SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Irrationalitet och transcendens hos talen e och pi

by

Anu Kokkarinen

2011 - No 13

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Irrationalitet och transcendens hos talen e och pi

Anu Kokkarinen

Självständigt arbete i matematik 30 högskolepoäng, GN

Handledare: Erik Svensson

2011

Sammanfattning

Antikens greker fick problem när de ville härleda exakta värden till irrationella tal såsom π. Senare generationer stötte på samma problem med talet e: det exakta värdet var omöjligt att bestämma. Först på 1700-talet lyckades man visa att e och π är irrationella. Ett algebraiskt tal är en rot till ett polynom med heltalskoefficienter. På 1800-talet visades att varken e eller π är algebraiskt.

Detta arbete ger en överblick över hur man kan visa att e och π är irrationella och transcendenta.

Innehåll

1 Introduktion

Vissa naturligt uppkommande tal, såsom $\sqrt{2}$ eller π, visade sig vara svåra att räknas ut exakt. Approximationer blev bättre och bättre men beräkningarna tycktes inte ta slut någonstans. Man började därför undra om det fanns tal som inte kunde bestämmas exakt, som bara kunde approximeras. *Som hade en oändlig, oregelbunden decimalutveckling.* Oändlighet var – eller är – inte något som är lätt att begripa. Därför började man kalla dessa hypotetiska tal *irrationella*, tal som inte var vettiga, inte var lika begripliga som 1 eller 2. Ekvivalent med oändlig, oregelbunden decimalutveckling är att säga att ett tal inte kan uttryckas som en kvot av två heltal. Redan under antiken i Grekland lyckades man visa att $\sqrt{2}$ inte är rationellt med ett enkelt motsägelsebevis. Ändå var greker motvilliga att acceptera irrationella tal, och enligt legenden dränktes Pythagoras lärunge Hippasos för att han avslöjade existensen av irrationella tal till allmännheten.

Ett tal som kan konstrueras med hjälp av en passare och rätskiva kallas konstruerbart (med rätskiva menas här en oändligt lång linjal som bara har en markering). Till exempel är $\sqrt{2}$ ett konstruerbart tal, eftersom det kan definieras som hypotenusan av en rätvinklig triangel vars kateter har längden ett. Man kom att fråga om det är möjligt – med passare och rätskiva – att rita en kvadrat med samma area som en cirkel. Många misslyckade försök tydde på att det inte går, men det tycktes vara oerhört svårt att bevisa. Problemet började kallas cirkelns kvadratur, och det är ett av de tre klassiska konstruktionsproblemen tillsammans med kubens fördubbling och vinkelns tredelning. Det var inte förrän slutet av 1800-talet då man äntligen kunde konstatera att cirkeln inte går att kvadrera. Svaret dök upp när man började undersöka ett nytt sätt att klassificera tal: *algebraiska* och *transcendenta*.

Ett algebraiskt tal är en rot till ett polynom med heltalskoefficienter. Eftersom varje polynom med rationella koefficienter efter multiplikation med ett lämpligt tal kan omvandlas till ett polynom med heltalskoefficienter (och omvänt), kan vi ekvivalent definiera algebraiska tal som rötter till något polynom i $\mathbb{Q}[x]$. I de flesta fall använder vi heltal, men ibland är det lättare att hantera rationella tal. Det är uppenbart att alla rationella tal är algebraiska, ty om p/q är ett rationellt tal, då löser det ekvationen

$$qx - p = 0$$

Omvänt om x löser en förstagradsekvation av formen $qx - p = 0$, så måste x vara ett rationellt tal. Därför kan en förstagradspolynom i $\mathbb{Z}[x]$ inte ha ett irrationellt tal som rot, eller omvänt om ett polynom i $\mathbb{Z}[x]$ har en irrationell rot, måste dess grad vara minst 2. Vidare är alla n:te rötter av rationella tal, till exempel $\sqrt{2}$ algebraiska ty de är rötter till polynom av formen

$$qx^n - p = 0$$

Efter att ha definierat algebraiska tal, är det naturligt att definiera en annan talgrupp: ett transcendent tal är *inte* en rot till något polynom med heltalskoefficienter.

Det var länge okänt om transcendenta tal överhuvudtaget existerade. Den generella uppfattningen bland matematiker under första halvan av 1800-talet var att mängden av transcendenta tal var tom. Lustigt nog visade det sig att de inte bara existerade, men år 1872 visade Georg Cantor (1845-1918) att nästan alla reella tal är transcendenta (på så sätt att mängden av transcendenta tal är överuppräknelig, medan mängden av algebraiska tal är uppräknelig). Att det finns ett uppräkneligt antal algebraiska tal är logiskt om man tänker på att det finns ett uppräkneligt antal polynom, och att var och en av dem har ett ändligt antal rötter. Ironiskt nog är det ytterst svårt att visa att ett specifikt tal är transcendent även om de transcendenta talen är så många.

I slutet av 1800-talet publicerades äntligen ett bevis att π är ett transcendent tal. Att π inte är en rot till ett poynom med rationella koefficienter medför naturligtvis att cirkeln inte kan kvadreras.

1.1 Två matematiska konstanter – π och e

Som känt betecknas förhållandet mellan en cirkels omkrets och diameter med den grekiska bokstaven π. Konstanten har varit känd i flera tusen år och den dyker upp i många olika grenar av matematik, inte bara geometri. På grund av dess lång historia och omedelbara geometriska egenskaper är det omöjligt att säga vem som kom på π först och när. Arkimedes tycks ha varit den förste att härleda en rigorös approximation av π. Han använde omkretser av regelbundna polygoner som var inskrivna och omskrivna en cirkel för att bestämma undre och övre gränsen för π. Metoden var mindre effektiv, och 96-sidiga polygoner gav bara två rätta decimaler.

Basen till den naturliga logaritmen betecknas med e, och kallas ibland Eulers konstant efter Leonhard Euler (1707-1783). Det var dock inte Euler som upptäckte e, utan äran ges vanligen till den italienske matematikern Jakob Bernoulli (1654-1705). Bernoulli stötte på e när han undersökte sammansatt ränta, eller ränta på ränta. Sammansatt ränta kan beskrivas med formeln

$$a\left(1+\frac{x}{n}\right)^n \tag{1.1}$$

där a är startkapitalet, x räntan och n antalet perioder. Bernoulli undrade om man, genom att öka antalet perioder, kunde uppnå obegränsat stora vinster. Med andra ord undrade han om (1.1) hade ett oändligt gränsvärde. För att underlätta beräkningarna förenklade han (1.1) något. Han tilldelade både startkapitalet och räntan värdet 1, och började undersöka följande gränsvärde:

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n \tag{1.2}$$

Värdet $x = 1$, räntan 100%, är naturligtvis inte någon realistisk ränta, men (1.2) ger en övre gräns för andra värden på $x \in [0, 1]$. Det visade sig att detta gränsvärde är ändlig, och senare generationer gav det beteckningen e efter Euler.

Definition 1.1.1.

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

Ett annat sätt att definiera e är som en oändlig summa.

Sats 1.1.2.

$$e = \sum_{n=0}^{\infty}\frac{1}{n!}$$

Vi avslutar detta avsnitt med att påminna läsaren om en känd formel som binder ihop e och π: $e^{i\pi} = -1$.

1.2 Lite analys

I detta avsnitt introducerar vi några elementära satser och definitioner. Notera att i denna uppsats räknas 0 med i de naturliga talen, det vill säga $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Vi börjar med att påminna läsaren om medelvärdessatsen:

Sats 1.2.1 (Medelvärdessatsen)**.** *Låt $f(x)$ vara kontinuerlig på det slutna intervallet $[a, b]$ och deriverbar på (a, b). Då finns det ett reellt tal $\xi \in (a, b)$ sådant att*

$$f(b) - f(a) = f'(\xi)(b - a)$$

Alternativt kan vi säga att det finns ett reellt tal $\lambda \in (0, 1)$ sådant att

$$f(b) - f(a) = f'(\lambda(b - a))(b - a)$$

Eftersom vi kommer att prata mycket om polynom, tar vi upp några ganska intuitiva satser angående dem. Ett polynom är *irreducibelt* i $R[x]$ (där R är en ring) om det inte kan faktoriseras i $R[x]$. Som exempel kan vi ta $x^2-4=(x-2)(x+2)$ (reducibelt i $\mathbb{Z}[x]$) och $x^2+4=(x-2i)(x+2i)$ (irreducibelt i $\mathbb{Z}[x]$, men inte i $\mathbb{C}[x]$).

Sats 1.2.2. *Om $p(x) \in \mathbb{Q}[x]$ är irreducibelt i $\mathbb{Q}[x]$, så har $p(x)$ inga rationella rötter.*

Denna sats är en enkel följd av formeln $p(x)=(x-a/b)q(x)+f(a/b)$, där $g(x) \in \mathbb{Q}[x]$, vilket följer av divisionsalgoritmen för polynom. Samma gäller naturligtvis för polynom i $\mathbb{Z}[x]$, och det är klart att varje algebraiskt tal är rot till ett polynom som är irreducibelt i $\mathbb{Z}[x]$.

Av symmetriskäl är det av intresse att betrakta polynom vars koefficient till x^n är lika med 1. Sådana polynom kallas *moniska*, och algebraiska tal som är rötter till något moniskt polynom i $\mathbb{Z}[x]$ kallas *algbraiska heltal*. Till exempel är $\sqrt{2}$ ett algebraiskt heltal, medan de enda rationella tal som är rötter till moniska polynom i $\mathbb{Z}[x]$ är heltal.

Sats 1.2.3. *Låt $p(x)=b_nx^n+\cdots+b_1x+b_0$ vara ett polynom i $\mathbb{Z}[x]$ med rötter $a_1,\ldots,a_n$. Då är a_ib_n ett algebraiskt heltal för $i \in [1,n]$.*

Denna sats följer direkt av att multiplicera $p(a_i)$ med b_n^{n-1}.

Sats 1.2.4. *För varje algebraiskt tal a existerar det ett unikt irreducibelt moniskt polynom $p(x)$ i $\mathbb{Q}[x]$ av lägsta grad, sådant att $p(a)=0$.*

$p(x)$ i satsen ovan karakteriseras av att det delar varje polynom där a är en rot. Notera att $p(x)$ är ett polynom i $\mathbb{Q}[x]$, inte $\mathbb{Z}[x]$ – detta beror på att $\mathbb{Z}$ inte är en kropp.

En funktion kallas symmetrisk om man kan byta plats mellan variablerna utan att ändra funktionens värde. Till exempel är $f(x,y)=x+y=y+x=f(y,x)$ symmetrisk, medan $f(x,y)=x^2+y \neq y^2+x=f(y,x)$ inte är det. Till varje n-tippel $(x_1,\ldots,x_n)$ kan vi definiera symmetriska funktioner av följande form

$$e_j(x_1,\ldots,x_n)=\sum_{i_1<\cdots<i_j} x_{i_1}\cdots x_{i_j}$$

för $j=0,1,\ldots,n$. Dessa funktioner kallas de *elementära symmetriska polynomen* av $(x_1,\ldots,x_n)$. Till exempel i tre varibler har vi följande elementära polynom:

$$\begin{aligned}
e_0(x,y,z)&=1\\
e_1(x,y,z)&=x+y+z\\
e_2(x,y,z)&=xy+xz+yz\\
e_3(x,y,z)&=xyz
\end{aligned}$$

Med denna definition är vi färdiga att presentera följande viktiga sats:

Sats 1.2.5 (Fundamentalsats för symmetriska polynom)**.** *Låt R vara en ring, och $p(x_1,\ldots,x_n)$ ett polynom vars koefficienter tillhör R. Låt $e_1,\ldots,e_n$ beteckna de elementära symmetriska polynomen av $x_1,\ldots,x_n$. Om p är symmetriskt, kan det skrivas som ett polynom av $(e_1,\ldots,e_n)$ med koefficienterna från R.*

Beviset för denna sats finns till exempel i [[13], Theorem 6.3.3.1]. Följande sats är en omskrivning av [[13], Lemma 6.4.1.1]:

Följdsats 1.2.6. *Låt $p(x)$ vara ett moniskt polynom i $\mathbb{Z}[x]$, och beteckna rötterna till $p(x)$ med $a_1,\ldots,a_n$. Varje symmetriskt polynom av $(a_1,\ldots,a_n)$ med heltalskoefficienter är ett heltal.*

Bevis Beteckna de elementära symmetriska polynomen av $a_1, \dots, a_n$ med $e_1, \dots, e_n$. Enligt antagandet har vi att

$$p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = (x - a_1)(x - a_2) \cdots (x - a_n) \in \mathbb{Z}[x]$$

Om vi utvecklar högerledet och matchar koefficienterna får vi att

$$\begin{aligned}
b_0 &= (-1)^n a_1 \cdots a_n \\
b_1 &= (-1)^{n-1}(a_2 \cdots a_n + a_1 a_3 \cdots a_n + \cdots + a_1 \cdots a_{n-1}) \\
&\vdots \\
b_{n-2} &= a_1 a_2 + a_1 a_3 + \cdots + a_1 a_n + a_2 a_3 + \cdots + a_{n-1} a_n \\
b_{n-1} &= -(a_1 + \cdots + a_n)
\end{aligned}$$

Varje koefficient motsvarar någon av de elementära symmetriska polynomen av $a_1, \dots, a_n$ (möjligen multiplicerad med -1), varav följer att $e_i \in \mathbb{Z}$ för varje $i \in 1, 2, \dots, n$. Enligt sats 1.2.5 kan varje symmetriskt polynom i $\mathbb{Z}[a_1, \dots, a_n]$ skrivas som ett polynom av de elementära symmetriska polynomen med koefficienterna från $\mathbb{Z}$. Det följer då direkt att varje symmetriskt polynom i $\mathbb{Z}[a_1, \dots, a_n]$ är ett heltal. ■

Om vi i följdsatsen ovan inte hade krävt att $p(x)$ är moniskt, så skulle varje symmetrisk polynom av $(a_1, \dots, a_n)$ i $\mathbb{Z}[x]$ (eller i $\mathbb{Q}[x]$) vara ett rationellt tal.

1.3 Kedjebråk

Av historiska skäl tar vi upp kedjebråk. Ett ändligt kedjebråk är ett matematiskt uttryck av formen

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

där a_0 är ett heltal och $a_i, i \geq 1$ är positiva heltal. Ofta används skrivsättet $[a_0; a_1, a_2, ..., a_n]$ för att spara utrymme och förbättra läsbarhet. På motsvarande sätt ges ett oändligt kedjebråk av

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

och betecknas $[a_0; a_1, a_2, ...]$. Oändliga kedjebråk kan definieras som gränsvärdet av en sekvens av ändliga kedjebråk, $\lim_{n\to\infty}[a_0; , a_1 a_2, \dots, a_n] = [a_0; a_1, a_2, \dots]$. Observera att en ändlig kedjebråksutveckling inte är unikt bestämd, men den enda möjliga omskrivningen är $[a_0; a_1, a_2, ..., a_n] = [a_0; a_1, a_2, ..., a_n - 1, 1]$. Oändliga kedjebråk har en unik form.

2 Irrationalitet

2.1 Kedjebråk och irrationalitet

Vi fortsätter med några egenskaper för kedjebråk. Skälet för att ta upp kedjebråk är att de ser annorlunda ut beroende på om talet ifråga är rationellt eller irrationellt. Betrakta ett godtyckligt rationellt tal p/q, där $p, q \in \mathbb{Z}, q \geq 1$. Enligt divisionsalgoritmen finns det unika heltal k_0 och r_0, $0 \leq r_0 < q$, sådana att

$$p = k_0 q + r_0$$

Om vi fortsätter detta förfarande, det vill säga tillämpar Euklides algoritm, kommer vi till slut att få en restterm lika med noll (eftersom varje restterm är strikt mindre är den föregående). Vi kommer att få följande ekvationer:

$$\begin{aligned}
\frac{p}{q} &= k_0 + \frac{r_0}{q} \\
\frac{q}{r_0} &= k_1 + \frac{r_1}{r_0} \\
\frac{r_0}{r_1} &= k_2 + \frac{r_2}{r_1} \\
&\vdots \\
\frac{r_{m-3}}{r_{m-2}} &= k_{m-1} + \frac{r_{m-1}}{r_{m-2}} \\
\frac{r_{m-2}}{r_{m-1}} &= k_m
\end{aligned}$$

Genom om ta inverser av dessa ekvationer och sätta in dem i varandra får vi att

$$\frac{p}{q} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots + \cfrac{1}{k_{m-1} + \cfrac{1}{k_m}}}}}$$

Ett rationellt tal har således ett ändligt kedjebråk. Omvänt kan man med induktion bevisa att ett ändligt kedjebråk kan skrivas om som en kvot mellan två heltal. Det följer då direkt att följande gäller:

Sats 2.1.1. *Ett reellt tal är irrationellt om och endast om det har ett oändligt kedjebråk.*

Kedjebråksutvecklingen för ett irrationellt tal kan bestämmas på liknande sätt som för ett rationellt tal. Betrakta omskriningen

$$x = \lfloor x \rfloor + (x - \lfloor x \rfloor)$$

där $\lfloor x \rfloor$ betecknar det största heltal som är mindre än eller lika med x. Om $x = p/q$, då ser vi att $\lfloor x \rfloor$ och $x - \lfloor x \rfloor$ motsvarar de unikt bestämda talen k_0 respektive r_0/q som vi fick med hjälp av divisionsalgoritmen. Divisionsalgoritmen är skapad endast för heltal, men ovanstående ekvation gäller för alla reella tal. Den enda stora skillnaden är att om x är irrationellt, då kan $x - \lfloor x \rfloor$ aldrig vara lika med 0.

Om vi antar att ξ är ett irrationellt tal, och sätter $\xi_0 = \xi$ och $a_0 = \lfloor \xi \rfloor$, samt $\xi_i = \frac{1}{\xi_{i-1} - a_{i-1}}$ och $a_i = \lfloor \xi_i \rfloor$ för $i = 1, 2, \ldots$, så får vi att

$$
\begin{aligned}
\xi = \xi_0 = a_0 + (\xi_0 - a_0) = a_0 + \frac{1}{\xi_1} = a_0 + \frac{1}{a_1 + (\xi_1 - a_1)} = \\
= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\xi_2}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + (\xi_2 - a_2)}} = \\
= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\xi_3}}} = \cdots
\end{aligned}
$$

För varje i gäller det att $0 < \xi_i - \lfloor \xi_i \rfloor < 1$, varav följer att $1/(\xi_i - \lfloor \xi_i \rfloor)$ alltid är större än 1, och a_i är ett positivt heltal för varje $i = 1, 2, \ldots$. Eftersom ξ är irrationellt är ξ_i aldrig ett heltal. Alltså är kedjebråksutvecklingen för ξ lika med $[a_0; a_1, a_2, \ldots]$. Metoden här ger också kedjebråksutvecklingen av ett godtyckligt rationellt tal. Då blir ξ_i ett heltal efter ett ändligt antal steg.

De första bevisen för att e och π är irrationella använde kedjebråksutvecklingar. Dessa metoder är dock ineffektiva och används sällan i litteraturen. Vi kommer ändå – av historiska skäl och för att illustrera metoden – att ta några exempel på hur man kan utnyttja kedjebråk. För att förbereda oss inför nästa avsnitt måste vi undersöka följande uttryck:

$$
r_i = [a_0; a_1, a_2, a_3, \cdots, a_i] = \frac{p_i}{q_i} \tag{2.1}
$$

r_i kallas den i:te konvergenten till ett kedjebråk. Vi anar att konvergenterna beter sig olika när vi låter i växa beroende om kedjebråksutveckling är ändlig eller oändlig. De två första konvergenterna är:

$$
\begin{aligned}
r_0 = a_0 = \frac{p_0}{q_0} \quad & \text{där} \quad p_0 = a_0, q_0 = 1 \\
r_1 = a_0 + \frac{1}{a_1} = \frac{p_0 a_1 + 1}{a_1} = \frac{p_1}{q_1} \quad & \text{där} \quad p_1 = p_0 a_1 + 1, q_1 = a_1
\end{aligned}
$$

Fortsätter man på samma sätt, så kommer man att se ett mönster. Detta formuleras i följande sats. Beviset är ett enkelt induktionsbevis, och lämnas till läsaren.

Sats 2.1.2. *Följande rekursionsrelationer gäller*

$$
\begin{aligned}
p_i &= a_i p_{i-1} + p_{i-2}, \quad i \geq 2 \\
q_i &= a_i q_{i-1} + q_{i-2}, \quad i \geq 2
\end{aligned}
$$

tillsammans med begynnelsevillkoren $p_0 = a_0$, $q_0 = 1$, $p_1 = p_0 a_1 + 1$ *och* $q_1 = a_1$.

Mer om kedjebråk finns i [12].

2.2 Irrationalitet hos e

Som vi alla vet är e ett irrationellt tal. Vi formulerar detta i en sats för att tydligare kunna referera till det senare:

Sats 2.2.1. *e är irrationellt.*

Att visa att e är irrationellt kräver ingen avancerad matematik. De första bevisen utnyttjar dock inte de eleganta analytiska sambanden som möjliggör enkla bevis, utan använder de något krångliga kedjebråken. I detta avsnitt presenteras två i princip helt olika bevis.

Cohn 2006

Den förste som lyckades fastställa att e verkligen är irrationellt var Leonhard Euler. I sitt mest kända verk *Introductio in analysin infinitorium* (1748) presenterar han följande samband:

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, ...] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \ddots}}}}} \tag{2.2}$$

Formel (2.2) visar att e är irrationellt enligt sats 2.1.1. Det är svårt att följa Eulers resonemang, eftersom han inte skriver ut alla steg utan bara konstaterar resultat. Vi kommer därför inte att presentera hans bevis här. Den intresserade läsaren hänvisas till [[14], Kapitel 32], där C. Edward Sandifer rekonstruerar Eulers beräkningar.

Henry Cohn formulerade ett speciellt kort bevis av (2.2) i artikeln [3]. Det speciella med Cohns bevis är att det är ovanligt kompakt med tanke på att det i princip bygger på kedjebråk.

Vi börjar med att skriva om (2.2) i en aning snyggare form:

$$e = [1; 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, ...] \tag{2.3}$$

Ovanstående är ekvivalent med (2.2), ty om $x = [1; 2, 1, 1, 4, \ldots]$, då är

$$e = 1 + \cfrac{1}{0 + \cfrac{1}{1 + \cfrac{1}{x}}} = 2 + \frac{1}{x}$$

För att visa kedjebråksutvecklingen (2.3) räcker det att visa att den i:te konvergenten $r_i = p_i/q_i$ av (2.3), definierad som i (2.1), konvergerar mot e. Om vi sätter $e = [a_0; a_1, a_2, \ldots]$ kan mönstret i kedjebråksutveckling (2.3) beskrivas matematiskt med följande formler:

$$a_{3i+1} = 2i \quad \text{och} \quad a_{3i} = a_{3i+2} = 1, \quad i = 0, 1, 2, \ldots$$

Med detta kan vi skriva om rekursionsrelationer i sats 2.1.2 som

$$\begin{array}{lll} p_{3n} = p_{3n-1} + p_{3n-2}, & q_{3n} = q_{3n-1} + q_{3n-2}, & n \geq 1 \\ p_{3n+1} = 2np_{3n} + p_{3n-1}, & q_{3n+1} = 2nq_{3n} + q_{3n-1}, & n \geq 1 \\ p_{3n+2} = p_{3n+1} + p_{3n}, & q_{3n+2} = q_{3n+1} + q_{3n}, & n \geq 1 \end{array}$$

tillsammans med begynnelsevillkoren $p_0 = 1$, $q_0 = 1$, $p_1 = 1$, $q_1 = 0$. På grund av nollan i utvecklingen, uppfyller (2.3) inte definitionen av kedjebråk. Därför är den första konvergenten

$r_1 = p_1/q_1$ odefinierad. Detta spelar dock ingen roll i vårt resonemang nedan. Definiera

$$\begin{aligned} A_n &= \int_0^1 \frac{x^n(x-1)^n}{n!} e^x \,\mathrm{d}x \\ B_n &= \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x \,\mathrm{d}x \\ C_n &= \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x \,\mathrm{d}x \end{aligned}$$

Nästa lemma binder ihop dessa integraler med kedjebråksutvecklingen.

Lemma 2.2.2. *Låt p_i och q_i vara definierade som i sats 2.1.2. Då gäller för $n \geq 0$ att*

$$\begin{aligned} A_n &= q_{3n}e - p_{3n} \\ B_n &= p_{3n+1} - q_{3n+1}e \\ C_n &= p_{3n+2} - q_{3n+2}e \end{aligned}$$

Bevis Det följer direkt av definitionerna av A_n, B_n och C_n att

$$C_n = B_n - A_n \tag{2.4}$$

för alla $n \geq 0$. För $n \geq 1$ har vi följande samband:

$$A_n = -B_{n-1} - C_{n-1} \tag{2.5}$$
$$B_n = -2nA_n + C_{n-1} \tag{2.6}$$

Låt oss börja med att visa sambandet (2.5). Från produktregeln får vi att

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{x^n(x-1)^n}{n!}e^x\right) = \frac{x^n(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n-1}}{(n-1)!}e^x + \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x$$

Om vi nu integrerar ovanstående ekvation från 0 till 1 så får vi att

$$A_n + B_{n-1} + C_{n-1} = \left[\frac{x^n(x-1)^n}{n!}e^x\right]_0^1 = 0$$

vilket är ekvivalent med (2.5). För att visa (2.6), betrakta

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{x^n(x-1)^{n+1}}{n!}e^x\right) &= \frac{x^{n-1}(x-1)^{n+1}}{(n-1)!}e^x + (n+1)\frac{x^n(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n+1}}{n!}e^x \\ &= (x-1)\frac{x^{n-1}(x-1)^n}{(n-1)!}e^x + (n+1)\frac{x^n(x-1)^n}{n!}e^x + (x-1)\frac{x^n(x-1)^n}{n!}e^x \\ &= \frac{x^{n+1}(x-1)^n}{n!}e^x + 2n\frac{x^n(x-1)^n}{n!}e^x - \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x \end{aligned}$$

(2.6) följer när vi integrerar båda ledena från 0 till 1.

Vi ska nu visa lemmat med hjälp av induktion. När $n = 0$, får vi att

$$\begin{aligned} A_0 &= \int_0^1 e^x \,\mathrm{d}x = e - 1 = p_0 e - q_0 \\ B_0 &= 1 = p_1 - q_1 e \\ C_0 &= 2 - e = p_2 - q_2 e \end{aligned}$$

Alltså gäller induktionsbasen. Antag att lemmat gäller för något $n \geq 0$. Då får vi, med hjälp av formler (2.4), (2.5) och (2.6) samt rekursionsrelationerna som vi gav för p_n och q_n, att

$$\begin{aligned} A_{n+1} &= -B_n - C_n = -p_{3n-1} + q_{3n-1}e - p_{3n-2} + q_{3n-2}e = \\ &= q_{3(n+1)}e - p_{3(n+1)} \end{aligned}$$

På analogt sätt får vi att

$$\begin{aligned} B_{n+1} &= p_{3(n+1)+1} - q_{3(n+1)+1}e \\ C_{n+1} &= p_{3(n+1)+2} - q_{3(n+1)+2}e \end{aligned}$$

Alltså gäller formlerna för alla $n \geq 0$. Beviset är därmed klart. ■

Med hjälp av detta lemma kan vi visa att e är irrationellt:

Bevis av kedjebråksutvecklingen (2.3) För talen p_n och q_n i lemma 2.2.2 gäller att

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n] \qquad \text{för } n = 2, 3, \ldots$$

där $a_{3i+1} = 2i$ och $a_{3i} = a_{3i+2} = 1$, för $i = 0, 1, 2, \ldots$. Integranderna i de integraler som definierar A_n, B_n och C_n har alla absolutbelopp som är mindre än eller lika med $1/n!$ för godtyckligt $x \in [0, 1]$ och för godtyckligt $n \geq 0$, och alltså går A_n, B_n och C_n mot 0 då n går mot oändlighet. Lemma 2.2.2 och att $q_n > 0$ för alla $n \geq 2$ visar sedan att p_{3n}/q_{3n}, p_{3n+1}/q_{3n+1} och p_{3n+2}/q_{3n2} alla går mot e då $n \to \infty$. Det följer att

$$e = \lim_{n\to\infty} \frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots] = [1; 0, 1, 1, 2, 1, 1, 4, ...]$$

och vi har därmed bevisat att kedjebråksutvecklingen (2.3) gäller för talet e. ■

Fourier 1815

Joseph Fouriers (1768-1830) eleganta metod att visa irrationalitet hos e är förmodligen den mest kända, och också den enklaste. Den är ett kompakt motsägelsebevis som utnyttjar definitionen av e som en oändlig serie:

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} \tag{2.7}$$

Beviset publicerades för första gången i [4], och kan hittas i de flesta böcker som hanterar ämnet.

Bevis av sats 2.2.1 Antag att e är rationellt. Då existerar det positiva heltal p och q sådant att $e = p/q$. Betrakta delsumman

$$s_q = \sum_{n=0}^{q} \frac{1}{n!}$$

Eftersom varje term i (2.7) är positiv, är även

$$\frac{p}{q} - s_q \tag{2.8}$$

positiv. Om vi multiplicerar (2.8) med $q!$, så får vi ett positivt heltal. Vidare har vi att

$$\begin{aligned}0 < q!\left(\frac{p}{q} - \sum_{n=0}^{q}\frac{1}{n!}\right) = q!\left(e - \sum_{n=0}^{q}\frac{1}{n!}\right) = q!\left(\sum_{n=0}^{\infty}\frac{1}{n!} - \sum_{n=0}^{q}\frac{1}{n!}\right) = \\ = q!\left(\frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \frac{1}{(q+3)!} + ...\right) = \\ = \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} + \cdots\end{aligned}$$

Men eftersom $q > 0$ (eller ekvivalent $q \geq 1$), så får vi att

$$\frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} + ... < \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + ... = 1$$

Vi försöker alltså hitta ett heltal mellan 0 och 1, vilket inte är möjligt. Vi har således kommit fram till en motsägelse, vilket innebär att vårt antagande att e är rationellt var felaktigt. ■

2.3 Irrationalitet hos π

Även om π har varit känt i flera tusen år, var det inte förrän på 1700-talet man lyckades bevisa att det är irrationellt. Detta beror på att π:s definition som förhållandet mellan en cirkels omkrets och diameter är svårutnyttjad när man ska formulera rigorösa matematiska bevis. Man behöver andra verktyg, som till exempel trigonometriska samband, för att åtgärda problemet. I detta avsnitt kommer vi att titta närmare på några bevis av nästa kända sats.

Sats 2.3.1. *π är irrationellt.*

Laczkovich 1997

Den förste som lyckades visa att π är irrationellt var Johann Heinrich Lambert (1728-1777) år 1761 i [10]. Precis som Euler använde han kedjebråk, och började med att visa att följande likhet gäller:

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \ddots}}}}$$

Efter det visade Lambert att om $x \neq 0$ är rationellt, då måste uttrycket ovan vara irrationellt. Det följer då direkt av sambandet $\tan(\frac{\pi}{4}) = 1$ att π är irrationellt. Lamberts bevis är väldigt komplicerat, och saknar viss exakthet. Ett enklare bevis av detta publicerades 1997 av Miklós Laczcovich i [9], och vi redogör nu för detta bevis.

Ofta använder man sekvenser av positiva heltal för att få fram motsägelser. Laczkovich använder en liknande idé, fast istället för heltal behandlar han heltalsmultipler. Mängden av heltalsmultipler av ett reellt tal y definieras som

$$y\mathbb{Z} = \{x \in \mathbb{R} \mid x = ay, a \in \mathbb{Z}\}$$

Sekvenser av heltal skilda från 0 kan inte konvergera mot 0, och det är klart att detta gäller även för sekvenser av $y\mathbb{Z}$ så fort y är skilt från 0.

Betrakta följande sekvens av funktioner:

$$\begin{aligned} f_k(x) &= 1 - \frac{x^2}{k} + \frac{x^4}{2!k(k+1)} - \frac{x^6}{3!k(k+1)(k+2)} + \cdots \\ &= 1 + \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{n!k(k+1)\cdots(k+n-1)} \end{aligned}$$

där $k \in \mathbb{Q}/\{0, -1, -2, ...\}$. Dessa funktioner är definierade för alla $x \in \mathbb{R}$, och dessutom har vi att

$$\begin{aligned} f_{1/2}(x) &= 1 - \frac{2^2x^2}{2!} + \frac{2^4x^4}{4!} - \frac{2^6x^6}{6!} + \cdots \\ &= \cos(2x) \end{aligned}$$

och på motsvarande sätt

$$f_{3/2}(x) = \frac{\sin(2x)}{2x}$$

Innan vi kan börja med själva beviset behöver vi några hjälpsatser.

Lemma 2.3.2. *Följande relation gäller för alla $x \in \mathbb{R}$:*

$$\frac{x^2}{k(k+1)} f_{k+2}(x) = f_{k+1}(x) - f_k(x)$$

Bevis Från definitionen av $f_k(x)$ får vi att

$$\begin{aligned} f_{k+1}(x) - f_k(x) &= 1 + \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{n!(k+1)(k+2)\cdots(k+n)} - 1 - \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{n!k(k+1)\cdots(k+n-1)} = \\ &= \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{n!(k+1)(k+2)\cdots(k+n-1)} \left(\frac{1}{k+n} - \frac{1}{k} \right) \\ &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^{2n}}{n!(k+1)(k+2)\cdots(k+n-1)} \frac{n}{k(k+n)} \\ &= \frac{x^2}{k(k+1)} + \sum_{n=2}^{\infty} \frac{(-1)^{n+1} x^{2n}}{(n-1)!k(k+1)\cdots(k+n)} \\ &= \frac{x^2}{k(k+1)} \left(1 + \sum_{n=1}^{\infty} \frac{(-1)^n x^{2n}}{n!(k+2)\cdots(k+n+1)} \right) \\ &= \frac{x^2}{k(k+1)} f_{k+2}(x) \quad \blacksquare \end{aligned}$$

Lemma 2.3.3. *För varje x har vi att*

$$\lim_{k \to +\infty} f_k(x) = 1$$

Bevis Fixera ett godtyckligt x. Vi har att $\lim_{n\to\infty} x^{2n}/n! = 0$, vilket innebär att $x^{2n}/n!$ är begränsat för varje $n \in \mathbb{Z}_+$. Låt $M = \sup_{n\in\mathbb{Z}_+} x^{2n}/n!$. Då är alltså M ett ändligt tal. Om $k > 1$ har vi då att

$$|f_k(x) - 1| \leq \sum_{n=1}^{\infty} \frac{M}{k^n} = M \frac{1/k}{1 - 1/k} = \frac{M}{k-1}$$

Resultatet följer när vi låter k gå mot oändligheten. $\blacksquare$

Lemma 2.3.4. *Om $x \neq 0$ och om x^2 är rationellt, då är*

$$f_k(x) \neq 0 \text{ och } \frac{f_{k+1}(x)}{f_k(x)} \notin \mathbb{Q}$$

Bevis Låt $x \neq 0$ vara ett reellt tal vars kvadrat är rationell, och låt $k \in \mathbb{Q}/\{0, -1, -2, ...\}$ vara givet. Antag nu, för att få en motsägelse, att antigen $f_k(x) = 0$ eller $f_{k+1}(x)/f_k(x) \in \mathbb{Q}$.

Vi börjar med att visa att det existerar ett reellt tal $y \neq 0$ sådant att $f_k(x)$ och $f_{k+1}(x)$ tillhör $y\mathbb{Z}$. Detta görs genom att hitta heltal a och b sådana att $f_k(x) = ay$ och $f_{k+1}(x) = by$. Om $f_k(x) = 0$, kan vi helt enkelt välja $y = f_{k+1}(x), a = 0$ och $b = 1$. Om $f_{k+1}(x)/f_k(x) \in \mathbb{Q}$, kan vi välja heltal a och b sådana att

$$\frac{f_{k+1}(x)}{f_k(x)} = \frac{b}{a}$$

och definiera

$$y = \frac{f_k(x)}{a} = \frac{f_{k+1}(x)}{b}$$

y kan inte vara 0, ty annars skulle det följa av rekursionsrelationen i lemma 2.3.2 att varje $f_{k+n}(x)$ för $n \in \mathbb{Z}$ skulle vara 0, vilket strider mot lemma 2.3.3. Välj nu ett heltal q sådant att

$$\frac{bq}{k}, \frac{qk}{x^2}, \frac{q}{x^2} \in \mathbb{Z} \tag{2.9}$$

Definiera $g_0 = f_k(x)$ och

$$g_n(x) = \frac{q^n}{k(k+1)...(k+n-1)} f_{k+n}(x) \quad (n = 1, 2, 3, \dots)$$

Nästa steg är att visa att $g_n \in y\mathbb{Z}$ för varje n. Vi har att

$$g_0(x) = f_k(x) = ay \in y\mathbb{Z}$$
$$g_1(x) = \frac{q}{k} f_{k+1}(x) = \frac{bq}{k} y \in y\mathbb{Z}$$

Om $n \geq 2$ då får vi med hjälp av lemma 2.3.2 att

$$\begin{aligned}
g_{n+2}(x) &= \frac{q^{n+2}}{k(k+1)...(k+n+1)} f_{k+n+2}(x) \cdot \frac{x^2(k+n)(k+n+1)}{x^2(k+n)(k+n+1)} \\
&= \frac{q^{n+2}}{x^2 k(k+1)...(k+n-1)} f_{k+n+1}(x) - \frac{q^{n+2}}{x^2 k(k+1)...(k+n-1)} f_{k+n}(x) \\
&= \frac{q(k+n)}{x^2} g_{n+1} - \frac{q^2}{x^2} g_n = \left(\frac{qk}{x^2} + \frac{q}{x^2} n \right) g_{n+1} - \frac{q^2}{x^2} g_n \in y\mathbb{Z}
\end{aligned}$$

Av (2.9) följer att $g_n(x) \in y\mathbb{Z}$ för varje n. När n växer obegränsad, vet vi att $f_{k+n}(x) \to 1$ (lemma 2.3.3), och att $q^n/k(k+1)...(k+n-1) \to 0$. Av dessa följer att g_n konvergerar mot 0 när $n \to \infty$. Å andra sidan är $g_n > 0$ (lemma 2.3.3). Men en sekvens av heltalsmultipler av y kan inte konvergera mot 0. ■

Med dessa resultat är vi färdiga att ge ett bevis för sats 2.3.1:

Bevis av sats 2.3.1 Eftersom vi har

$$f_{1/2}\left(\frac{\pi}{4}\right) = \cos\frac{\pi}{2} = 0$$

följer det direkt av lemma 2.3.4 att $\pi^2/16$ är irrationellt, vilket medför att även π är irrationellt. ■

Med Lemma 2.3.4 kan man också visa att om $x \neq 0$ är rationellt, då är $\tan x$ irrationellt. Ty om x är rationellt, då är även $(x/2)^2$ rationellt, och

$$\frac{f_{3/2}(x/2)}{f_{1/2}(x/2)} = \frac{\tan x}{x}$$

är ett irrationellt tal, vilket medför att $\tan x$ är irrationellt.

Niven 1956

Charles Hermite (1822-1901) visade att π är irrationellt som biprodukt av sitt arbete inom transcendens. Hermite noterade att vissa integraler blir omöjliga om π vore ett rationellt tal. Ivan Niven ger ett liknande bevis i [12], och det är det som vi kommer att presentera här.

Bevis av Sats 2.3.1 Antag att π är rationellt. Då existerar det positiva heltal p och q sådana att $\pi = p/q$. Låt oss nu med hjälp av dessa tal definiera polynomet

$$f(x) = \frac{x^n(p-qx)^n}{n!} \tag{2.10}$$

där n är ett positivt heltal som bestäms senare. Konstruera ett till polynom genom att använda jämna derivator till f:

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x) = \sum_{j=0}^{n} (-1)^j f^{(2j)}(x)$$

Niven visar att

$$\int_0^\pi f(x)\sin x \,\mathrm{d}x = F(0) + F(\pi) \tag{2.11}$$

är ett heltal. Precis som i Fouriers bevis leder detta till att försöka hitta heltal mellan 0 och 1. Låt oss nu övertygas att (2.11) gäller. Kedjeregeln ger att

$$\frac{d}{dx}\left(F'(x)\sin x - F(x)\cos x\right) = F''(x)\sin x + F(x)\sin x = f(x)\sin x$$

Den sista likheten följer av definitionen av F och av att $f^{(2n+2)}(x) = 0$. Vi får att

$$\int_0^\pi f(x)\sin x\,\mathrm{d}x = |F'(x)\sin x - F(x)\cos x|_0^\pi = F(\pi)\cdot 1 - F(\pi)\cdot 0 - F'(0)\cdot 0 + F(0)\cdot 1 =$$
$$= F(0) + F(\pi)$$

Nästa steg är att visa att $F(0) + F(\pi)$ är ett heltal. Det framgår tydligt av (2.10) att $f(x)$ är ett polynom vars termer är lägst av grad n. Vi kan skriva om det som

$$f(x) = \frac{c_n x^n + c_{n+1}x^{n+1} + \cdots + c_{2n}x^{2n}}{n!}$$

där c_k, $n \leq k \leq 2n$, alla är heltal. Om vi deriverar detta k gånger, där $k < n$, följer att $f^{(k)}(0) = 0$. Om $n \leq k \leq 2n$, har vi att

$$f^{(k)}(x) = \sum_{j=k}^{d} \frac{j!c_j x^{j-k}}{(j-k)!n!}$$

vilket ger

$$f^{(k)}(0) = \frac{k!c_k}{n!} = k(k-1)\cdots(n+1)c_k \in \mathbb{Z}$$

Alltså är $F(0)$ ett heltal. Vidare har vi att

$$f(\pi - x) = f\left(\frac{p}{q} - x\right) = f(x)$$

och $(-1)^k f^{(k)}(\pi) = f^{(k)}(0)$. Därför är även $F(\pi)$ ett heltal. Av (2.10) följer att för $0 \leq x \leq \pi = p/q$:

$$0 < f(x)\sin x \leq \frac{\pi^n p^n}{n!}$$

Väljer vi n på ett lämpligt sätt så ligger därför vänsterledet i (2.11) mellan 0 och 1, vilket ger oss en motsägelse. ■

3 Transcendens

3.1 Rationella approximationer av transcendenta tal

År 1844 publicerade Joseph Liouville (1809-1883) en artikel [11] som visade existensen av transcendenta tal. Eftersom transcendens definieras i termer av att de *inte* har en egenskap, så är det svårt att komma åt villkor som alla transcendenta tal måste uppfylla. Liouville angrep problemet genom att hitta en egenskap som alla algebraiska tal måste uppfylla, och från det konstruerade han en klass av transcendenta tal. I detta avsnitt redogör vi för Liouvilles teorem och Liouvilles konstant.

Sats 3.1.1 (Liouvilles teorem)**.** *Låt α vara ett algebraiskt irrationellt reellt tal som är nollställe till ett irreducibelt polynom i $\mathbb{Z}[x]$ med grad n. Då existerar ett reellt tal $c(\alpha) > 0$, som endast beror av α, sådant att för varje rationellt tal p/q, där $q \geq 1$, gäller*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n} \tag{3.1}$$

Bevis Låt α vara ett irrationellt tal som är rot till det irreducibla polynomet

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$$

Låt p och $q \geq 1$ vara heltal. Om $|\alpha - p/q| > 1$, får vi direkt att

$$\left|\alpha - \frac{p}{q}\right| > 1 \geq \frac{1}{q^n} \tag{3.2}$$

Antag nu att $|\alpha - p/q| \leq 1$. Eftersom $f(x)$ är irreducibelt i $\mathbb{Z}$ så följer det av sats 1.2.2 att $f(p/q) \neq 0$. Då är $q^n f(p/q)$ ett heltal skilt från 0, och

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}$$

Av medelvärdessatsen följer det att det existerar ett reellt tal ξ mellan a och p/q sådant att

$$\left(\alpha - \frac{p}{q}\right) f'(\xi) = f(\alpha) - f\left(\frac{p}{q}\right) = -f\left(\frac{p}{q}\right)$$

vilket ger att

$$\frac{1}{q^n} \leq \left|f\left(\frac{p}{q}\right)\right| \leq |f'(\xi)| \left|\alpha - \frac{p}{q}\right| + |f(\alpha)| \leq |f'(\xi)| \left|\alpha - \frac{p}{q}\right| \tag{3.3}$$

Låt $M = \max |f(x)|$ på intervallet $[\alpha - 1, \alpha + 1]$. Vi vet att ξ ligger på detta intervall eftersom $|\alpha - p/q| \leq 1$ och ξ ligger mellan α och p/q. Det största värdet existerar eftersom $f'(x)$ är kontinuerlig och intervallet ifråga är kompakt. Av (3.3) får vi att

$$\frac{M^{-1}}{q^n} \leq \left|\alpha - \frac{p}{q}\right|$$

Satsen följer nu genom att kombinera ovanstående ekvation med (3.2), det vill säga genom att sätta $c(\alpha) = \min(1, M^{-1})$. ■

Tal som inte uppfyller Liouvilles teorem har ett speciellt namn: Liouvilletal. Ett reellt tal β är ett Liouvilletal om det för varje naturligt tal n finns $p > 0$ och $q > 1$ sådana att

$$0 < \left|\beta - \frac{p}{q}\right| < \frac{1}{q^n} \tag{3.4}$$

Följande sats är en naturlig konsekvens av Liouvilles teorem.

Sats 3.1.2. *Liouvilletal är transcendenta.*

Bevis Låt β vara ett Liouvilletal. Innan sats 3.1.1 kan användas måste vi visa att β är irrationellt. Antag att vi kan skriva $\beta = a/b$, och välj n sådant att $2^{n-1} > b$. Då har vi att för alla heltal $p > 0$ och $q > 1$ att

$$\left|\beta - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| \geq \frac{1}{bq} > \frac{1}{2^{n-1}q} \geq \frac{1}{q^n}$$

Denna olikhet strider mot (3.4), vilket medför att β omöjligen kan vara rationellt.

Om nu β vore algebraiskt, då skulle det följa av sats 3.1.1 att det finns ett reellt tal $c(\beta)$ sådant att för alla rationella tal p/q, $q \geq 1$ så gäller

$$\left|\beta - \frac{p}{q}\right| > \frac{c(\beta)}{q^n} \tag{3.5}$$

där n är graden till ett irreducibelt polynom som har β som rot. Välj ett heltal m sådant att $1/2^m < c(\beta)$ och sätt $k = m + n$. Eftersom β är ett Liouvilletal finns det heltal $p > 0$ och $q > 1$ sådana att

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{q^k} = \frac{1}{q^m q^n} \leq \frac{1}{2^m q^n} < \frac{c(\beta)}{q^n}$$

Men detta strider mot (3.5). Alltså är β transcendent. ■

Vi har visat att alla Liovilletal är transcendenta – motsatsen gäller dock inte. Till exempel är varken e eller π ett Liouvilletal. Det första talet som visades vara transcendent, och som avgjorde existensen av transcendenta tal ges i nästa sats.

Sats 3.1.3 (Liouvilles konstant)**.** *Talet*

$$\mathscr{L} = \sum_{k=1}^{\infty} 10^{-k!} = 0.1100010000...$$

är transcendent.

Bevis Vi visar att $\mathscr{L}$ är ett Liouvilletal. Låt n vara ett godtyckligt naturligt tal, och definiera heltalsföljder $\{p_n\}$ och $\{q_n\}$ genom att sätta

$$p_n = 10^{n!} \sum_{k=1}^{n} 10^{-k!}$$
$$q_n = 10^{n!}$$

Då har vi att

$$\left|\mathscr{L} - \frac{p_n}{q_n}\right| = \sum_{k=1}^{\infty} 10^{-k!} - \sum_{k=1}^{n} 10^{-k!} = 10^{-(n+1)!} + 10^{-(n+2)!} + 10^{-(n+3)!} + \cdots$$

Eftersom $(n+1+m)! \geq (n+1)! + m$ för alla positiva heltal m, så får vi att

$$10^{-(n+1)!} + 10^{-(n+2)!} + \cdots \leq 10^{-(n+1)!} + 10^{-(n+1)!-1} + 10^{-(n+1)!-2} + \cdots = \sum_{k=(n+1)!}^{\infty} 10^{-k}$$

Den sista termen är en geometrisk serie, och således lika med

$$\frac{10^{-(n+1)!}}{1-10^{-1}} = \frac{10}{9} 10^{-(n+1)!}$$

Lite omskrivningar ger oss att

$$\frac{10}{9} 10^{-(n+1)!} < 10 \cdot 10^{-(n+1)!} = \frac{10}{(10^{n!})^{n+1}} \leq \frac{1}{(q_n)^n}$$

Tillsammans ger ovanstående att $|\mathscr{L} - p_n/q_n| < 1/(q_n)^n$ för $n = 1, 2, \ldots$. Alltså är $\mathscr{L}$ ett Liouvilletal, och därmed transcendent. ■

Liouvilles konstant var det första talet vars transcendens styrktes. Tyvärr slutar dess intressanta egenskaper där. Liouville försökte naturligtvis tillämpa sin teori för att se om mer användbara tal såsom e var transcendenta. Han visade att e inte är en rot till ett andragradspolynom, men lyckades aldrig generalisera detta resultat till högre grader.

3.2 Transcendens hos e

Detta avsnitt ägnas åt följande sats:

Sats 3.2.1. *e är transcendent.*

Charles Hermite publicerade sitt bevis för transcendens hos e i *Sur la fonction exponentielle* år 1873. Som vi nämde e förut, gav han även ett enkelt bevis för att π är irrationellt i samma publikation.

Hurwitz 1893

Adolf Hurwitz (1859-1919) förenklade Hermites bevis för att e är transcendent i [8]. Hans bevis baserar sig på det faktum att för varje polynom $f(x)$ med grad d, så uppfyller

$$F(x) = f'(x) + f''(x) + \cdots + f^{(d)}(x) = \sum_{i=0}^{d} f^{(i)}(x)$$

att

$$\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}f(x) \tag{3.6}$$

Detta följer av att

$$\begin{aligned} F'(x) &= f'(x) + f^{(2)}(x) + \cdots + f^{(d)}(x) \\ &= F(x) - f(x) \end{aligned}$$

vilket medför att

$$\begin{aligned} \frac{d}{dx}(e^{-x}F(x)) &= -e^{-x}F(x) + e^{-x}F'(x) \\ &= -e^{-x}F(x) + e^{-x}(F(x) - f(x)) \\ &= -e^{-x}f(x) \end{aligned}$$

Alltså gäller (3.6). Tillsammans med medelvärdessatsen ger det att

$$e^{-x}F(x) - F(0) = -xe^{-\xi x}f(\xi x)$$

eller

$$F(x) - e^{x}F(0) = -xe^{x(1-\xi)}f(\xi x)$$

för något tal ξ mellan 0 och 1. Med detta är vi nu färdiga att presentera Hurwitz bevis.

Bevis av sats 3.2.1 Antag att e är algebraiskt. Då existerar det ett polynom $q(x)$ med heltalskoefficienter sådant att

$$q(e) = a_n e^n + a_{n-1}e^{n-1} + ... + a_1 e + a_0 = 0$$

där $a_i \in \mathbb{Z}, i = 1, ..., n$. Vi kan anta att a_0 är ett positivt heltal, ty om $a_0 = 0$, då kunde vi dela $q(x)$ med x, och få ett nytt polynom som har e som rot. Å andra sidan om $a_0 < 0$, kunde vi multiplicera $q(x)$ med -1. Betrakta nu polynomet

$$f(x) = \frac{x^{p-1}}{(p-1)!}(x-1)^p(x-2)^p \cdots (x-n)^p \tag{3.7}$$

där p är ett primtal större än a_0 och n. Definiera $F(x)$ från $f(x)$ som ovan. Sätt

$$\epsilon_k = -ke^{k(1-\xi)}\frac{(\xi k)^p(1-\xi k)^{p-1}\cdots(n-\xi k)^{p-1}}{(p-1)!}$$

för $k = 1, ..., n$. Då gäller att

$$\begin{aligned} F(1) - eF(0) &= \epsilon_1 \\ F(2) - e^2F(0) &= \epsilon_2 \\ &\vdots \\ F(n) - e^nF(0) &= \epsilon_n \end{aligned}$$

Av definitionen av $F(x)$ ser man att $F(1), ..., F(n)$ är heltal delbara med p, medan $F(0)$ är ett heltal inte delbart med p. Vi får att

$$\begin{aligned} a_1F(1) + a_2F(2) + \cdots + a_nF(n) + a_0F(0) &= a_1\epsilon_1 + \cdots + a_n\epsilon_n + F(0)\sum_{k=0}^{\infty} a_k e^k \\ &= a_1\epsilon_1 + \cdots + a_n\epsilon_n \end{aligned}$$

När vi låter p växa, går ϵ_k mot noll för $k = 1, \ldots, n$. Då går även $c_1\epsilon_1 + \cdots + c_n\epsilon_n$ mot noll. Men $a_1F(1) + a_2F(2) + \cdots + a_nF(n) + a_0F(0)$ är ett heltal skilt från 0 eftersom det inte är delbart med p. En följd av heltal skilda från 0 kan inte konvergera mot 0, vilket ger oss en motsägelse. Alltså är e transcendent. ■

Här har vi presenterat bara ett sätt att visa att e är transcendent, vilket beror på att transcendensbevisen för e och π är så lika. Genom att göra några enkla modifikationer av bevisen i nästa avsnitt kan man visa att även e är transcendent.

3.3 Transcendens hos π

Huruvida π är transcendent bekymrade matematiker i flera tusen år, dock var problemställningen lite annorlunda: är cirkeln kvadrerbar? Ferdinand von Lindemanns (1852-1939) artikel [16] från 1882 gav ett negativt svar på frågan.

Sats 3.3.1. *π är transcendent.*

Hilbert 1893

David Hilberts (1862-1943) bevis är relativt enkelt, och är väl det som används mest flitigt. Detta bevis publicerades först i [7].

Bevis av sats 3.3.1 Antag att π är algebraiskt. Då är även $i\pi$ algebraiskt, vilket innebär att det existerar ett polynom $q(x)$ i $\mathbb{Z}[x]$ med rötterna $x_1 = i\pi$ samt $x_2, \ldots, x_n \in \mathbb{C}$. Graden för $q(x)$ måste vara större än 1 eftersom $i\pi$ inte är rationellt. Av sambandet $e^{i\pi} + 1 = 0$ följer att

$$\prod_{i=1}^{n} (e^{x_i} + 1) = (e^{x_1} + 1) \cdots (e^{x_n} + 1) = 0 \tag{3.8}$$

Vi kan utveckla ovanstående produkt, och får en summa av 2^n stycken exponentialfunktioner, vars exponenter är av formen

$$\begin{aligned}
&x_1, x_2, \ldots \\
&x_1 + x_2, x_1 + x_3, \ldots \\
&x_1 + x_2 + x_3, x_1 + x_2 + x_3, \ldots \\
&\quad \vdots \\
&x_1 + x_2 + \cdots + x_n
\end{aligned}$$

Låt c vara antalet sådana exponenter lika med 0, och låt $a_1, \ldots, a_m$ beteckna de återstående exponenterna. Då kan (3.8) skrivas som

$$\sum_{i=1}^{m} e^{a_i} + c \cdot e^0 = \sum_{i=1}^{m} e^{a_i} + c = 0 \tag{3.9}$$

där c är ett positivt heltal. En funktion av formen

$$\phi(x) = (x - a_1)(x - a_2) \cdots (x - a_m)$$

tillhör $\mathbb{Q}[x]$, eftersom ϕ är symmetriskt med avseende på $x_1, \ldots, x_n$ (se beviset av följdsats (1.2.6)). Därför finns det ett heltal $b \neq 0$ sådant att

$$f(x) = b\phi(x) = b_m x^m + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$$

där $b_0, b_m \neq 0$. $f(x)$ har samma rötter som $\phi(x)$, det vill säga $a_1, \ldots, a_m$. Betrakta integralen

$$\int_0^\infty = \int_0^\infty z^p g(z)^{p+1} e^{-z} \, \mathrm{d}z$$

där p är ett postitivt heltal som väljs senare, och $g(z) = b_m^m f(z)$. Multiplicerar vi (3.9) med detta får vi att

$$e^{a_1} \int_0^\infty + \cdots + e^{a_m} \int_0^\infty + c \int_0^\infty = 0 \tag{3.10}$$

Detta kan skrivas som $P_1 + P_2 = 0$, där

$$P_1 = e^{a_1}\int_{a_1}^{\infty} + \cdots + e^{a_m}\int_{a_m}^{\infty} + c\int_0^{\infty}$$
$$P_2 = e^{a_1}\int_0^{a_1} + \cdots + e^{a_m}\int_0^{a_m}$$

Division av (3.10) med $p!$ ger att

$$\frac{P_1}{p!} + \frac{P_2}{p!} = 0 \tag{3.11}$$

Vi ska nu visa att denna ekvation är omöjlig, eftersom $\frac{P_1}{p!}$ är ett heltal skilt från 0, och $\frac{P_2}{p!}$ ligger på intervallet $(-1, 1)$.

Om j är ett positivt heltal, så får vi med partialintegration att

$$\int_0^{\infty} z^j e^{-z}\,\mathrm{d}z = j!$$

Utvecklar man $z^p g(z)^{p+1}$ får man en summa av termer med formen $d_i z^{p+i}$, $i = 0, \ldots, mp+m+p$, där talen d_i alla är heltal. Med detta är det lätt att se att $\int_0^{\infty}$ är ett heltal delbart med $p!$. Vidare har vi att

$$\begin{aligned}\frac{1}{p!}\int_0^{\infty} &= \frac{b_m^{mp+m}}{p!}\int_0^{\infty}\sum_{i=0}^{mp+m+p} d_i z^{p+i}e^{-z}\,\mathrm{d}z = \frac{b_m^{mp+m}}{p!}\sum_{i=0}^{mp+m+p} d_i(p+i)! \\ &= b_m^{mp+m}d_0 + b_m^{mp+m}\sum_{i=0}^{mp+m+p} d_i(p+1)\cdots(p+i)\end{aligned}$$

Det är klart att $d_0 = b_0^{p+1}$, vilket ger oss kongruensen

$$\frac{1}{p!}\int_0^{\infty} \equiv b_m^{mp+m}b_0^{p+1} \mod (p+1) \tag{3.12}$$

Med substitutionen $y = z + a_i$ får vi att

$$e^{a_i}\int_{a_i}^{\infty} = \int_0^{\infty}(y+a_i)^p g(y+a_i)^{p+1}e^{-y}\,\mathrm{d}y = (p+1)!G(b_m a_i) \tag{3.13}$$

där $G(b_m a_i)$ är ett polynom med heltalskoefficienter, som beror endast av $b_m a_i$. Att detta gäller kan ses genom att partialintegrera (3.13) successivt. Vi får då ett uttryck av formen

$$\sum_{k=1}^{d}\left[-h^{(k)}(y)e^{-y}\right]_0^{\infty} + \int_0^{\infty} h^{(d)}(y)e^{-y}\,\mathrm{d}y$$

där $h(y) = (y+a_i)^p g(y+a_i)^{p+1}$ och $d = \mathrm{grad}(h(y))$. Eftersom $g(a_i) = 0$, måste vi ha deriverat bort $g(y+a_i)$ innan vi får termer skilda från 0. Det som återstår är då kombinationer av derivator till $(y+a_i)^p$ och till $g(y+a_i)$. När vi sätter $y = 0$ så får får vi en summa av polynom av a_i med heltalskoefficienter. Vart och ett av dessa polynom har graden mindre än $pm+m$, och är delbara med b_m^{pm+m}. Alltså gäller (3.13).

Eftersom $G(b_m a_i)$ är ett polynom med heltalskoefficienter, och $b_m a_i$ är ett algebraiskt heltal för varje i (se sats 1.2.3), får vi av följdsats 1.2.6 att polynomet

$$G(b_m a_1) + \cdots + G(b_m a_m)$$

som är symmetriskt med avseende på $b_m a_1, \ldots, b_m a_m$ är ett heltal. Ekvation (3.13) medför att P_1 ett heltal delbart med $p!$. Vidare följer det av (3.12) och (3.13) att

$$\frac{P_1}{p!} \equiv \frac{e^{a_1}}{p!} \int_{a_1}^{\infty} + \cdots + \frac{e^{a_m}}{p!} \int_{a_m}^{\infty} + \frac{c}{p!} \int_{0}^{\infty} \equiv c b_m^{mp+m} b_0^{p+1} \mod (p+1) \tag{3.14}$$

Om vi sätter

$$K = \sup_{z \in (0, a_i)} |z g(z)| \text{ och } k = \sup_{z \in (0, a_i)} \left| g(z) e^{-z} \right|$$

så får vi att

$$\left| \int_0^{a_i} \right| = \left| \int_0^{a_i} z^p g(z)^{p+1} e^{-z} \, \mathrm{d}z \right| < |a_i| k K^p$$

Om vi använder förkortningen

$$\sigma = (|a_1 e^{a_1}| + |a_2 e^{a_2}| + \cdots + |a_m e^{a_m}|) k$$

så får vi att

$$|P_2| < \sigma K^p \tag{3.15}$$

Låt oss nu välja p så att p är delbart med $c b_m^{mp+m} b_0^{p+1}$ och

$$\sigma \frac{K^p}{p!} < 1$$

Det följer av kongruensen i (3.14) att $P_1/p!$ inte är delbart $p+1$, och därför är ett tal skilt från 0. Av (3.15) följer att $P_2/p!$ är mellan -1 och 1, vilket ger att (3.11) inte kan vara sant. Vi har fått en motsägelse, alltså måste π vara transcendent. ■

Gordan 1893

Paul Gordan (1837-1912) visade att e och π är transcendenta i [6]. Vi ska bara gå igenom det senare fallet eftersom bevisen är nästan identiska.

Bevis av sats 3.3.1 På samma sätt som i Hilberts bevis börjar vi med att anta att π är algebraiskt. Då existerar det ett polynom

$$b(x - x_1) \cdots (x - x_n) = b_m x^m + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$$

vars rötter är lika med $x_1 = i\pi$ och $x_2, \ldots, x_n \in \mathbb{C}$. Vi har då $b \in \mathbb{Z}$. Sambandet $e^{i\pi} = -1$ ger oss då att

$$\prod_{i=1}^{n} (e^{x_i} + 1) = \sum_{i=1}^{m} e^{a_i} + c = 0 \tag{3.16}$$

där $a_1, \ldots, a_m$ är algebraiska tal skilda från 0, och c ett positivt heltal. Symmetriska polynom av bx_i, och därmed även ba_i, är heltal (se följdsats 1.2.6). Betrakta Taylorutvecklingen

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \tag{3.17}$$

och låt

$$f(x) = c_d x^d + \cdots + c_1 x + c_0$$

vara en funktion i $\mathbb{Q}[x]$ med grad d. Om vi inför beteckningarna

$$r! = h^r \quad \text{och} \quad u_r = \frac{x}{r+1} + \frac{x^2}{(r+1)(r+2)} + \cdots$$

så får vi, genom att multiplicera (3.17) med $c_r h^r$, där $0 \leq r \leq d$, att

$$c_r h^r e^x = c_r (x+h)^r + c_r x^r u_r \tag{3.18}$$

Detta följer av att

$$c_r \sum_{k=0}^{r} \frac{h^r x^k}{k!} = c_r \sum_{k=0}^{r} \frac{r! x^k (r-k)!}{k!(r-k)!} = c_r \sum_{k=0}^{r} \binom{r}{k} h^{r-k} x^k = c_r (x+h)^r$$

enligt binomialsatsen, och att

$$c_r \sum_{k=r+1}^{\infty} \frac{h^r x^k}{k!} = c_r x^r \sum_{k=1}^{\infty} \frac{r! x^k}{(r+k)!} = c_r x^r u_r$$

Av Taylorutvecklingen för e^x följer att

$$|u_r| < e^{|x|}$$

och om vi sätter $u_r = q_r e^{|x|}$, så är $|q_r| < 1$. Vi kan då skriva (3.18) i formen

$$c_r h^r e^x = c_r (x+h)^r + c_r x^r q_r e^{|x|}$$

Summering över r ger att

$$e^x \sum_{r=0}^{d} c_r h^r = \sum_{r=0}^{d} c_r (x+h)^r + e^{|x|} \sum_{r=0}^{d} c_r x^r q_r$$

Genom att sätta $\phi(x) = \sum_{r=0}^{d} c_r x^r q_r$ kan detta skrivas mer kompakt som

$$e^x f(h) = f(x+h) + e^{|x|} \phi(x) \tag{3.19}$$

Denna ekvation är nyckeln till Gordans bevis. Låt oss nu definiera följande funktion (notera likheten med (3.7))

$$f(x) = \frac{x^{p-1}}{(p-1)!} b^{mp+p-1} (x-a_1)^p (x-a_2)^p \cdots (x-a_m)^p \tag{3.20}$$

där p är ett primtal som är större än c, n, b, $a_1, a_2, \ldots, a_n$. Om vi sätter $x = a_i$ i (3.19) och summerar över i, så får vi att (kom ihåg att $\sum_i e^{a_i} = -c$):

$$-cf(h) = \sum_{i=1}^{m} f(a_i + h) + \sum_{i=1}^{m} e^{|a_i|} \phi(a_i) \tag{3.21}$$

Eftersom $h^p = p!$, så får vi att

$$\begin{aligned} f(h) &= \frac{h^{p-1}}{(p-1)!} b^{mp+p-1} (h-a_1)^p (h-a_2)^p \cdots (h-a_m)^p = \\ &= b^{p-1} (bh - ba_1)^p (bh - ba_2)^p \cdots (bh - ba_m)^p \end{aligned}$$

$f(h)$ är en symmetrisk funktion av $ca_1, ca_2, \ldots, ca_m$ med heltalskoefficienter, och är således ett heltal. Däremot är $cf(h)$ inte delbart med p, vilket medför att $cf(h)$ är skilt från 0. Vidare har vi att

$$\sum_{i=1}^{m} f(a_i + h) = \sum_{i=1}^{m} \frac{(bh + ba_i)^{p-1}}{(p-1)!}(bh + ba_i - ba_1)^p \cdots (bh + ba_i - ba_m)^p$$

Varje term i summan ovan innehåller termen $b^m p!$. Alltså kan vi förkorta bort $(p-1)!$.

$\sum_{i=1}^{m} f(a_i + h)$ har faktorn p, och det är ett heltal eftersom det är ett symmetriskt polynom av $a_1, a_2, \ldots, a_m$ med heltalskoefficienter.

Om vi låter p växa, går f och ϕ mot 0. Men eftersom en följd av heltal skilda från 0 inte kan konvergera mot 0, kan inte vänsterledet gå mot 0. Vi har fått en motsägelse, alltså måste π vara transcendent. ■

3.4 Lindemann–Weierstrass Teorem

Lindemann-Weierstrass teorem är ett intressant resultat som i vissa fall kan tillämpas för att bestämma om ett tal är transcendent eller inte. Det första beviset för att π är transcendent presenterades som ett korollarium till denna sats.

Sats 3.4.1 (Lindemann–Weierstrass Teorem)**.** *Om $\alpha_1, \ldots, \alpha_m$ är distinkta algebraiska tal, och $\beta_1, \ldots, \beta_m$ är algebraiska tal skilda från 0, så är*

$$\beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m} \neq 0$$

Denna sats kallas ibland Hermite-Lindemann eller Hermite-Lindemann-Weierstrass teorem. Hermite bevisade satsen (1873) i specialfallet då $\alpha_1 \ldots \alpha_m$ och $\beta_1, \ldots, \beta_m$ är heltal, och Lindemann generaliserade det. Weierstrass (1885) förenklade beviset avsevärt. Beviset finns till exempel i [[1], s. 6-8] och [5].

Med Lindemann-Weierstrass teorem är det lätt att visa att e och π är transcendenta. Om vi sätter $\alpha_1 = i\pi$, $\alpha_2 = 0$ och $\beta_1 = 1$, $\beta_2 = 1$, så har vi att

$$e^{i\pi} + 1 = 0$$

det följer då direkt av sats 3.4.1 att $i\pi$ – och därmed även π – är transcendent. På samma sätt, om vi sätter $\alpha_1 = 1$, $\alpha_2 = 2$ och $\beta_1 = e$, $\beta_2 = -1$, så har vi att

$$e^2 - e^2 = 0$$

vilket medför att e är transcendent.

3.5 Vidare resultat av Gelfond, Schneider och Schanuel

Lindemann-Weierstrass teorem är inte det enda som ger möjlighet att komma åt en större mängd transcendenta tal. Aleksandr Gelfond och Theodor Schneider visade följande sats oberoende av varandra 1934:

Sats 3.5.1 (Gelfond-Schneider teorem)**.** *Om α och β är är algebraiska tal sådana att $\alpha \neq 0, 1$ och β är irrationellt, då är α^β transcndent.*

Schneiders bevis finns i [15]. Gelfond-Schneiders teorem implicerar transcendensen av många (kanske mindre intressanta) tal, såsom $2^{\sqrt{2}}$ och $e^{\pi} = (e^{i\pi})^{-i} = (-1)^{-i}$ (ett av värdena).

Det finns en sats som skulle implicera både Lindemann-Weierstrass och Gelfond-Schneider teorem, om den kunde visas. Schanuel presenterade sin idé utan bevis 1960, och hittills har ingen lyckats visa den. Innan vi presenterar Schanuels förmodan måste vi definiera några algebraiska begrepp. I detta avsnitt använder vi $\mathbb{Q}$ istället för $\mathbb{Z}$, eftersom det senare inte är en kropp.

I följande definitioner antar vi att K är en delkropp av en kropp E.

Definition 3.5.2 (Algebraiskt oberoende)**.** Talen $a_1, \ldots, a_n \in E$ kallas algebraiskt oberoende över K om det för varje icke-trivialt polynom $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ gäller att $p(a_i \ldots, a_n) \neq 0$. Annars är $a_1, \ldots, a_n$ algebraiskt beroende över K.

Definition 3.5.3. Låt A vara en delmängd av E. Mängden $K[A]$ betecknar då ringen av alla ändliga summor av typen

$$\sum_{i_1 \ldots i_n \geq 0} b_{i_1 \ldots i_n} a_1^{i_n} \cdots a_n^{i_n}, \quad b_{i_1 \ldots i_n} \in K, \quad a_1, \ldots, a_n \in A,$$

och mängden $K(A)$ betecknar kroppen av alla element $c_1 c_2^{-1}$ där $c_1, c_2 \in K[A]$ och $c_2 \neq 0$.

Om A är en ändlig delmängd av E, säg $A = \{a_1, \ldots, a_n\}$, där $a_1, \ldots, a_n \in E$, är alltså $K[A] = K[a_1, \ldots, a_n]$ och $K(A) = K(a_1, \ldots, a_n)$. Som vanligt är här $K[x_1, ..., x_n]$ ringen av alla polynom i variablerna $x_1, ..., x_n$ med koefficienter i K och $K(x_1, ..., x_n)$ är kroppen av alla kvoter mellan sådana polynom.

Definition 3.5.4. Låt A vara en delmängd av E. Ett element $a \in E$ kallas algebraiskt över $K(A)$ precis om det finns ändligt många $b_0, b_1, \ldots, b_{n-1} \in K(A)$, sådana att

$$a^n + b_{n-1}a^{n-1} + \cdots + b_1 a + b_0 = 0$$

Eller ekvivalent: Ett element $a \in E$ kallas algebraiskt över $K(A)$ precis om det finns ändligt många $b_0, b_1, \ldots, b_n \in K[A]$, $b_n \neq 0$, sådana att

$$b_n a^n + \cdots + b_1 a + b_0 = 0$$

Kroppen E kallas algebraisk över $K(A)$ precis om varje $a \in E$ är algebraiskt över $K(A)$.

Definition 3.5.5 (Transcendensbas)**.** En transcendensbas för E över K är en delmängd A av E som är algebraiskt oberoende över K och sådan att E är algebraisk över $K(A)$.

Man kan visa att två olika (eventuellt oändliga) transcendensbaser för E över K har samma kardinalitet.

Definition 3.5.6 (Transcendensgrad)**.** Kardinaliteten för en transcendensbas för E över K kallas transcendensgraden för E över K.

Till exempel är transcendensgraden för $\mathbb{Q}(\pi)$ över $\mathbb{Q}$ lika med 1, medan transcendensgraden för $\mathbb{C}$ över $\mathbb{Q}$ är ∞. Det är känt att π och e^{π} är algebraiskt oberoende över $\mathbb{Q}$, men man vet inte om e och π är det.

Vi är nu färdiga att presentera Schanuels förmodan:

> Givet komplexa tal $\alpha_1, \ldots, \alpha_n$, som är linjärt oberoende över $\mathbb{Q}$, är transcendensgraden av kroppsutvidgningen $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ över $\mathbb{Q}$ minst n.

För att lättare se att Lindemann-Weierstrass teorem följer av Schanuels förmodan låt oss betrakta en ekvivalent formulering av satsen:

Sats 3.5.7 (En alternativ formulering av sats 3.4.1)**.** *Om $\alpha_1, \ldots, \alpha_n$ är algebraiska tal som är linjärt oberoende över $\mathbb{Q}$, då är transcendensgraden för $\mathbb{Q}(e^{\alpha_1}, \ldots, e^{\alpha_n})$ över $\mathbb{Q}$ lika med n.*

Från ovanstående ser man direkt att Lindemann-Weiestrass teorem är ett specialfall av Schanuels förmodan, där $\alpha_1, \ldots, \alpha_n$ antas vara algebraiska.

En generalisering till Gelfond-Schneider teorem, formulerad av Baker [[1], Sats 2.1], skulle också följa av Schanuels förmodan:

Sats 3.5.8 (En generalisering till Gelfond-Schneider teorem)**.** *Om $\alpha_1, \ldots, \alpha_n$ är algebraiska tal skilda från 0, sådana att $\ln \alpha_1, \ldots, \ln \alpha_n$ är linjärt oberoende över $\mathbb{Q}$, då är $1, \ln \alpha_1, \ldots, \ln \alpha_n$ algebraiskt oberoende över $\mathbb{Q}$.*

Schanuels förmodan skulle implicera att e och π är algebraiskt oberoende (detta kan ses genom att sätta $\alpha_1 = 1$, $\alpha_2 = i\pi$) och att $e + \pi$ är transcendent. Båda av dessa frågor ser enkla ut men saknar fortfarande svar. Mer om detta finns till exempel i [2].

Referenser

[1] Alan Baker. *Transcendental Number Theory.* Cambridge University Press, 1975.

[2] Timothy Y. Chow. What is a Closed-Form Number? *The American Mathematical Monthly*, 106(5):440–448, 1999.

[3] Henry Cohn. A Short Proof of the Simple Continued Fraction Expansion of e. *The American Mathematical Monthly*, 113(1):57–62, 2006.

[4] Janot de Stainville. *Mélange d'analyse Algébrique et de Géométrie.* Imprimeur Vve Courcier, 1815.

[5] J. P. Bezivin och P. Robba F. Beukers. An Alternative Proof of the Lindemann-Weierstrass Theorem. *The American Mathematical Monthly*, 97(3):193–197, 1990.

[6] P. Gordan. Transcendenz von e und π. *Matematische Annalen*, 43:222–224, 1893.

[7] David Hilbert. Über die Transcendenz der Zahlen e und π. *Matematische Annalen*, 43:216–219, 1893.

[8] Adolf Hurwitz. Beweis der Transcendenz der Zahl e. *Nachrichten v. d. Kgl. Gesellschaft d. Wiss.*, (4):153–155, 1893.

[9] Miklós Laczkovich. On Lambert's proof of the irrationality of π. *The American Mathematical Monthly*, 104(5):439–443, 1997.

[10] J. H. Lambert. Mémoire sur quelques propriétés remarquables des quantités transcendentes circulaires et logarihmiques. *Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlin*, 1768:265–322, 1761.

[11] Joseph Liouville. A propos de l'existence des nombres transcendants". *Comptes-rendus de l'Académie des sciences*, 18:883–885, 1844.

[12] Ivan Niven. *Irrational Numbers.* The Mathematical Association of America, 1956.

[13] Benjamin Fine och Gerhard Rosenberger. *Number Theory: an Introduction via the distribution of primes.* Birkhauser Boston Inc, 2006.

[14] C. Edward Sandifer. *How Euler Did It.* The Mathematical Association of America, 2007.

[15] Theodor Schneider. Transzendenzuntersuchungen periodischer Funktionen I. *Journal für die reine und angewandte Mathematik*, 172:65–69, 1935.

[16] Ferdinand von Lindemann. Über die Zahl π. *Mathematische Annalen*, 2:213–225, 1882.