korábbi 4.5.2. Következmény is. Meg fogjuk mutatni, hogy nem minden valós szám közelíthető meg ily módon racionális számokkal, nevezetesen, az erősen is approximálható valós számok irracionálisok, sőt az e és a π ilyenén tulajdonsága döntő fontosságú lesz a későbbiekben.

Példa. Megmutatjuk, hogy az e szám közelíthető ily módon is racionális számokkal. Ismeretes, hogy $e = \sum_{k=0}^{\infty} \frac{1}{k!}$, s legyen valamely $n \geq 1$ -

re $A_n = \sum_{k=0}^n \frac{1}{k!}$. Ekkor

$$\begin{aligned} e &= A_n + \frac{1}{(n+1)!} \left(1 + \frac{1}{(n+2)} + \frac{1}{(n+2)(n+3)} + \dots \right) \\ &\leq A_n + \frac{1}{(n+1)!} \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \dots \right) \\ &= A_n + \frac{2}{(n+1)!}. \end{aligned}$$

Legyen $\varepsilon > 0$ tetszőleges, s $n > \frac{2}{\varepsilon}$, azaz $\frac{2}{n} < \varepsilon$. Ha $m = n!$, $m_1 = n!A_n$ (ez egész!), akkor ε_1 választható a kívánalmaknak megfelelően.

6.1.1. Állítás. Legyen $\alpha \in \mathbb{R}$ olyan, hogy minden valós $\varepsilon > 0$ -hoz van olyan $m, m_1 \in \mathbb{Z}$, s $\varepsilon_1 \in \mathbb{R}$ úgy, hogy $0 < |\varepsilon_1| < \varepsilon$ és

$$\alpha = \frac{m_1 + \varepsilon_1}{m}.$$

Ekkor α irracionális.

Bizonyítás. Tegyük föl, hogy $\alpha = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q > 0$, s legyen $\varepsilon = \frac{1}{2q}$. A föltétel szerint ezen ε -hoz is létezik olyan m, m_1, ε_1 , hogy

$$\alpha = \frac{p}{q} = \frac{m_1 + \varepsilon_1}{m}.$$

Ebből $pm - qm_1 = q\varepsilon_1$ adódik. A bal oldal egész, míg a jobb oldalon

$$0 < |q\varepsilon_1| = q|\varepsilon_1| < q\frac{1}{2q} = \frac{1}{2},$$

ami ellentmondás.

A példából és a fönti állításból azonnal adódik a

6.1.2. Következmény. Az e irracionális szám.

Ezek után már hozzáfoghatunk az e transzcendens voltának igazolásához. Mivel a bizonyítás meglehetősen hosszú — összevetve az eddig látott bizonyításokkal — előbb megfogalmazzuk a bizonyítás egy rövid vázlatát.

A bizonyítás vázlata.

Tegyük föl, hogy e algebrai szám, legyen t az e $\mathbb{Q}$ -fölötti minimálpolinomja. Ekkor

$$0 = t(e) = a_0 + a_1e + a_2e^2 + \dots + a_{n-1}e^{n-1} + e^n.$$

Nyilván $a_0 \neq 0$. Az együtthatók nevezőivel szorozva

$$c_0 + c_1e + c_2e^2 + \dots + c_ne^n \quad (1)$$

ahol $c_0, c_1, \dots, c_n \in \mathbb{Z}$, és $c_0 \neq 0$, $c_n \neq 0$.

Láttuk, hogy e erősen approximálható racionális számokkal. Megmutatjuk, hogy ugyanez teljesül az e hatványaira is, azaz bármely $\varepsilon > 0$ -hoz léteznek olyan $\varepsilon_1, \dots, \varepsilon_n$ nemzéró valós számok, hogy $|\varepsilon_i| < \varepsilon$ $i = 1, 2, \dots, n$, s olyan $m, m_1, \dots, m_n$ egészek, hogy

$$e^k = \frac{m_k + \varepsilon_k}{m}, \quad \text{ha } k = 1, 2, \dots, n.$$

Ezeket (1)-be helyettesítve kapjuk, hogy

$$(c_0m + c_1m_1 + \dots + c_nm_n) + (c_1\varepsilon_1 + c_2\varepsilon_2 + \dots + c_n\varepsilon_n) = 0.$$

Ha az összeg első tagjáról ki tudjuk mutatni, hogy egy nemzéró egész, s a másodikról pedig azt, hogy abszolút értéke kisebb $\frac{1}{2}$ -nél akkor nyilván ellentmondásra jutunk, s így e nem lehet algebrai szám.

Az ε -ok és az m -ek előállítás

Az elkövetkezőkben elemi analízisbeli eredményeket használunk föl, s állításaink egy része is ilyen jellegű. Ezek bizonyítását általában nem részletezzük.

6.1.3. Lemma. *Tetszőleges $k \geq 0$ egészhez vannak olyan $g_k, h_k \in \mathbb{R}$ fölötti polinom, hogy minden $r \in \mathbb{R}$ -re*

$$\int_0^r x^k e^{-x} dx = k! - e^{-r} g_k(r) \quad (a)$$

és

$$\int_0^r (x-r)^k e^{-x} dx = h_k(r) - e^{-r} k!. \quad (b)$$

Bizonyítás. k -szerinti teljes indukciót alkalmazva az 6.1.B Tétel segítségével azonnal adódnak az állítások.

E lemma segítségével az $m, m_1, m_2, \dots, m_n$ egészeket $\int_0^r f(x) e^{-x} dx$ alakú integrálokkal fogjuk kiszámítani.

6.1.4. Példa Legyen $f(x) = 3 + 4x - 10x^3$. Ekkor

$$\begin{aligned} \int_0^r f(x)e^{-x}dx &= \int_0^r (3 + 4x - 10x^3)e^{-x}dx \\ &= 3 \int_0^r e^{-x}dx + 4 \int_0^r xe^{-x}dx - 10 \int_0^r x^3e^{-x}dx. \end{aligned}$$

Az előző lemma alapján

$$\begin{aligned} \int_0^r f(x)e^{-x}dx &= 3(0! - e^{-r}g_0(r)) + 4(1! - e^{-r}g_1(r)) - 10(3! - e^{-r}g_3(r)) \\ &= (3 \cdot 0! + 4 \cdot 1! - 10 \cdot 3!) - e^{-r}(3g_0(r) + 4g_1(r) - 10g_3(r)). \end{aligned}$$

Nyilván $g_0, g_1, g_3 \in \mathbb{R}[x]$, így kaptuk hogy

$$\int_0^r f(x)e^{-x}dx = m - e^{-r}G(r),$$

ahol $m = 3 \cdot 0! + 4 \cdot 1! - 10 \cdot 3! \in \mathbb{Z}$, míg $G(x) = 3g_0(x) + 4g_1(x) - 10g_3(x) \in \mathbb{R}[x]$.

E példa általánosítása a következő lemma, amely az előző példabeli konstrukció és az 6.1.C Lemma alapján egyszerűen igazolható.

6.1.5. Lemma. Legyen $f \in \mathbb{R}[x]$. Pontosan egy olyan m valós szám és $G \in \mathbb{R}[x]$ polinom van, hogy minden $r \in \mathbb{R}$ -re

$$\int_0^r f(x)e^{-x}dx = m - e^{-r}G(r),$$

Definíció. Legyen az előző lemmabeli f polinom a következő:

$$f(x) = \frac{x^{p-1}}{(p-1)!}(x-1)^p(x-2)^p \dots (x-n)^p,$$

ahol p egy (nagy) prímszám, n pedig e minimálpolinomjának fokszáma. Legyen továbbá

(i) $m, G(x)$ az 6.1.5. Lemma alapján ezen f polinomhoz tartozó valós szám és polinom.

(ii) $m_r = G(r)$, ha $r \in \{1, 2, \dots, n\}$.

(iii) $\varepsilon_r = e^r \int_0^r f(x)e^{-x}dx$, $r \in \{1, 2, \dots, n\}$.

Nyilván $\deg(f) = np + p - 1$.

Írjuk föl az előbbi f polinomot $(x - r)$ hatványai szerint rendezve:

$$f(x) = \frac{1}{(p-1)!} (d_0(r) + d_1(r)(x-r) + \dots + d_n(r)(x-r)^n) \quad (*)$$

6.1.7. Lemma. Ha $r \in \{1, 2, \dots, n\}$, akkor a $(*)$ -beli jelölésekkel

$$d_0(r) = d_1(r) = \dots = d_{p-1}(r) = 0.$$

Bizonyítás. Legyen $r \in \{1, 2, \dots, n\}$ rögzített. Mivel $(x-r)^p | f(x)$,

$$f(x) = \frac{1}{(p-1)!} (x-r)^p g(x)$$

valamilyen $g \in \mathbb{Z}[x]$ -re. Ha most g -t $(x-r)$ hatványai szerint írjuk föl, s azt beszorozzuk $(x-r)^p$ -nel azt kapjuk, hogy

$$f(x) = \frac{1}{(p-1)!} (b_p(x-r)^p + b_{p+1}(x-r)^{p+1} + \dots + b_n(x-r)^n)$$

ahol $b_p, \dots, b_n \in \mathbb{R}$, amiből az állítás már nyilvánvaló.

Az $m, m_1, \dots, m_n$ és az $\varepsilon_1, \dots, \varepsilon_n$ -ek tulajdonságai.

6.1.8. Lemma.

(a) m egész, és bármely $p > n$ prímre $p \nmid m$.

(b) Van olyan $G_1 \in \mathbb{Z}[x]$, $\deg(G_1) \leq n$, hogy $G(r) = pG_1(r)$ minden $r \in \{1, 2, \dots, n\}$ -re. Speciálisan, $m_1, \dots, m_n$ p -vel osztható egészek.

Bizonyítás.

(a) f -et rendezzük x hatványai szerint:

$$f(x) = \frac{1}{(p-1)!} (a_{p-1}x^{p-1} + a_px^p + \dots + a_nx^n),$$

ahol $a_{p-1}, \dots, a_n \in \mathbb{Z}$ és $a_{p-1} = \pm(n!)^p \neq 0$. Az integrál linearitása (3.1.A Tétel) miatt

$$\begin{aligned} \int_0^r f(x)e^{-x}dx &= \int_0^r \frac{1}{(p-1)!} (a_{p-1}x^{p-1} + \dots + a_nx^n) e^{-x}dx \\ &= \frac{1}{(p-1)!} \left(a_{p-1} \int_0^r x^{p-1}e^{-x}dx + \dots + a_n \int_0^r x^ne^{-x}dx \right). \end{aligned}$$

Az 6.1.3. Lemma (a) része alapján minden egyes integrál egy kéttagú különbség, amelynek második tagjában szerepel e^{-r} . Így az 6.1.4. Példában látott módszer segítségével $\int_0^r f(x)e^{-x}dx$ két összeg különbsége, amelynek első tagja

$$\frac{1}{(p-1)!} (a_{p-1}(p-1)! + \dots + a_nn!),$$

míg a második $e^{-r} \times x$ egy polinomja. Az f polinom definíciója (i) pontja, valamint az 6.1.5. Lemma alapján (az egyértelműséget használva) az első tag éppen m , azaz

$$m = a_{p-1} + a_p p + \dots + a_n n(n-1) \dots (p+1)p.$$

Mivel az $a_{p-1}, a_p, \dots, a_n$ együtthatók egészek, m is egész, s a p prím, ha $p > n$ neki nem osztója ($a_{p-1} = \pm(n!)^p$ lévén).

(b) Rendezzük át most $f(x)$ -et $(x-r)$ hatványai szerint:

$$\begin{aligned} \int_0^r f(x)e^{-x}dx &= \frac{1}{(p-1)!} \left(d_0(r) \int_0^r e^{-x}dx + d_1(r) \int_0^r (x-r)e^{-x}dx \right. \\ &\quad \left. + \dots + d_n(r) \int_0^r (x-r)^n e^{-x}dx \right). \end{aligned}$$

Ismét az 6.1.3. Lemma alapján (most a (b) pontot használjuk) mind-egyik integrál két tag különbsége, s a másodikban szerepel e^{-r} . Így $\int_0^r f(x)e^{-x}dx$ két összeg különbségeként írható, ahol a második

$$\frac{e^{-r}}{(p-1)!} (d_0(r) + d_1(r)1! + \dots + d_n(r)n!),$$

míg az első r egy $\mathbb{R}$ fölötti polinomja. Az 6.1.5. Lemma alapján (egyértelműség) $G(r)$ egyenlő az előbbi kifejezés polinom részével:

$$G(r) = \frac{1}{(p-1)!} (d_0(r) + d_1(r)1! + \dots + d_n(r)n!).$$

Abban a speciális esetben, amikor $r \in \{1, 2, \dots, n\}$ tudjuk, hogy

$$G(r) = \frac{1}{(p-1)!} (d_p(r)p! + \dots + d_n(r)n!).$$

Ezt $(p-1)!$ -sal beosztva kapjuk, hogy

$$G(r) = p(d_p(r) + d_{p+1}(r)(p+1) + \dots + d_n(r)n(n-1) \dots (p+1)).$$

Ha $G_1(x) = d_p(x) + \dots + d_n(x)n(n-1) \dots (p+1)$, akkor az előbbi

$$G(r) = pG_1(r)$$

alakban írható.

Vegyük észre, hogy $G_1 \in \mathbb{Z}[x]$ és $\deg(G_1) \leq n$. Az f definíciója (ii) pontja alapján $m_r = pG_1(r)$, ami egész és osztható p -vel.

A következő lemma az ε -ok elegendően kicsinek választását biztosítja.

6.1.9. Lemma. Ha $f(x)$ a definícióban adott polinom, $r \in \{1, 2, \dots, n\}$, akkor

$$\lim_{p \rightarrow \infty} \int_0^r f(x) e^{-x} dx = 0.$$

Bizonyítás. Legyen $r \in \{1, 2, \dots, n\}$, $x \in [0, r]$. Ekkor egy rutin becslést alkalmazva

$$\begin{aligned} |f(x)e^{-x}| &\leq |f(x)| \\ &= \frac{x^{p-1}}{(p-1)!} |(x-1)^p \dots (x-n)^p| \\ &\leq \frac{x^{p-1}}{(p-1)!} (x+1)^p \dots (x+n)^p \\ &\leq \frac{r^{p-1}}{(p-1)!} (r+1)^p \dots (r+n)^p \\ &= \frac{1}{r} \frac{c^p}{(p-1)!} \end{aligned}$$

ahol $c = r(r+1) \dots (r+n)$, ami független p -től. Így

$$\left| \int_0^r f(x) e^{-x} dx \right| \leq r \cdot \frac{1}{r} \cdot \frac{c^p}{(p-1)!} = \frac{c^p}{(p-1)!},$$

ami az 6.1.D Lemma alapján 0-hoz tart, ha $p \rightarrow \infty$.

A főtétel bizonyítása.

6.1.10. Tétel. Az e transzcendens szám.

Bizonyítás. Tegyük föl, hogy e algebrai szám, s legyen $h \in \mathbb{Z}[x]$ a minimálpolinomból a nevezőkkkel való beszorzás útján kapott egész együtthatós polinom. Ekkor

$$h(e) = c_0 + c_1 e + c_2 e^2 + \dots + c_n e^n. \quad (*)$$

Legyenek m, m_r, ε_r $r \in \{1, 2, \dots, n\}$ az f definícióban adott számok. Ekkor

$$\begin{aligned} e^{-r} \varepsilon_r &= \int_0^r f(x) e^{-x} dx = m - e^{-r} G(r) \\ &= m - e^{-r} m_r, \end{aligned}$$

s ebből

$$e^r = \frac{m_r + \varepsilon_r}{m}.$$

Ezeket (*)-ba helyettesítve

$$(c_0m + c_1m_1 + \dots + c_nm_n) + (c_1\varepsilon_1 + \dots + c_n\varepsilon_n) = 0. \quad (**)$$

Ha a p prímet elegendően nagynak választjuk (ha $p > m$), akkor az 6.1.8. Lemma alapján m egész és $p \nmid m$. Ha $p > |c_0|$ is teljesül, akkor $p \nmid c_0m$. Mivel $m_1, m_2, \dots, m_n$ mind oszthatók p -vel,

$$p \nmid c_0m + c_1m_1 + \dots + c_nm_n.$$

Így a $c_0m + c_1m_1 + \dots + c_nm_n$ egész különbözik 0-tól.

Másrészt, ha p elég nagy, akkor az f definíciója (iii) pontja és az 6.1.9. Lemma alapján nyilvánvaló, hogy

$$|c_1\varepsilon_1 + \dots + c_n\varepsilon_n| < \frac{1}{2}.$$

Ezzel ellentmondásra jutottunk (**)-gal, s ezért az e nem lehet algebrai szám.

6.1.11. Megjegyzés. Az f polinom megválasztását a következők indokolják:

- (1) a nevezőben azért szerepel $(p-1)!$, hogy ε_r elegendően kicsi lehessen nagy p -re;
- (2) x^{p-1} azért szerepel, hogy m egész legyen a nevezőbeli $(p-1)!$ ellenére is;
- (3) az $(x-1)^p, \dots, (x-n)^p$ biztosítja, hogy a nevezőbeli $(p-1)!$ ellenére $m_1, \dots, m_n$ egész szám legyen;
- (4) az előbbiek együttesen biztosítják, hogy megkapjuk a kívánt közelítéseket $e, e^2, \dots, e^n$ -re.

6.2. A Riemann-féle ζ függvény.

Történeti háttér.

Az egyik legismertebb végtelen sor az ún. harmónikus sor:

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$$

Mivel e sorban egészek szerepelnek, fölkelte a számelmélszkek érdeklődését is. Sajnos a sor divergens, de a divergencia relatíve lassú, az első n tag összege közelítőleg $\log n$. Konvergencia tehető azonban a sor, ha az általános tagot $\frac{1}{n}$ -ről $\frac{1}{n^s}$ -re változtatjuk, ahol $s > 1$. Ez tette lehetővé a következő — ma *Riemann-féle ζ függvénynek* nevezett —

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots \quad (1)$$

függvény bevezetését.

Megjegyzés. E függvényt — bár már Euler is alkalmazta 1730 körül — azért nevezték el Riemannról, mert ő írta róla az első alapvető cikket, egyúttal kiterjesztve komplex kitevőkre.

Euler megmutatta, hogy a függvény végtelen szorzatként is előállítható,

$$\zeta(s) = \prod_{p \text{ prím}} \left(\frac{1}{1 - p^{-s}} \right). \quad (2)$$

Megjegyezzük, hogy meglehetősen bonyolult eljárással e függvény kiterjeszthető tetszőleges komplex számra, és e kiterjesztéssel kapcsolatos egy híres megoldatlan probléma. Riemann sejtése szerint a teljes komplex síkra kiterjesztett ζ függvény komplex zéróhelyei mindegyikének $\frac{1}{2}$ a valós része. Jelenleg több millió komplex zéróhely ismert expliciten, és valamennyinek $\frac{1}{2}$ a valós része, de a sejtés, az ún. *Riemann-hipotézis* bizonyítása egyelőre elérhetetlennek tűnik.

Az (1) sor az $s > 1$ esetben való konvergenciáját a bevezető függvényttel foglalkozó előadásokban bizonyítani szokták, így itt nem foglalkozunk vele. A (2) alternatív definíció jogosságának bizonyítását is csak vázoljuk.

A (2) jobb oldalán szereplő tényezők geometriai sorba fejthetők:

$$\frac{1}{1 - p^{-s}} = \sum_{k=1}^{\infty} p^{-ks},$$

ahol a jobb oldalon álló sor konvergens, mivel $0 < p^{-s} < 1$ minden $s > 1$ -re. Ha összeszorozzuk ezen sorokat (képezve azokat minden p prímre) a kapott szorzat minde tagja

$$p_1^{k_1 s} \cdots p_m^{k_m s} = \frac{1}{n^s},$$

ahol $p_1, \dots, p_m$ különböző prímelek, $k_i \geq 0$ és $n = p_1^{k_1} \cdots p_m^{k_m}$. A számelmélet alaptétele értelmében minden természetes szám egyértelműen előáll ilyen alakban, és pontosan egyszer szerepel $\frac{1}{n^s}$ alakú összeadandóként. Ez igazolja az Euler-féle (2) szerinti előállítást.

Alkalmazások a prímszámok elméletében.

Két — a bevezető számelméleti kurzusból — ismert tételre adunk új, analitikus bizonyítást.

6.2.1. Tétel. *Végtelen sok prímszám van.*

Bizonyítás. Tegyük föl, hogy csak véges sok prím létezik, s ezek $p_1, \dots, p_k$. Tetszőleges $p = p_i$ prímre, lévén $0 < 1/p_i < 1$ az $1/p$ kvóciensű mértani sor konvergens,

$$\sum_{n=1}^{\infty} \frac{1}{p^n} = \frac{1}{1 - p^{-1}}. \quad (3)$$

Képezzük ezeket a sorokat minden p_i -re, majd a kapott k sort szorozzuk össze

$$\prod_{i=1}^k \left(\sum_{n=1}^{\infty} \frac{1}{p_i^n} \right) = \prod_{i=1}^k \frac{1}{1 - p_i^{-1}} \quad (4)$$

Mivel a (3) baloldalán álló sor — lévén pozitív tagú — abszolút konvergens is, a (4)-beli sor is abszolút konvergens, így a tagok tetszőlegesen átrendezhetők. Tekintsünk a (4) bal oldalán álló sorokból, a szorzet tényezőiből rendre az $1/p_1^{m_1}, \dots, 1/p_k^{m_k}$ tagokat. Ezek szorzata

$$\frac{1}{p_1^{m_1}} \cdot \frac{1}{p_2^{m_2}} \cdot \dots \cdot \frac{1}{p_k^{m_k}} = \frac{1}{p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}}$$

amely egy „tipikus” kifejezés (4)-ből.

A számelmélet alaptétele szerint minden n természetes szám pontosan egyféleképp áll elő $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ alakban, ahol $m_i \geq 0$. Vegyük észre ugyanis, hogy e tétel bizonyítása független a prímszámok számától. Az előállítás unicitása miatt $1/n$ pontosan egyszer szerepel (2)-ben, így ezen egyenlőségből következik, hogy

$$\prod_{i=1}^k \left(\sum_{n=1}^{\infty} \frac{1}{p_i^n} \right) = \sum_{n=1}^{\infty} \frac{1}{n}.$$

A jobb oldalon a divergens harmónikus sor áll, míg a bal oldali szorzat véges. Így ez az egyenlőség lehetetlen, tehát a prímszámok száma nem lehet véges.

6.2.2. Tétel. *A prímszámok reciprokaiból álló sor divergens. Azaz, ha p_k jelöli az k -adik prímszámot, akkor a*

$$\sum_{k=1}^{\infty} \frac{1}{p_k} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots \quad (5)$$

végtelen sor divergens.

Bizonyítás. Tegyük föl, hogy az (5) sor konvergens, és az összege l . Ekkor részletösszegeire teljesül, hogy

$$\left| \sum_{k=1}^n \frac{1}{p_k} - l \right| \leq \frac{1}{2}$$

minden elegendően nagy n -re, ami azt (is) jelenti, hogy minden ilyen n -re

$$\sum_{m>n} \frac{1}{p_m} \leq \frac{1}{2}.$$

Következésképpen a

$$\sum_{k=1}^{\infty} \left(\sum_{m>n} \frac{1}{p_m} \right)^k \quad (6)$$

sor konvergens, hiszen majorálja a konvergens $\sum_{k=1}^{\infty} 1/2^k$ mértani sor.

Ha $q = p_1 \dots p_n$, akkor a $p_1, \dots, p_n$ prímek egyike sem osztója a $qr + 1$ ($r \geq 1$) egészeknek, ezért szükségképp

$$qr + 1 = p_{n_1} \dots p_{n_k}, \quad n_i > n,$$

ahol a szereplő prímek nem föltétlenül különbözők. Ezért reciproka $\frac{1}{p_{n_1} \dots p_{n_k}}$ alakban előfordul a

$$\left(\sum_{m>n} \frac{1}{p_m} \right)^k$$

sor kifejtésében. Mivel a számelmélet alaptétele értelmében pontosan egyszer fordul elő (6)-ban, az tartalmazza a

$$\sum_{r=1}^{\infty} \frac{1}{qr + 1}$$

sort, tehát ez utóbbi is konvergens.

Ezen sor azonban divergens, ugyanis

$$\begin{aligned} \sum_{r=1}^{\infty} \frac{1}{qr + 1} &> \sum_{r=1}^{\infty} \frac{1}{qr + q} \\ &= \frac{1}{q} \sum_{r=1}^{\infty} \frac{1}{r + 1} = \sum_{r=2}^{\infty} \frac{1}{r}, \end{aligned}$$

ami bizonyítja az (5) sor divergenciáját.

Megjegyzések.

(1) Az (5) sor divergenciája igen lassú, közelítőleg $\log \log n$ nagyságrendben növekszik csak a részletösszegek sorozata. Egy jellemző példa, hogy

$$\sum_{p < 10^{18}} \frac{1}{p} < 4,$$

azaz az első 50 millió prímszám reciprokának összege nem éri el a 4-et.

(2) Előbbi tételünkből az is következik, hogy végtelen sok prímszám van.

6.3. A $\zeta(2)$ meghatározása.

Eljárásunk — amely T.M. Apostoltól származik — alapja az az ötlet, amellyel 1979-ben R. Apéry igazolta $\zeta(3)$ irracionális voltát. Egy kettős integrált fogunk kiszámítani kétféleképp, s ebből adódik, hogy $\zeta(2) = \frac{\pi^2}{6}$. Nevezetesen, az

$$I = \int_0^1 \int_0^1 \frac{1}{1 - xy} dx dy \quad (7)$$

integrált fogjuk kétféleképp kiszámolni.

Először fejtsük hatványsorba az integranduszt,

$$\int_0^1 = \sum_{n=0}^{\infty} x^n y^n,$$

és így

$$\begin{aligned} I &= \int_0^1 \int_0^1 \frac{1}{1-xy} dx dy = \int_0^1 \int_0^1 \sum_{n=0}^{\infty} x^n y^n \\ &= \int_0^1 \sum_{n=0}^{\infty} \frac{y^n}{n+1} dy = \sum_{n=0}^{\infty} \frac{1}{(n+1)^2} = \zeta(2). \end{aligned} \quad (8)$$

Másodikként vezessük be az

$$x = \frac{u-v}{\sqrt{2}}, \quad y = \frac{u+v}{\sqrt{2}}$$

helyettesítést, amely lényegében egy $\frac{\pi}{4}$ -es elforgatást jelent. Így

$$1-xy = \frac{2-u^2+v^2}{2},$$

és az integrációs tartomány most az uv síkon egy olyan négyzet, amelynek átellenes csúcsai a $(0,0)$, $(\sqrt{2},0)$ pontok.

Vegyük észre, hogy az integrációs tartomány szimmetrikus az u tengelyre, és így

$$I = 4 \int_0^{1/\sqrt{2}} \left(\int_0^u \frac{dv}{2-u^2+v^2} \right) du + 4 \int_{1/\sqrt{2}}^{\sqrt{2}} \left(\int_0^{\sqrt{2}-u} \frac{dv}{2-u^2+v^2} \right) du. \quad (9)$$

Tudjuk, hogy

$$\int_0^x \frac{dt}{a^2+t^2} = \frac{1}{a} \arctan \frac{x}{a},$$

és így

$$\int_0^u \frac{dv}{2-u^2+v^2} = \frac{1}{\sqrt{2-u^2}} \arctan \frac{u}{\sqrt{2-u^2}},$$

továbbá

$$\int_0^{\sqrt{2}-u} \frac{dv}{2-u^2+v^2} = \frac{1}{\sqrt{2-u^2}} \arctan \frac{\sqrt{2}-u}{\sqrt{2-u^2}}.$$

Ezeket alkalmazva

$$I = 4 \int_0^{1/\sqrt{2}} \arctan \frac{u}{\sqrt{2-u^2}} \frac{du}{\sqrt{2-u^2}} + 4 \int_{1/\sqrt{2}}^{\sqrt{2}} \arctan \frac{\sqrt{2}-u}{\sqrt{2-u^2}} \frac{du}{\sqrt{2-u^2}} = I_1 + I_2.$$

Az integrálok kiszámításához ismét helyettesítéseket alkalmazunk. I_1 -ben legyen $u = \sqrt{2} \sin 2\vartheta$, és ekkor $du = \sqrt{2} \cos 2\vartheta d\vartheta = \sqrt{2-u^2} d\vartheta$, valamint $\tan \vartheta = \frac{u}{\sqrt{2-u^2}}$.

Ezután már rutin számolással adódik, hogy

$$I_1 = 4 \int_0^{\pi/6} \vartheta d\vartheta = 2 \left(\frac{\pi}{6} \right)^2. \quad (10)$$

Ha az I_2 integrálnál az $u = \sqrt{2} \cos 2\vartheta$ helyettesítést alkalmazzuk, akkor az előbbihez hasonló számolással

$$I_2 = 8 \int_0^{\pi/6} \vartheta d\vartheta = 4 \left(\frac{\pi}{6} \right)^2 \quad (11)$$

adódik.

Így (10) és (11) alapján

$$I = I_1 + I_2 = 6 \left(\frac{\pi}{6} \right)^2 = \frac{\pi^2}{6}$$

adódik, azaz

$$\zeta(2) = \frac{\pi^2}{6}.$$

Ezzel igazoltuk a következő tételt.

6.3.1. Tétel. *A $\zeta(2)$ transzcendens szám.*

Mit tudunk a ζ függvény egész helyeken fölvevett értékeiről?

1. 1978-ban igazolta Apéry azt a régi sejtést, miszerint $\zeta(3)$ irracionális. Sajnos meglehetősen keveset tudunk $\zeta(s)$ értékeiről, ha s páratlan természetes szám.

2. Ismert, hogy tetszőleges $k \in \mathbb{N}$ -re

$$\zeta(2k) = b_k \pi^{2k},$$

ahol $b_k \in \mathbb{Q}$ minden k -ra, így a $\zeta(2k)$ értékek transzcendensek minden $k \in \mathbb{N}$ -re.

7. HILBERT VII. PROBLÉMÁJÁRÓL.

David Hilbert fiatal göttingeni matematikus professzor, aki a matematika alapjaival kapcsolatos kutatásaival vált először híressé, fölhívást kapott a II. Matematikai Világkongresszus (1900. Párizs) szervezőitől egy plenáris előadás tartására. A szervezők nem rögzítették előre az előadás témáját, mert azt hitték, hogy a legújabb eredményeiről, a bizonyításelméletben elértokről fog beszélni.

Nem ez történt. Hilbert előadásában 23 olyan problémát vetett föl — ismertetve röviden azok előzményeit — amelyeket a legfontosabbaknak tartott a XX. század matematikusai számára. Az összeállítás meglehetősen heterogénre sikeredett. Volt köztük olyan, amelyet a kongresszus alatt megoldottak, de a mai napig megoldatlan is. Számos fölvetése egészen új kutatási irányokat jelölt ki, elméletek teljesedtek ki belőlük.

Egy részlet D. Hilbert 1900-as párizsi előadásából.

Hermite és Lindemann eredményeit — amelyek az exponenciális függvényekre vonatkoznak — minden matematikus nagyra értékeli. Ezen az úton tovább kell haladni, s az elkövetkező időben az alábbi problémát kellene megoldani.

Bizonyos — az analízisben fontos — transzcendens függvények egyes algebrai szám helyeken algebrai szám értékeket vesznek föl. Úgy tűnik, hogy ezt érdemes alaposan megvizsgálni. Ugyanis általában azt képzeljük, hogy a transzcendens függvények mindenütt transzcendens értékeket vesznek föl. Tesszük ezt annak ellenére, hogy ismerünk olyan transzcendens függvényeket, amelyek algebrai számokhoz algebrai számot, sőt racionálisat rendelnek.

Például az $e^{i\pi z}$ exponenciális függvény értéke minden $z \in \mathbb{Q}$ -ra algebrai, míg minden $z \in \mathbb{A} \setminus \mathbb{Q}$ -ra transzcendens. Ezen állítás geometriailag is megfogalmazható. Ha egy egyenlőszárú háromszögben az alapon fekvő szög és a szárak által alkotott szög aránya transzcendens, akkor az alap és a szár aránya is transzcendens. Bár ez egy igen egyszerűen hangzó állítás, ekvivalens Hermite és Lindemann eredményével, s a bizonyítása is igen nehéz, sőt meglehetősen bonyolult. Hasonlóan nehéz lehet a bizonyítása a következő állításnak is.

Hilbert kérdése, a VII. Probléma. Legyen $\alpha \in \mathbb{A}$ és $\beta \in \mathbb{A} \setminus \mathbb{Q}$, ekkor az α^β alakú számok, például $2^{\sqrt{2}}$, $e^\pi = i^{-2i}$ mindig transzcendens szám, vagy legalább irracionális.

Tovább az előadás.

Biztos vagyok benne, hogy ezen, és a hasonló problémák megoldása egészen új módszereket igényel, s egy új szemléletet is ad. Új megvilágításba helyezi az irracionális és a transzcendens számokat.

Részlet Hilbert egy előadásából, Göttingen 1919.

A VII. Probléma nagyon nehéz, így érdemes összehasonlítani néhány ismert problémával.

- A Riemann-hipotézis bizonyítása irányába az utóbbi években komoly előrehaladás történt, így nagyon reméli, hogy még megéri a bizonyítását.
- Számos biztató eredmény van a Fermat-sejtéssel kapcsolatban is, ezért talán a hallgatóság legfiatalabb tagjai megérik a sejtés bizonyítását.
- Annak a bizonyítását azonban, hogy a $2^{\sqrt{2}}$ transzcendens szám, a jelenlevők közül senki sem fogja látni.

Hilbert vélekedéséről.

- A Riemann-hipotézis, azaz a ζ függvény minden komplex zéróhelyének a valós része $\frac{1}{2}$, a mai napig nyitott kérdés.
- A Fermat sejtés bizonyítását 1993-ban publikálta A. Wiles.
- Azaz egy kérdésben Hilbert tévedett, egyben talán nem, ha ...

A harmadikról. Az első részleges megoldás, az első nem teljes válasz 1929-ben jelent meg, majd pár év alatt teljessé vált a megoldás.

A VII. Probléma részleges megoldása.

1. Gelfond tétele. (1929) *Ha β komplex kvadratikus irracionális szám, akkor α^β transzcendens.*

Ez tartalmazza az e^π esetet.

2. Kuzmin és Siegel tétele. (1930) *α^β akkor is transzcendens, ha β valós kvadratikus irracionális szám.*

Megjegyzések.

- (1) A két matematikus eredményét egymástól függetlenül érte el.
- (2) Hilbert megérte annak bizonyítását, hogy $2^{\sqrt{2}}$ transzcendens szám.

A VII. Probléma teljes megoldása.

Gelfond - Schneider tétel. (1934) *Ha α, β 0 és 1-től különböző algebrai számok, továbbá β irracionális, akkor α^β transzcendens szám.*

Két további ekvivalens állítás.

- 1.** Ha α, β 0, 1-től különböző algebrai számok, akkor $\log \alpha / \log \beta$ racionális, vagy transzcendens.
- 2.** Legyenek α, β nemzéró algebrai számok. Ha $\log \alpha, \log \beta$ lineárisan függetlenek a racionális számtest fölött, akkor lineárisan függetlenek az algebrai számok teste fölött.

Megjegyzések.

- (1) Gelfond és Schneider egymástól függetlenül jutott el ezen eredményhez.
- (2) Hilbert sejtése a legerősebb formában bizonyult igaznak.
- (3) Hilbert 1943-ban halt meg, azaz megérte sejtése teljes bizonyítását.
- (4) Még egy 1919-es tévedése.
- (5) Az előbbi tévedések nem árnyékolják be azon általános vélekedést, miszerint David Hilbert a XIX. század utolsó harmadának és a XX. század első felének egyik legnagyobb hatású matematikusa volt.