CHALMERS

Komplexanalytiska metoder inom talteori

Kandidatarbete vid institutionen för Matematiska vetenskaper

Handledare: Hossein Raufi och Magnus Önnheim
Examinator: Maria Roginskaya

Edvin Listo Zec
Emma Ekberg
Gustav Lindwall
Jessica Fredby
Robin Andersson
Sofia Toivonen

Först av allt vill vi tacka Elias M. Stein och Remi Shakarchi, författarna till de böcker som har lagt grunden till vår rapport.

Vi vill även tacka alla doktorander som ihärdigt har lyssnat och ställt frågor under våra presentationer gällande delar av vårt arbete.

Till sist vill vi rikta vårt allra största tack till våra två handledare, Hossein Raufi och Magnus Önnheim. Under ett halvårs tid har ni hjälpt och stöttat oss på vår komplexa färd. Vi kan även säga att utan den röda rollern hade vår rapport inte varit vad den är idag.

Sammandrag

I det här kandidatarbetet redogör vi för bevis av tre klassiska satser från talteorin. Vi kommer att bevisa primtalssatsen, två- och fyrkvadratssatsen och Dirichlets sats om primtal i aritmetiska följder. Till vår hjälp tar vi begrepp ifrån komplexanalys och Fourieranalys, och arbetet innehåller därför också en grundlig teorigenomgång innan själva satserna kan bevisas.

Abstract

In this bachelor thesis we outline proofs for three classic theorems from number theory. We will prove the prime number theorem, Jacobi's two- and four-squares theorems and Dirichlet's theorem on primes in arithmetic sequences. In proving these theorems, methods from complex analysis and Fourier analys will be needed. Thus, this thesis includes a thorough review of the necessary theory.

Innehåll

Del I

Introduktion

Kapitel 1

Introduktion och repetition

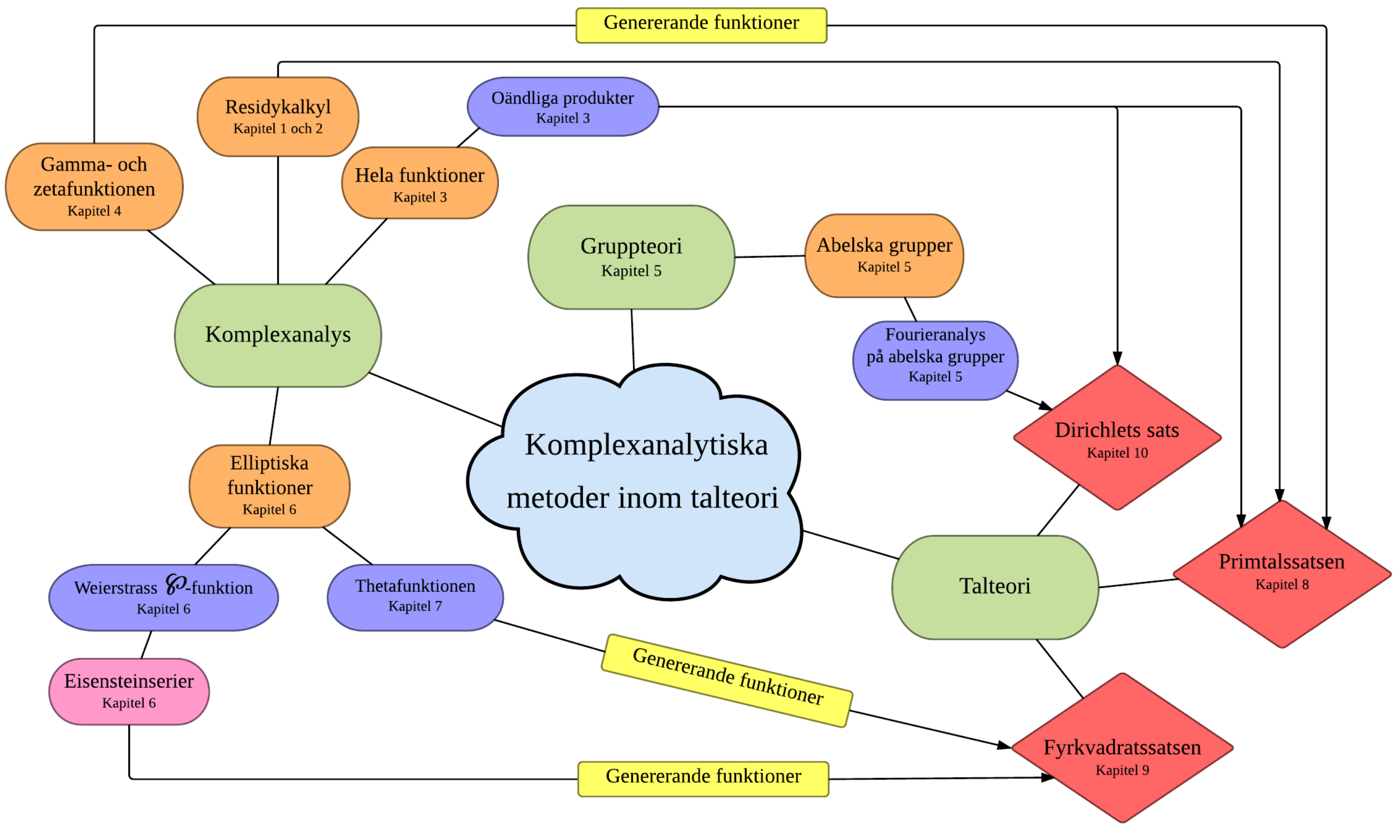
1.1 Syfte och bakgrund

Syftet med detta arbete är att med hjälp av metoder och resultat från komplex- och Fourieranalys bevisa tre klassiska satser inom talteori: primtalssatsen, Jacobis fyrkvadratssats och Dirichlets sats om primtal i aritmetiska följder. Denna gren av talteori, det vill säga den del där matematisk analys spelar en viktig roll, kallas för analytisk talteori. I detta arbete har vi inte bevisat något som tidigare inte har visats, utan fokus har istället legat på vår egen inlärning och att presentera teorin på ett tydligt sätt. Vår huvudsakliga källa är de två böckerna *Fourier Analysis: An introduction* och *Complex Analysis* skrivna av Elias M. Stein och Remi Shakarchi.

För att få en bättre bild av hur teorin och satserna hänger ihop har vi en mindmap, se Figur 1.1. Nu ska vi gå igenom lite mer om varje sats.

Primtalssatsen beskriver den asymptotiska fördelningen av primtal bland de positiva heltalen, och det visar sig att primtalen blir mindre vanliga då de blir större. Satsen formulerades först av Legendre och Gauss utifrån några begåvade gissningar i slutet av 1700-talet, men det var ungefär 100 år senare som Hadamard och la Valleé Poussin obereonde av varandra bevisade satsen med hjälp av komplexanalytiska metoder. Satsen säger mer precist att om vi låter $\pi(x)$ vara antalet primtal mindre än eller lika med x får vi att $\pi(x)$ beter sig som $x/\log(x)$ för ett obegränsat växande x. För att kunna bevisa satsen kommer vi främst att använda oss av komplexanalytiska metoder så som residykalkyl och en stor del av beviset är baserat på hur den så kallade zetafunktionen beter sig. Vi kommer strax att se att kopplingen mellan zetafunktionen och primtal är att zetafunktionen kan skrivas som en oändlig produkt bestående av just primtal.

Fyrkvadratssatsen säger att varje positivt heltal kan skrivas som en summa av fyra kvadrater och ger en formel för hur många olika sätt detta kan göras på. Intresset för att studera summor av kvadrater uppkom redan på Pythagoras tid då man insåg att i en rätvinklig triangel kommer hypotenusan i kvadrat att vara lika med summan av de båda kvadrerade kateterna. Ett bevis för att varje positivt heltal kan skrivas som en summa av fyra kvadrater publicerades år 1770 av Lagrange. Först år 1834 hittade Jacobi en formel för hur många olika sätt ett heltal kan uttryckas på som en summa av fyra kvadrater, vilket resulterade i Jacobis fyrkvadratssats. I hans bevis är en av de viktigare teoridelarna den om elliptiska funktioner och framförallt teorin bakom thetafunktionen och Eisensteinserierna. Med hjälp av genererande funktioner kan man koppla båda dessa funktioner till talteorin och därigenom bevisa Jacobis fyrkvadratssats.



Figur 1.1: Mindmap över teorin och satserna.

Dirichlets sats om primtal i aritmetiska talföljder säger att för varje par av positiva heltal q och ℓ som saknar gemensamma delare finns det oändligt många primtal på formen $\ell + kq$, där k är ett heltal. Satsen kan ses som en generalisering av Euklides sats som säger att det finns oändligt många primtal. Självklart var det Dirichlet som år 1837 publicerade satsen och han bevisade den med hjälp av komplexanalytiska metoder. Två huvudingredienser i beviset är oändliga produkter och ändliga abelska grupper, där vi vill kunna använda Fourieranalys på en ändlig abelsk grupp.

1.2 Riemanns zetafunktion

En av de mest centrala funktionerna i analytisk talteori är Riemanns zetafunktion, $\zeta(s)$.

Definition 1.1 (Riemanns zetafunktion)**.** *För $s > 1$ definieras Riemanns zetafunktion som*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{1.1}$$

Teorin för zetafunktionen, såsom dess nollställen, dess analytiska fortsättning och dess koppling till andra speciella funktioner kommer vi att behandla i kapitel 4. Redan nu kan vi dock beskriva funktionens remarkabla koppling till primtalen.

Sats 1.1 (Eulers produktformel)**.** *Om $s > 1$ har vi att*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \tag{1.2}$$

där produkten är över alla primtal p.

Vi kommer inte att presentera ett rigoröst bevis av Eulers produktformel här utan istället bara motivera att det är troligt att formeln stämmer. Explicit utskrivet har vi att

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots .$$

Multiplicerat med $1/2^s$ får vi att

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \dots .$$

Subtrahera nu denna serie från Riemanns zetafunktion

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \dots . \tag{1.3}$$

Vi noterar nu att den termen som följer ettan i summan är en trea, vilket i likhet med två även det är ett primtal. Om vi gör som tidigare och multiplicerar ekvation (1.3) med $1/3^s$ erhåller vi

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} \dots . \tag{1.4}$$

Vi följer samma procedur som tidigare och subtraherar ekvation (1.4) från ekvation (1.3),

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} \dots .$$

Här noterar vi att talet efter ett i summan återigen är ett primtal. Faktum är att det alltid kommer vara det. Alla icke-primtal har blivit eliminerade, då de måste vara en faktor av tidigare tal. Vi itererar processen över *alla* primtal, och får, formellt, identiteten

$$\prod_p \left(1 - p^{-s}\right)\zeta(s) = 1\,, \tag{1.5}$$

vilket är resultatet vi sökte efter.

Vi noterar att som en följd av att

$$\lim_{s \to 1^+} \zeta(s) = \infty\,, \tag{1.6}$$

inser man snabbt att antalet primtal är obegränsat. Om vi betraktar varje faktor i produkten

$$\prod_p \frac{1}{1 - p^{-s}}\,,$$

så inser man snabbt att varje faktor är ett begränsat tal större än 1, även när $s = 1$. Högerledet däremot divergerar enligt ekvation (1.6), vilket innebär att antalet primtal måste vara oändligt - det enda sättet att få en produkt av ändliga tal att bli oändligt stor är att ta oändligt många tal multiplicerat med varandra.

1.3 Illustrativa exempel

I stora drag baseras bevisen av satserna i den tredje och sista delen av detta arbete på metoder och tankebanor som förmodligen redan är välkända för läsaren. Satserna i sig behandlar i sin kärna beteendet hos vissa särskilda sekvenser av tal, men analytiskt är en talsekvens besvärlig att arbeta med. Vi väljer därför att göra omskrivningar till något som vi *kan* arbeta med, analytiska funktioner. Målet med samtliga av våra bevis är helt enkelt att hitta analytiska funktioner som berättar för oss hur vår sekvens av intresse beter sig. Nu följer två enklare exempel, som illustrerar denna idé.

1.3.1 Att uppskatta $n!$ med Laplaces metod

Vi börjar med att introducera Laplaces metod för uppskattning av integraler. Beviset utelämnas, men bygger på Taylorutvecklingar och den Gaussiska integralen $\int_0^\infty e^{-kx^2}\,\mathrm{d}x = \sqrt{\pi/k}$.

Sats 1.2 (Laplaces metod)**.** *Låt $\psi(x)$ vara en positiv funktion av maximal exponentiell tillväxt. Låt $\phi(x)$ vara en reellvärd, två gånger deriverbar funktion, med $\phi''(x_0) < 0$, där x_0 är funktionens extrempunkt i intervallet $[a,b]$, och s är en positiv parameter. Då gäller att*

$$\int_a^b \psi(x)e^{-s\phi(x)}\,\mathrm{d}x \sim \sqrt{\frac{2\pi}{s|\phi''(x_0)|}}\psi(x_0)e^{s\phi(x_0)}\,,$$

när s växer obegränsat.

Vi skall nu använda Laplaces metod i kombination med gammafunktionen $\Gamma(s)$ för att härleda en uppskattning för $n!$ som kallas för Stirlings formel.

Sats 1.3 (Stirlings formel)**.** *När n växer obegränsat gäller att*

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n(1+\varepsilon)},$$

där $\varepsilon \to 0$ då $n \to \infty$.

Definition 1.2 (Gammafunktionen)**.** *För $s > 0$ definieras Γ-funktionen som*

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}\,\mathrm{d}x.$$

Sats 1.4. *Med hjälp av partiell integration kan man visa att om s är ett heltal n så gäller att $\Gamma(n) = (n-1)!$.*

Speciellt gäller att

$$n! = n^{n+1}\int_0^\infty e^{n(\log x - x)}\,\mathrm{d}x. \tag{1.7}$$

Vi betraktar den här formuleringen utifrån Sats 1.2. Notera att $\log x - x$ är två gånger deriverbar och har en extrempunkt för $x = 1$. Andraderivatan av $\log x - x$ är $-1/x^2$, vilken är negativ för vår extrempunkt. Integralen i ekvation (1.7) uppfyller alla krav för att få använda Laplaces metod, med $\phi(x) = \log x - x$, och $\psi(x) = n^{n+1}$. Med direkt insättning enligt Sats 1.2 har vi nu fått fram Stirlings formel:

$$n! = n^{n+1}\int_0^\infty e^{n(\log x - x)}\,\mathrm{d}x \sim n^{n+1}\sqrt{\frac{2\pi}{n|\phi''(1)|}}e^{n\phi(1)},$$

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n(1+\varepsilon)},$$

där $\varepsilon \to 0$ när $n \to \infty$.

Det här tankesättet går igen i bevisen vi senare skall ägna oss åt. Vi har en intressant sekvens av tal, i fallet ovan $n!$, och vill studera dess beteende. Vi gör det genom att hitta en integral, gammafunktionen, som berättar något om sekvensen, och utför istället våra manipulationer på integralen, då en integral tillåter att man använder analytiska metoder. Efter en rad manipulationer av integralen får man fram ett asymptotiskt beteende för talföljden, vilket visar sig vara Stirlings formel. I beviset av primtalssatsen följer man samma princip. Dock kräver manipulationerna där mer kunskaper i komplexanalys än vad vi besitter just nu.

Gammafunktionen är i sig även den intressant, och återkommer i många satser som vi kommer att behandla. Där behandlas den som en analytisk funktion då $s \in \mathbb{C}$, och utvidgas till hela det komplexa talplanet.

1.3.2 Genererande funktioner

Att föra över en följd av tal på integralform är inte det enda sättet att bilda en analytisk funktion. Begreppet genererande funktion syftar på någon holomorf funktion $G(s)$ relaterad till en talföljd $\{a_n\}_{n=0}^{\infty}$ enligt

$$G(s) = \sum_{n=0}^{\infty} a_n s^n \,. \tag{1.8}$$

Vi kan som exempel betrakta de välbekanta Fibonacci-talen som rekursivt definieras som $F_n = F_{n-1} + F_{n-2}$, $F_0 = 0$, $F_1 = 1$. En genererande funktion till denna sekvens bygger på följande beräkning,

$$\begin{aligned}(1-s-s^2)\sum_{n=0}^{\infty} F_n s^n &= \sum_{n=0}^{\infty} F_n s^n - \sum_{n=1}^{\infty} F_{n-1} s^n - \sum_{n=2}^{\infty} F_{n-2} s^n = \\ &= F_0 + (F_1 - F_0)s + \sum_{n=2}^{\infty}(F_n - F_{n-1} - F_{n-2})s^n = s\,,\end{aligned}$$

det vill säga

$$\sum_{n=0}^{\infty} F_n s^n = \frac{s}{1-s-s^2}\,.$$

För att relatera detta till något möjligtvis mer välkänt är det värt att ta upp Z-transformen $X\left(a_n\right)(z)$ av en talföljd $\{a_n\}_{n=0}^{\infty}$ som definieras som

$$X\left(a_n\right)(z) = \sum_{n=0}^{\infty} a_n z^{-n}\,. \tag{1.9}$$

Z-transformen av $\{F_n\}_{n=0}^{\infty}$ blir alltså $X\left(F_n\right)(z) = z^{-1}/(1 - z^{-1} - z^{-2})$.

Z-transformen är vanligt förekommande inom signalbehandling för att hantera diskret mätdata, eftersom man överför en sekvens av tal till en analytisk funktion som sedan går att behandla. Sekvenserna inom talteori är inte som tillämpbar mätdata, men vi kan hantera dem på ett meningsfullt sätt med samma metoder som i mer tillämpade fall. Ett exempel är i bevisen av två- och fyrkvadratssatserna, där sekvensen som anger hur många sätt ett tal n kan skrivas på som en summa av 2 respektive 4 kvadrater har en genererande funktion.

1.4 Repetition av residykalkyl

Vi avslutar vår inledning med att repetera stommen i komplex analys, Cauchys sats, och den relaterade residysatsen.

Sats 1.5 (Cauchys sats)**.** *Låt $f(z)$ vara en holomorf funktion på en öppen, enkelt sammanhängade mängd i $\mathbb{C}$ innehållande en enkel, sluten kurva γ. Då gäller att*

$$\int_\gamma f(z)\,\mathrm{d}z = 0\,. \tag{1.10}$$

Sats 1.6 (Residysatsen)**.** *Låt D vara en öppen, enkelt sammanhängande delmängd av $\mathbb{C}$, och låt $z_1, z_2, ..., z_n$ vara ändligt många punkter i D. Om f är en funktion definierad och holomorf i $D \backslash \{z_1, z_2, ..., z_n\}$, och γ en enkel, positivt orienterad och sluten kurva i D, som ej går genom någon av punkterna $z_1, z_2, ..., z_n$, så gäller att*

$$\oint_\gamma f(z)\,\mathrm{d}z = 2\pi i \sum_k \mathrm{Res}(f, z_k)\,,$$

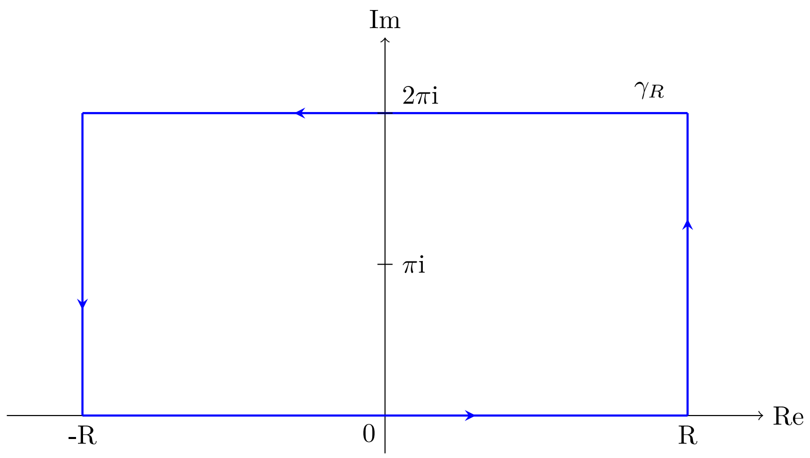
där k löper över all punkter z_k som ligger innanför γ.

En huvudsaklig tillämpning av residysatsen är beräkning av reella integraler, där huvudidén vanligtvis baseras på att man deformerar en ursprunglig kurva på ett smart sätt. Vi repeterar denna princip med ett exempel.

Exempel

$$I = \int_{\mathbb{R}} \frac{e^{ax}}{1+e^x}\,\mathrm{d}x = \frac{\pi}{\sin(\pi a)}\,, \quad 0 < a < 1\,.$$

Låt $f(z) = \frac{e^{az}}{1+e^z}$ och betrakta konturen nedan i figur 1.2.



Figur 1.2: *Konturen som vi integrerar över.*

Funktionen är holomorf i alla punkter innanför konturen förutom i $z = \pi i$. Låt $\gamma_R = \gamma_1 \cup \gamma_2 \cup \gamma_3 \cup \gamma_4$, räknat moturs med γ_1 som den nedre horisontella linjen. Vi noterar att

$$(z - \pi i) f(z) = e^{az} \frac{z - \pi i}{1 + e^z} = e^{az} \frac{z - \pi i}{e^z - e^{\pi i}}\,.$$

Vidare ser vi att
$$\frac{z-\pi i}{e^z - e^{\pi i}} \to \frac{1}{e^{\pi i}} = -1, \text{ då } z \to \pi i\,,$$
eftersom e^z är sin egna derivata. Därmed är $f'(\pi i)$ nollskild så $f(z)$ har en enkelpol i $z = \pi i$ och residyn beräknas genom att derivera nämnaren. Vi får att
$$\operatorname{Res}(f, \pi i) = \frac{e^{az}}{e^z}\Big|_{z=\pi i} = -e^{a\pi i}\,.$$
Residysatsen ger således att
$$\int_{\gamma_R} f(z)\,\mathrm{d}z = -2\pi i e^{a\pi i}\,. \tag{1.11}$$
Det återstår nu att undersöka integralen på varje del av konturen. Låt
$$I_R = \int_{\gamma_1} f(z)\,\mathrm{d}z = \int_{-R}^{R} f(x)\,\mathrm{d}x\,.$$
Vi ser att $I_R \to I$ då $R \to \infty$. Vidare har vi att
$$\int_{\gamma_3} f(z)\,\mathrm{d}z = \int_R^{-R} \frac{e^{a(x+2\pi i)}}{1+e^{x+2\pi i}}\,\mathrm{d}x = -e^{2a\pi i}\int_{-R}^{R}\frac{e^{ax}}{1+e^x}\,\mathrm{d}x = -e^{2a\pi i} I_R\,.$$
Samtidigt ser vi att
$$\left|\int_{\gamma_2} f(z)\,\mathrm{d}z\right| \le \int_0^{2\pi}\left|\frac{e^{a(R+iy)}}{1+e^{R+iy}}\right|\mathrm{d}y \le C\left|\frac{e^{aR}}{e^R-1}\right| = \left|C\frac{e^{(a-1)R}}{1-e^{-R}}\right|\,,$$
vilket går mot noll då R går mot oändligheten eftersom $a < 1$. På exakt samma sätt får vi att integralen över γ_4 går mot noll för stora värden på R. Sammantaget ger dessa observationer och ekvation (1.11) att
$$I - e^{2\pi i a} I = -2\pi i e^{a\pi i}\,.$$
Löser vi nu ut I och förenklar får vi att
$$I = -2\pi i \frac{e^{a\pi i}}{1-e^{2\pi i a}} = \frac{2\pi i}{e^{\pi i a} - e^{-\pi i a}} = \frac{\pi}{\sin(\pi a)}\,.$$

Del II

Teori

Kapitel 2

Fourieranalys

Fourieranalys kommer att spela en central roll i alla de tre stora bevisen. Syftet med det här kapitlet är att kort introducera några begrepp och resultat som eventuellt inte är så välkända från en grundläggande kurs i ämnet. Innan vi gör detta låt oss först påminna om den grundläggande definitionen.

Definition 2.1. *Låt f vara en lämplig funktion på $\mathbb{R}$. Då definieras Fouriertransformen av f som*

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x\xi} \,\mathrm{d}x\,, \quad \xi \in \mathbb{R}\,. \tag{2.1}$$

Låt oss också påminna om att under lämpliga förutsättningar gäller Fouriers inversionsformel

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi) e^{2\pi i x\xi} \,\mathrm{d}\xi\,, \quad x \in \mathbb{R}\,. \tag{2.2}$$

2.1 Funktionsklasserna $\mathfrak{F}$ och $\mathfrak{F}_a$

För varje $a > 0$ låter vi $\mathfrak{F}_a$ beteckna klassen av alla funktioner f som uppfyller följande två villkor.

(i) Funktionen f är holomorf i den horisontella remsan

$$S_a = \{z \in \mathbb{C} : |\mathrm{Im}(z)| < a\}\,.$$

(ii) Det existerar ett positivt tal A så att

$$|f(x+iy)| \le \frac{A}{1+x^2}\,, \qquad \text{för alla } x+iy \in S_a\,. \tag{2.3}$$

Med andra ord består $\mathfrak{F}_a$ av alla holomorfa funktioner på S_a som avtar kvadratiskt på varje horisontell linje $\mathrm{Im}(z) = y$ likformigt i $-a < y < a$. Vi låter även $\mathfrak{F}$ beteckna klassen av alla funktioner som tillhör $\mathfrak{F}_a$ för något a, det vill säga $\mathfrak{F} = \bigcup_{a>0} \mathfrak{F}_a$.

Sats 2.1. *Om $f \in \mathfrak{F}_a$ för något $a > 0$ så gäller att*

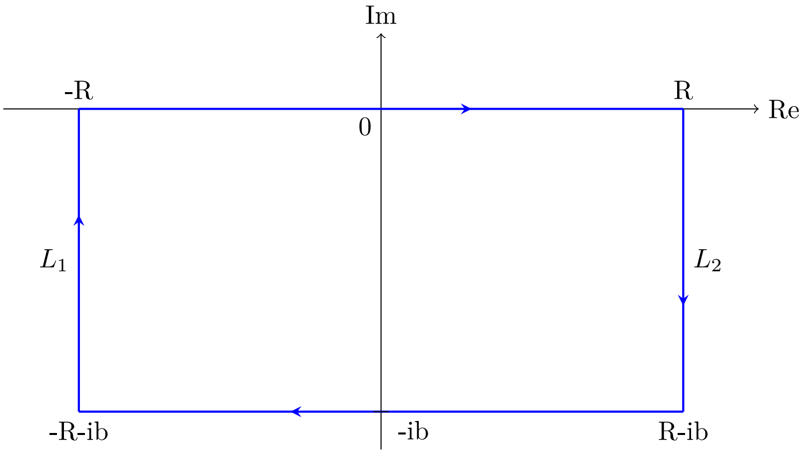
$$|\hat{f}(\xi)| \le B e^{-2\pi b|\xi|}\,, \tag{2.4}$$

för varje $0 \le b < a$.

Bevis. Vi har att

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e^{-2\pi i x\xi}\,\mathrm{d}x\,. \tag{2.5}$$

Specialfallet då $b = 0$ innebär att $\hat{f}(\xi)$ är begränsad, vilket följer från ekvation (2.5), antagandet att f uppfyller (2.3) och att $e^{-2\pi i x\xi}$ är begränsad av 1. För det allmänna fallet $0 < b < a$ antar vi först att $\xi > 0$. Betrakta funktionen $g(z) = f(z)e^{-2\pi i z\xi}$ och konturen i Figur 2.1.



Figur 2.1: *Konturen i beviset av Sats 2.1 när* $\xi > 0$.

Då R går mot oändligheten kommer integralen av g över de vertikala segmenten L_1 och L_2 att gå mot noll. Till exempel kan integralen av g över L_1 uppskattas som

$$\left|\int_{L_1} g(z)\,\mathrm{d}z\right| \leq \int_0^b \left|f(-R-it)e^{-2\pi i(-R-it)\xi}\right|\,\mathrm{d}t \leq \int_0^b \frac{A}{1+R^2}e^{-2\pi t\xi}\,\mathrm{d}t = O(1/R^2)\,.$$

Samma uppskattning gäller för L_2. Därför, om vi tillämpar residysatsen på rektangeln och låter R går mot oändligheten, följer att

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x-ib)e^{-2\pi i(x-ib)\xi}\,\mathrm{d}x\,, \tag{2.6}$$

vilket ger

$$\left|\hat{f}(\xi)\right| \leq \int_{-\infty}^{\infty} \frac{A}{1+x^2}e^{-2\pi b\xi}\,\mathrm{d}x \leq Be^{-2\pi b\xi}\,,$$

för någon lämplig konstant B. Liknande argument kan göras för $\xi < 0$, men med konturen utbytt mot en rektangel i det övre halvplanet. □

Exempel. Vi ska nu använda våra nyförvärvade kunskaper om klassen $\mathfrak{F}_a$ för att kort och koncist motivera ett sällsamt resultat,

$$I = \int_{\mathbb{R}} \frac{e^{-2\pi i x\xi}}{\cosh(\pi x)}\,\mathrm{d}x = \frac{1}{\cosh(\pi\xi)}\,. \tag{2.7}$$

Med andra ord vill vi visa att $1/(\cosh \pi x)$ är sin egen Fouriertransform. Då $\cosh(t)$ har exponentiell tillväxt, är det tydligt att den tillhör klassen $\mathfrak{F}_a$. Vi kan börja med att betrakta samma typ av kurva som i Figur 2.1, fast med $b = -2i$. Vi har alltså fyra kurvor att integrera längs. Låt γ beteckna hela kurvan och låt

$$I_R = \int_{-R}^{R} \frac{e^{-2\pi i x\xi}}{\cosh(\pi x)} \, \mathrm{d}x.$$

På det övre linjestycket där $z = x + 2i$ är integranden lika med

$$\frac{e^{-2\pi i(x+2i)\xi}}{\cosh(\pi x)} = e^{4\pi\xi} \frac{e^{-2\pi i x\xi}}{\cosh(\pi x)} \,,$$

alltså

$$\int_\gamma \frac{e^{-2\pi i z\xi}}{\cosh(\pi z)} \, \mathrm{d}z = -I_R + e^{4\pi\xi} I_R - \int_{L_2} \frac{e^{-2\pi i z\xi}}{\cosh(\pi z)} \, \mathrm{d}z - \int_{L_4} \frac{e^{-2\pi i z\xi}}{\cosh(\pi z)} \, \mathrm{d}z \,.$$

Om integralen över de vertikala linjesegmenten går mot noll för stora R, så gäller det tillsammans med residysatsen att

$$I = 2\pi i \frac{-1}{1 - e^{4\pi\xi}} \sum \operatorname{Res}(f, z_i) \,,$$

där x_i betecknar enkelpolerna $z_1 = -i/2$ samt $z_2 = -3i/2$, med tillhörande residyer $-\frac{e^{-\pi\xi}}{\pi i}$ och $\frac{e^{-3\pi\xi}}{\pi i}$. Vi behöver alltså slutligen verifiera att integranden går mot noll för $z = R + iy$, då R går mot oändligheten. Men detta följer direkt av att $|\cosh(z)|$ går mot noll då $\operatorname{Re}(z)$ går mot oändligheten. Alltså, integralen längs L_2 och L_4 går mot noll och detta ger därför att

$$\int_{\mathbb{R}} \frac{e^{-2\pi i x\xi}}{\cosh(\pi x)} \, \mathrm{d}x = \frac{1}{\cosh(\pi\xi)} \,.$$

2.2 Poissons summationsformel

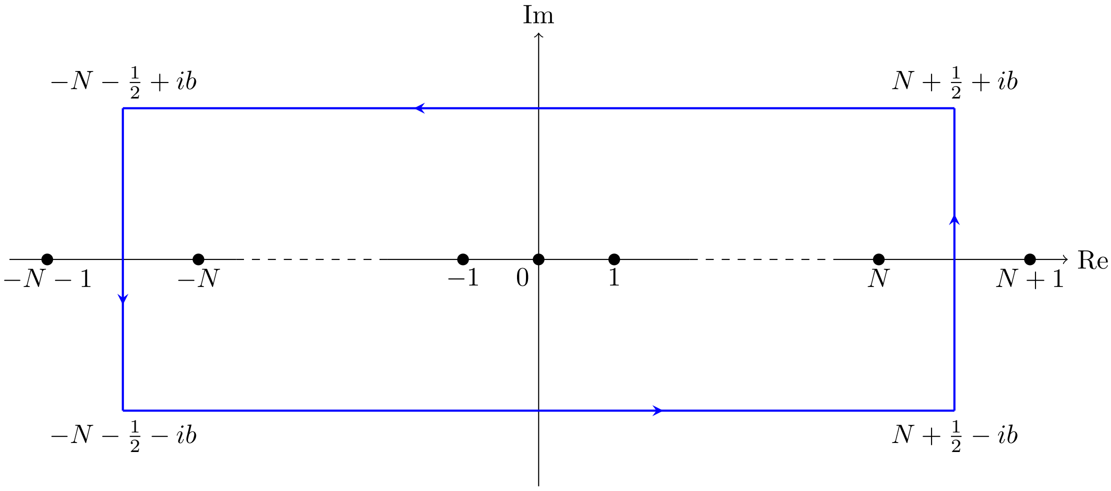
Vi kommer nu till ett resultat som relaterar summan av en funktion f i en mängd diskreta punkter till dess Fouriertransform $\hat{f}$. Detta är ett mycket användbart resultat inte bara inom analytisk talteori, utan också exempelvis inom signalbehandling. Satsen kommer att användas flitigt framöver i kommande kapitel samt i beviset för två- och fyrkvadratssatsen.

Sats 2.2 (Poissons summationsformel)**.** *Om $f \in \mathfrak{F}$ så gäller att*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n) \,. \tag{2.8}$$

Bevis. Antag $f \in \mathfrak{F}_a$ och välj $0 < b < a$. Funktionen $1/(e^{2\pi iz} - 1)$ har enkelpoler med residy $1/(2\pi i)$ i alla heltal. Funktionen $f(z)/(e^{2\pi iz} - 1)$ har därmed också enkelpoler vid $n \in \mathbb{Z}$ med residy $f(n)/(2\pi i)$.

Vi vill använda residysatsen så vi inför följande kontur:



Figur 2.2: *Konturen i beviset för Poissons summationsformel. Vi låter konturen betecknas med γ.*

Denna kontur kan parametriseras som

$$\gamma = \gamma_1 \cup \gamma_2 \cup \gamma_3 \cup \gamma_4 = \begin{cases} \gamma_1 : \ z = x - ib\,, & x \in [-N-\frac{1}{2}, N+\frac{1}{2}], N \in \mathbb{Z}\,, \\ \gamma_2 : \ z = N + \frac{1}{2} - iy\,, & y \in [-b, b]\,, \\ \gamma_3 : \ z = x + ib\,, & x \in [N+\frac{1}{2}, -N-\frac{1}{2}], N \in \mathbb{Z}\,, \\ \gamma_4 : \ z = -N - \frac{1}{2} + iy\,, & y \in [b, -b]\,, \end{cases} .$$

Residysatsen ger nu

$$\sum_{|n| \le N} f(n) = \int_\gamma \frac{f(z)}{e^{2\pi i z} - 1}\, \mathrm{d}z\,.$$

Om vi låter N gå mot oändligheten ser vi att summan i ekvationen konvergerar mot $\sum_{n\in\mathbb{Z}} f(n)$. Vi vill nu visa att integralerna längs γ_2 och γ_4 går mot noll. Vi uppskattar I_{γ_2} till belopp och får att

$$\begin{aligned} |I_{\gamma_2}| = \left| \int_{\gamma_2} \frac{f(z)}{e^{2\pi i z} - 1}\, \mathrm{d}z \right| \le \left| \frac{1}{i} \int_{-b}^{b} \frac{f(N+\frac{1}{2}+iy)}{e^{2\pi i(N+\frac{1}{2}+iy)} - 1}\, \mathrm{d}y \right| \le \\ \le \int_{-b}^{b} \frac{|f(N+\frac{1}{2}+iy)|}{|e^{2\pi i(N+\frac{1}{2}+iy)} - 1|}\, \mathrm{d}y\,. \end{aligned} \tag{2.9}$$

Låt oss undersöka det sista uttrycket ovan. Nämnaren kan skrivas som

$$|e^{2\pi i(N+\frac{1}{2}+iy)} - 1| = |e^{-2\pi y} e^{2\pi i(N+\frac{1}{2})} - 1| = |e^{-2\pi y} e^{2\pi i N} e^{\pi i} - 1| = |e^{-2\pi y} + 1|\,, N \in \mathbb{N}\,.$$

Med detta insatt i (2.9) fås

$$|I_{\gamma_2}| \le \int_{|y| \le b} \frac{|f(N+\frac{1}{2}+iy)|}{|e^{-2\pi y} + 1|}\, \mathrm{d}y\,.$$

Då $f \in \mathfrak{F}$ har vi enligt (2.3) att

$$|I_{\gamma_2}| \le \int_{|y| \le b} \frac{A}{1 + (N+\frac{1}{2})^2} \frac{1}{|e^{-2\pi y} + 1|}\, \mathrm{d}y \underset{N\to\infty}{\longrightarrow} 0\,.$$

Med ett analogt resonemang kan integralen längs γ_4 uppskattas och därmed följer att $|I_{\gamma_4}|$ går mot noll då N går mot oändligheten.

Alltså följer att

$$\sum_{n\in\mathbb{Z}} f(n) = \lim_{N\to\infty}\left(\int_{\gamma_1}\frac{f(z)}{e^{2\pi iz}-1}\,\mathrm{d}z - \int_{\gamma_3}\frac{f(z)}{e^{2\pi iz}-1}\,\mathrm{d}z\right), \tag{2.10}$$

där γ_1 och γ_3 är de två horisontella linjerna, det vill säga real-axeln förskjutna i det komplexa talplanet ner respektive upp med b.

Vi använder nu formeln för en geometrisk summa

$$\frac{1}{\omega-1} = -\sum_{n=0}^{\infty}\omega^n, \quad \text{för} \quad |\omega|<1\,.$$

Välj $\omega = e^{2\pi iz}$. På γ_3 har vi $z = x+ib$ och får att $|\omega|<1$, så på γ_3 gäller att

$$\frac{1}{e^{2\pi iz}-1} = -\sum_{n=0}^{\infty} e^{2\pi inz}\,.$$

På γ_1 har vi $z = x - ib$, vilket ger att $|\omega| > 1$. Vi gör då en omskrivning av den geometriska summan genom att sätta $|\tilde{\omega}| = 1/|\omega|$, vilket ger att

$$\frac{1}{\omega-1} = \omega^{-1}\sum_{n=0}^{\infty}\omega^{-n}, \quad \text{för} \quad |\omega|>1\,.$$

På γ_1 gäller därför att

$$\frac{1}{e^{2\pi iz}-1} = e^{-2\pi iz}\sum_{n=0}^{\infty} e^{-2\pi inz}\,.$$

Med insättning av dessa geometriska summor i (2.10) får vi att

$$\begin{aligned}\sum_{n\in\mathbb{Z}} f(n) &= \int_{\gamma_1} f(z)\left(e^{-2\pi iz}\sum_{n=0}^{\infty}e^{-2\pi inz}\right)\mathrm{d}z - \int_{\gamma_3} f(z)\left(-\sum_{n=0}^{\infty}e^{2\pi inz}\right)\mathrm{d}z = \\ &= \sum_{n=0}^{\infty}\int_{\gamma_1} f(z)e^{-2\pi i(n+1)z}\,\mathrm{d}z + \sum_{n=0}^{\infty}\int_{\gamma_3} f(z)e^{2\pi inz}\,\mathrm{d}z\,.\end{aligned}$$

På γ_1 har vi att z kan parametriseras som $z = x - ib$ och på γ_3 får vi $z = x + ib$. Från (2.6) följer nu att

$$\begin{aligned}\sum_{n\in\mathbb{Z}} f(n) &= \sum_{n=0}^{\infty}\int_{-\infty}^{\infty} f(x)e^{-2\pi i(n+1)x}\,\mathrm{d}x + \sum_{n=0}^{\infty}\int_{-\infty}^{\infty} f(x)e^{2\pi inx}\,\mathrm{d}x = \\ &= \sum_{n=0}^{\infty}\hat{f}(n+1) + \sum_{n=0}^{\infty}\hat{f}(-n) = \sum_{n\in\mathbb{Z}}\hat{f}(n)\,.\end{aligned}$$

□

Kapitel 3

Hela funktioner

En viktig klass av funktioner är de hela funktionerna, vilka är komplexvärda funktioner som är holomorfa på hela det komplexa talplanet. Klassiska exempel på sådana funktioner är polynom och exponentialfunktioner. Exempel på icke-hela funktioner är $\frac{1}{z}$ och $\log z$. Det finns många viktiga begrepp och resultat relaterade till hela funktioner, och det vi framförallt är intresserade av är oändliga produkter, Weierstraß produktformel, Hadamards faktoriseringssats samt tillväxtordning hos hela funktioner.

3.1 Oändliga produkter

Givet en sekvens $\{a_n\}_{n=1}^{\infty}$ av komplexa tal kan vi konstruera en oändlig produkt

$$\prod_{n=1}^{\infty} a_n = a_1 a_2 a_3 \dots .$$

Vi säger att produkten konvergerar om gränsvärdet av den partiella produkten existerar, det vill säga om

$$\lim_{N\to\infty} \prod_{n=1}^{N} a_n = P < \infty.$$

Ett nödvändigt krav som garanterar att en oändlig produkt konvergerar är följande proposition.

Proposition 3.1. *Om $\sum_{n=1}^{\infty} |a_n|$ konvergerar så konvergerar $\prod_{n=1}^{\infty}(1+a_n)$. Dessutom så konvergerar den oändliga produkten mot noll om och endast om en av faktorerna är noll.*

Bevis. Vi har att $\sum |a_n|$ konvergerar, vilket innebär att vi kan välja N tillräckligt stor så att $|a_n| < 1/2$ för alla $n > N$, och genom att bortse från ändligt många termer kan vi anta att $|a_n| < 1/2$ för alla n. Vi kan således definiera $\log(1 + a_n)$ med hjälp av serieutvecklingen för logaritmen, det vill säga

$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots = -\sum_{n=1}^{\infty} (-1)^n \frac{z^n}{n} \text{ för } |z| < 1.$$

Denna logaritm har egenskapen att $1 + z = e^{\log(1+z)}$ för $|z| < 1$, vilket ger att

$$\prod_{n=1}^{N}(1+a_n) = \prod_{n=1}^{N} e^{\log(1+a_n)} = e^{B_N},$$

med $B_N = \sum_{n=1}^{N} b_n$ och där $b_n = \log(1 + a_n)$. För $|z| < 1/2$ gäller det från logaritmens serieutveckling att $|\log(1 + z)| \leq 2|z|$. Alltså har vi att $|b_n| \leq 2|a_n|$, vilket ger oss att

$$\lim_{N\to\infty} B_N = \lim_{N\to\infty} \sum_{n=1}^{N} b_n = B < \infty,$$

då $\sum |a_n|$ konvergerar. Till följd av kontinuitet har vi att e^{B_N} går mot e^B då N går mot oändligheten. Således är första delen av propositionen bevisad.

För att se att produkten endast konvergerar mot noll om en av faktorerna är noll noterar vi att om $1 + a_n \neq 0$ för alla n gäller det att produkten konvergerar mot ett nollskilt tal då produkten är en summa av exponentialer. $\square$

Vi går nu vidare och betraktar oändliga produkter av holomorfa funktioner. För detta behöver vi dock först påminna om följande grundläggande egenskaper hos holomorfa funktioner. För den intresserade återfinns bevisen på sidorna 53-55 i Complex Analysis av Stein & Schakarchi.

Sats 3.2. *Låt $\{f_n\}_{n=1}^{\infty}$ vara en sekvens av holomorfa funktioner som konvergerar likformigt mot en funktion f på varje kompakt delmängd K av D. Då är f holomorf på hela D.*

Sats 3.3. *Om Sats 3.2 gäller, så gäller även att sekvensen $\{f'\}$ konvergerar likformigt mot f' på varje kompakt delmängd K av D.*

Proposition 3.4. *Antag att $\{F_n\}$ är en sekvens av holomorfa funktioner på en öppen mängd $D \subset \mathbb{C}$. Om det existerar konstanter $c_n > 0$ sådana att*

$$\sum c_n < \infty \text{ och } |F_n(z) - 1| \leq c_n \quad \text{för alla } z \in D,$$

så gäller att

(i) Produkten $\prod_{n=1}^{\infty} F_n(z)$ konvergerar likformigt på D mot en holomorf funktion $F(z)$.

(ii) Om $F_n(z) \neq 0$ för alla n, så kommer

$$\frac{F'(z)}{F(z)} = \sum_{n=1}^{\infty} \frac{F_n'(z)}{F_n(z)}.$$

Bevis. (i) För alla z kan vi skriva $F_n(z) = 1 + a_n(z)$, med $|a_n(z)| \leq c_n$. Eftersom c_n är konstanter, vet vi att uppskattningen är likformig i z. Det följer enligt Proposition 3.1 att produkten konvergerar likformigt på D mot en funktion $F(z)$. Enligt Sats 3.2 är då $F(z)$ holomorf.

(ii) För att visa andra delen av propositionen låter vi K vara en godtycklig kompakt delmängd av D och låter

$$G_N(z) = \prod_{n=1}^{N} F_n(z).$$

Från (i) vet vi att G_N konvergerar likformigt mot F på D. Sats 3.3 ger oss då att $\{G_N'\}$ konvergerar likformigt mot F' på K. Eftersom K valdes godtyckligt kommer detsamma att gälla för varje punkt i D. Alltså får vi att

$$\frac{G_N'}{G_N} \to \frac{F'}{F} = \sum_{n=1}^{\infty} \frac{F_n'}{F_n}, \quad \text{för varje punkt i } D,$$

eftersom $|G_N|$ är likformigt begränsad underifrån. $\square$

3.2 Weierstraß produktformel

Weierstraß produktformel visar att hela funktioner kan faktoriseras, precis som polynom. Som ett led på vägen till att visa detta börjar vi med att visa en omvändning till detta påstående: givet en sekvens av nollställen är det möjligt att skapa en hel funktion med exakt dessa nollställen.

Lemma 3.5. *Givet en följd av komplexa tal, $\{a_n\}$, där $|a_n| \to \infty$ då $n \to \infty$ så existerar det en hel funktion f som är noll för $z = a_n$ och annars är skild från noll.*

Den naturliga kandidaten till f ges av produktformeln

$$f(z) = \prod_{n=1}^{\infty}(1 - z/a_n).$$

Problemet med denna produkt är att den endast konvergerar för vissa följder av $\{a_n\}$. För att korrigera detta definierar vi de kanoniska faktorerna.

Definition 3.1. *För varje $k \geq 0$, definierar vi de kanoniska faktorerna, E_k, som*

$$E_k(z) = \begin{cases} (1-z) & k = 0 \\ (1-z)e^{z+z^2/2+\ldots+z^k/k} & k \geq 1. \end{cases}$$

Här kallas k graden av de kanoniska faktorerna.

Det visar sig att vi kan använda dessa faktorer för att få produkten att konvergera utan att vi lägger till fler nollställen. För detta behöver vi följande lemma.

Lemma 3.6. *För $|z| \leq 1/2$ gäller att $|1 - E_k(z)| \leq c|z|^{k+1}$ för något $c > 0$.*

Bevis. Då $|z| \leq 1/2$, har vi att

$$1 - z = e^{\log(1-z)} = e^{-\sum z^n/n},$$

vilket ger att

$$E_k(z) = e^{\log(1-z)+z+z^2/2+\ldots+z^k/k} = e^w, \text{ där } w = -\sum_{n=k+1}^{\infty} z^n/n.$$

Notera att eftersom $|z| \leq 1/2$ har vi att

$$|w| \leq |z|^{k+1} \sum_{n=k+1}^{\infty} \frac{|z|^{n-k-1}}{n} \leq |z|^{k+1} \sum_{j=0}^{\infty} 2^{-j} \leq 2|z|^{k+1}.$$

Särskilt har vi att $|w| < 1$, vilket ger att

$$|1 - E_k(z)| = |1 - e^w| \leq c'|w| \leq c|z|^{k+1}.$$

□

Observera att konstanten c i lemmat ovan är oberoende av n. I beviset ser vi att vi kan sätta $c' = e$, vilket ger att $c = 2e$.

Vi är nu redo att bevisa Lemma 3.5.

Bevis av Lemma 3.5. Antag att vi har ett nollställe av ordning m i $z = 0$ och att alla $a_1, a_2...$ är skilda från noll. Då använder vi oss av Weierstraß-produkten

$$f(z) = z^m \prod_{n=1}^{\infty} E_n(z/a_n). \tag{3.1}$$

Vi påstår att denna funktion är hel med ett nollställe av ordning m i $z = 0$, att den har ett nollställe i varje punkt av följden $\{a_n\}$ och att den i övrigt är skild från noll. För att bevisa Lemma 3.5 räcker det nu att visa att detta påstående gäller på disken $|z| < R$, för ett godtyckligt positivt R. Vi betraktar de två fallen $|a_n| \leq 2R$ och $|a_n| > 2R$ var för sig. Eftersom $|a_n|$ går mot oändligheten ser vi att det finns ett begränsat antal termer i det första fallet. Det här ger att den begränsade produkten är noll i alla $z = a_n$, där $|a_n| \leq 2R$. För $|a_n| > 2R$ har vi att $|z/a_n| < 1/2$. Från Lemma 3.6 får vi att

$$|1 - E_n(z/a_n)| \leq c \left|\frac{z}{a_n}\right|^{n+1} \leq \frac{c}{2^{n+1}},$$

där c är oberoende av n enligt observationen ovan. Enligt Proposition 3.4 har vi att produkten

$$\prod_{|a_n| \geq 2R} E_n(z/a_n)$$

definierar en holomorf funktion för $|z| < R$ och som inte är noll på denna cirkelskiva. Då $R > 0$ är godtyckligt har vi härmed lyckats konstruera en hel funktion f som endast försvinner i $z = a_n$ och vi har bevisat Lemma 3.5. □

Sats 3.7 (Weierstraß produktformel)**.** *Låt f vara hel med nollställen i $\{a_n\}$, där $a_1, a_2...$ är skilda från noll och med ett nollställe av ordning m i $z = 0$ och. Då kan f skrivas som*

$$f(z) = e^{g(z)} z^m \prod_{n=1}^{\infty} E_n\left(\frac{z}{a_n}\right), \tag{3.2}$$

där $g(z)$ är en hel funktion.

Bevis. Enligt Lemma 3.5 är

$$f_1 = z^m \prod_{n=1}^{\infty} E_n\left(\frac{z}{a_n}\right)$$

en hel funktion med samma nollställen och

$$h(z) = \frac{f(z)}{f_1(z)}$$

är hel och saknar nollställen. Det räcker därför att visa att vi kan skriva $h(z) = e^{g(z)}$, för någon hel funktion $g(z)$, vilken vi kan skriva som

$$g(z) = \log h(0) + \int_0^z \frac{h'(w)}{h(w)}\,\mathrm{d}w.$$

Eftersom h är en hel funktion utan nollställen har vi att g är en hel funktion. Löser vi integralen ovan får vi att

$$h(z) = e^{g(z)},$$

Vi har alltså att

$$f(z) = \underbrace{\frac{f(z)}{f_1(z)}}_{=h(z)} f_1(z) = e^{g(z)} z^m \prod_{n=1}^{\infty} E_n \left(\frac{z}{a_n} \right).$$

□

3.3 Hadamards faktoriseringssats

Vi är nu redo att introducera Hadamards faktoriseringssats som förfinar en av Weierstraß produktformel. För att kunna göra detta behövs dock begreppet tillväxtordning för hela funktioner.

Definition 3.2. *Låt f vara en hel funktion. Om det finns ett positivt heltal ρ och två konstanter $A, B > 0$ sådana att*

$$|f(z)| \leq Ae^{B|z|^{\rho}} \quad \textit{för alla } z \in \mathbb{C} \ , \tag{3.3}$$

säger vi att f har tillväxtordning $\leq \rho$. Vidare definierar vi också tillväxtordningen av f som $\rho_f = \inf \rho$.

Exempelvis har vi att tillväxtordningen för funktionen e^{z^2} är exakt lika med 2, medan för ett godtyckligt polynom $p(z)$ är tillväxtordningen noll. Följdsats 3.7 visar att en hel funktion f med nollskilda nollställen $\{a_n\}_{n=1}^{\infty}$ kan skrivas enligt ekvation (3.2). Hadamard visade dock att för hela funktioner med ändlig tillväxtordning kan graden för de kanoniska faktorerna betraktas som konstant, och funktionen $g(z)$ är då ett polynom.

Sats 3.8 (Hadamards faktoriseringssats)**.** *Antag att f är hel och har tillväxtordning ρ. Låt k vara ett heltal sådant att $k \leq \rho < k + 1$. Om $a_1, a_2, \ldots$ är nollställen till f och är skilda från noll, så gäller att*

$$f(z) = e^{P(z)} z^m \prod_{n=1}^{\infty} E_k \left(\frac{z}{a_n} \right) ,$$

där P är ett polynom av grad $\leq k$, och m är ordningen av nollstället till f i $z = 0$.

Vi kommer behöva denna sats i våra senare studier av zetafunktionen, $\zeta(s)$, men vi utelämnar beviset. För den intresserade läsaren hänvisar vi till Complex Analysis av Stein & Shakarchi, kapitel 5 avsnitt 5.

Kapitel 4

Gamma- och zetafunktionen

I det här avsnittet kommer vi att studera teorin för gamma- och zetafunktionen, två viktiga funktioner inom bland annat talteori. Teorin vi behandlar i detta kapitel har delvis utvecklats specifikt för att bevisa primtalssatsen, en av våra tre stora satser.

Gammafunktionen har haft en betydande roll i den matematiska historien och många framträdande matematiker har ägnat mycket tid åt denna funktion. Philip J. Davis har dokumenterat gammafunktionens historia i en artikel, i vilken han skriver att varje generation har funnit något intressant att säga om gammafunktionen och att nästa generation förmodligen också kommer att ha det.[1]

Riemanns zetafunktions användningsområde är minst lika stort som gammafunktionens och används inom allt från sannolikhetslära och statistik till fysik. Zetafunktionen kommer att vara en huvudpelare till bron vi bygger från komplexanalysen till den analytiska talteorin.

4.1 Gammafunktionen

Definition 4.1. *För komplexa tal $s \in \mathbb{C}$ med $Re(s) > 0$ definieras gammafunktionen som den konvergenta integralen*

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} \,\mathrm{d}t \tag{4.1}$$

och kan ses som en funktion som generaliserar fakulteten av ett heltal.

Vi kommer även att se att gammafunktionen med hjälp av analytisk fortsättning kan utvidgas till det komplexa talplanet för alla s som inte är negativa heltal eller noll. Innan vi bevisar detta påminner vi dock först om följande grundläggande sats från komplexanalysen.

Sats 4.1. *Antag att $F(z,s)$ är definierad för $(z,s) \in D \times [0,1]$, där D är en öppen delmängd i $\mathbb{C}$. Antag vidare att F uppfyller följande egenskaper*

(i) *$F(z,s)$ är holomorf i z för varje s.*

(ii) *F är kontinuerlig på $D \times [0,1]$.*

[1] Davis, P. J. (1959). Leonhard Euler's Integral: A Historical Profile of the Gamma Function", The American Mathematical Monthly, Vol. 66, No. 10 (Dec., 1959), pp. 849–869.

Då gäller det att funktionen f definierad på D som

$$f(z) = \int_0^1 F(z, s)\, \mathrm{d}s$$

är holomorf.

För bevis av satsen hänvisar vi till Complex Analysis av Stein och Shakarchi sida 56.

Proposition 4.2. *Gammafunktionen är holomorf i halvplanet* $\mathrm{Re}(s) > 0$*.*

Bevis. Det räcker att bevisa att integralen i ekvation (4.1) definierar en holomorf funktion på varje remsa

$$S_{\delta,M} = \{\delta < \mathrm{Re}(s) < M\}, \tag{4.2}$$

där $0 < \delta < M < \infty$. Notera att om vi låter σ beteckna realdelen av s får vi att

$$|e^{-t}t^{s-1}| = e^{-t}t^{\sigma-1}.$$

Detta ger att integralen

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\, \mathrm{d}t,$$

som definieras av att gränsvärdet

$$\lim_{\varepsilon\to 0} \int_\varepsilon^{1/\varepsilon} e^{-t}t^{s-1}\, \mathrm{d}t,$$

konvergerar för varje $s \in S_{\delta,M}$. Låt

$$F_\varepsilon(s) = \int_\varepsilon^{1/\varepsilon} e^{-t}t^{s-1}\, \mathrm{d}t.$$

Om $\{F_\varepsilon\}$ är en sekvens av holomorfa funktioner som konvergerar likformigt till Γ på varje remsa $S_{\delta,M}$ får vi från Sats 3.2 att Γ är holomorf på halvplanet $\mathrm{Re}(s) > 0$. För att visa att F_ε är en holomorf funktion definierar vi först

$$G(s,t) = e^{-t}t^{s-1}.$$

Här är G definierad för mängden

$$(s,t) \in S_{\delta,M} \times [\varepsilon, 1/\varepsilon]. \tag{4.3}$$

Funktionen G är en holomorf funktion i s för varje t och är kontinuerlig på mängden (4.3). Detta ger att G uppfyller alla egenskaper för Sats 4.1 som ger att $\{F_\varepsilon\}$ är en sekvens av holomorfa funktioner på remsan $S_{\delta,M}$. Kvar att visa är att F_ε konvergerar likformigt till Γ på remsan. Notera först att

$$|\Gamma(s) - F_\varepsilon(s)| \leq \int_0^\varepsilon e^{-t}t^{\sigma-1}\, \mathrm{d}t + \int_{1/\varepsilon}^\infty e^{-t}t^{\sigma-1}\, \mathrm{d}t. \tag{4.4}$$

I den första integralen är e^{-t} begränsad, vilket ger att

$$\left|\int_0^\varepsilon e^{-t}t^{\sigma-1}\, \mathrm{d}t\right| \leq \int_0^\varepsilon t^{\sigma-1}\, \mathrm{d}t = \left[\frac{t^\sigma}{\sigma}\right]_{t=0}^{t=\varepsilon} \leq \frac{\varepsilon^\delta}{\delta},$$

då $0 < \varepsilon < 1$. Det här ger att den första integralen i (4.4) går likformigt mot noll på remsan $S_{\delta,M}$ när ε går mot noll. Den andra integralen i (4.4) kan uppskattas som

$$\left|\int_{1/\varepsilon}^{\infty} e^{-t} t^{\sigma-1}\,\mathrm{d}t\right| \leq \int_{1/\varepsilon}^{\infty} e^{-t} t^{M-1}\,\mathrm{d}t \leq C_2 \int_{1/\varepsilon}^{\infty} e^{-t/2}\,\mathrm{d}t.$$

Uppskattningen ovan ger att även den andra integralen i ekvation (4.4) konvergerar likformigt mot noll när ε går mot noll. Därmed har vi visat att F_ε konvergerar likformigt till Γ på remsan $S_{\delta,M}$. □

4.2 En analytisk fortsättning av gammafunktionen

Vi har tidigare noterat att gammafunktionen inte är definierad på hela det komplexa talplanet. Faktum är dock att vi kan utvidga vår definition av gammafunktionen och visa att det existerar en meromorf funktion definierad i hela $\mathbb{C}$ som är identiskt lika med gammafunktionen i högra halvplanet. Vi säger alltså att denna funktion, som är definierad i hela $\mathbb{C}$, är den analytiska fortsättningen av gammafunktionen, och vi fortsätter att beteckna den med symbolen Γ. För att visa detta behöver vi följande lemma.

Lemma 4.3. *För alla $s \in \mathbb{C}$ sådana att $\mathrm{Re}(s) > 0$ gäller att*

$$\Gamma(s+1) = s\Gamma(s)\,.$$

Bevis. Låt $\varepsilon > 0$. Vi har att

$$\int_{\varepsilon}^{\frac{1}{\varepsilon}} \frac{\mathrm{d}}{\mathrm{d}t}\left(e^{-t} t^{s}\right)\,\mathrm{d}t = -\int_{\varepsilon}^{\frac{1}{\varepsilon}} e^{-t} t^{s}\,\mathrm{d}t + s\int_{\varepsilon}^{\frac{1}{\varepsilon}} e^{-t} t^{s-1}\,\mathrm{d}t\,,$$

och noterar att vänsterledet försvinner då ε går mot noll. Det följer att $\Gamma(s+1) = s\Gamma(s)$. □

Som en konsekvens får vi från upprepning av lemmat ovan att

$$\Gamma(n+1) = n!$$

för varje positivt heltal n om vi utnyttjar att

$$\Gamma(1) = \int_{0}^{\infty} e^{-t}\,\mathrm{d}t = \left[-e^{-t}\right]_{0}^{\infty} = 1.$$

Vi går nu vidare med att utvidga Gammafunktionen till hela det komplexa talplanet.

Sats 4.4. *Funktionen $\Gamma(s)$, inledningsvis definierad för $\mathrm{Re}(s) > 0$, kan med analytisk fortsättning utvidgas till en meromorf funktion på hela det komplexa talplanet. De enda singulariteterna till Γ är enkla poler i de icke-positiva heltalen. Residyn för Γ vid $s = -n$ är*

$$\mathrm{Res}(\Gamma,\,-n) = \frac{(-1)^n}{n!}.$$

Bevis. För att bevisa satsen räcker det att utvidga Γ till varje halvplan $\mathrm{Re}(s) > -m$, där $m \geq 1$ är ett heltal. För fallet $\mathrm{Re}(s) > -1$ sätter vi

$$F_1(s) = \frac{\Gamma(s+1)}{s}.$$

Eftersom $\Gamma(s+1)$ är holomorf i $\mathrm{Re}(s) > -1$ fås att F_1 är meromorf för $\mathrm{Re}(s) > -1$ med en singularitet i enkelpolen $s = 0$. Vi vet att $\Gamma(1) = 1$ vilket ger att funktionen F_1 i enkelpolen $s = 0$ har residyn 1. Om $\mathrm{Re}(s) > 0$ fås från Lemma 4.3 att

$$F_1(s) = \frac{\Gamma(s+1)}{s} = \Gamma(s).$$

Detta ger att F_1 utvidgar $\Gamma(s)$ till en meromorf funktion på $\mathrm{Re}(s) > -1$. Om vi nu gör på samma sätt för en funktion F_m på halvplanet $\mathrm{Re}(s) > -m$, där $m \geq 1$ är ett heltal, får vi att

$$F_m(s) = \frac{\Gamma(s+m)}{s(s+1)\dots(s+m-2)(s+m-1)}.$$

På samma sätt som ovan får vi att F_m är en meromorf funktion på $\mathrm{Re}(s) > -m$ med enkelpoler i $s = 0 - 1, \dots, -m+1$. Residyn för F_m i en enkelpol $s = -n$ är då

$$\begin{aligned}
\mathrm{Res}(F_m, -n) &= \lim_{s\to -n}(s+n)F_m(s) = \\
&= \lim_{s\to -n}(s+n)\frac{\Gamma(s+m)}{s\dots(s+n)\dots(s+m-1)} = \\
&= \lim_{s\to -n}\frac{\Gamma(s+m)}{s\dots(s+n-1)(s+n+1)\dots(s+m-1)} = \\
&= \frac{\Gamma(-n+m)}{(-n)\dots(-1)(+1)\dots(-n+m-1)} = \\
&= \frac{\Gamma(-n+m)}{(-n)\dots(-1)(-n+m-1)!} = \\
&= \frac{(-n+m-1)!}{(-n)\dots(-1)(-n+m-1)!} = \frac{(-1)^n}{n!}.
\end{aligned}$$

I uträkningarna ovan har vi använt att $\Gamma(n+1) = n!$. För $\mathrm{Re}(s) > 0$ får vi från samma lemma att

$$\begin{aligned}
F_m(s) &= \frac{\Gamma(s+m)}{s(s+1)\dots(s+m-2)(s+m-1)} = \\
&= \frac{\Gamma(s+m-1)}{s(s+1)\dots(s+m-2)} = \dots = \frac{\Gamma(s+1)}{s} = \Gamma(s).
\end{aligned}$$

Detta ger att F_m utvidgar Γ till en meromorf funktion på $\mathrm{Re}(s) > -m$ med singulariteter i enkelpolerna. Om vi nu tar en funktion F_k, där $1 \leq k \leq m$, har vi att $F_m = F_k$ på $\mathrm{Re}(s) > -k$. Från detta får vi att Γ har en analytisk fortsättning till en meromorf funktion på hela det komplexa talplanet. □

Vi fortsätter nu med några viktiga egenskaper som Γ-funktionen besitter.

Sats 4.5. *För alla $s \in \mathbb{C}$ gäller att*

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}.$$

För att bevisa satsen behöver vi följande lemma.

Lemma 4.6. *För $0 < a < 1$ gäller att*

$$\int_0^\infty \frac{v^{a-1}}{1+v}\,\mathrm{d}v = \frac{\pi}{\sin \pi a}. \tag{4.5}$$

Bevis. Genom att göra variabelbytet $v = e^x$ får vi att

$$\int_0^\infty \frac{v^{a-1}}{1+v}\,\mathrm{d}v = \int_{-\infty}^\infty \frac{e^{ax}}{1+e^x}\,\mathrm{d}x.$$

Denna integral kan beräknas med hjälp av residykalkyl över en kontur i övre halvplanet. Detta är redan gjort i första integralexemplet i Kapitel 1, vilket visade att integralen är lika med $\pi/\sin \pi a$. □

Bevis av sats 4.5. Vi noterar att för $s \in (0,1)$ ger variabelbytet $u = vt$ att

$$\Gamma(1-s) = \int_0^\infty e^{-u}u^{-s}\,\mathrm{d}u = t\int_0^\infty e^{-vt}(vt)^{-s}\,\mathrm{d}v.$$

Med hjälp av detta och Lemma 4.5 får vi att

$$\begin{aligned}
\Gamma(1-s)\Gamma(s) &= \int_0^\infty e^{-t}t^{s-1}\Gamma(1-s)\,\mathrm{d}t \\
&= \int_0^\infty e^{-t}(t)^{s-1}\left(t\int_0^\infty e^{-vt}(vt)^{-s}\,\mathrm{d}v\right)\mathrm{d}t \\
&= \int_0^\infty \int_0^\infty e^{-t[1+v]}v^{-s}\,\mathrm{d}v\,\mathrm{d}t \\
&= \int_0^\infty \frac{v^{-s}}{1+v}\,\mathrm{d}v \\
&= \frac{\pi}{\sin \pi(1-s)} = \frac{\pi}{\sin \pi s}.
\end{aligned}$$

□

Vi fortsätter nu att studera gammafunktionen genom att istället betrakta $1/\Gamma(s)$.

Sats 4.7. *Gammafunktionen har följande egenskaper*

(i) $1/\Gamma(s)$ *är en hel funktion med enkla nollställen i* $s = 0, -1, -2, \ldots$ *och är annars skild från noll.*

(ii) $1/\Gamma(s)$ *har tillväxt*

$$\left|\frac{1}{\Gamma(s)}\right| \leq c_1 e^{c_2|s|\log|s|}.$$

Detta ger att $1/\Gamma(s)$ *har tillväxtordning 1, det vill säga för alla* $\varepsilon > 0$ *finns ett* $c(\varepsilon)$ *sådant att*

$$\left|\frac{1}{\Gamma(s)}\right| \leq c(\varepsilon)e^{c_2|s|^{1+\varepsilon}}.$$

Bevis. (i) Från Sats 4.5 har vi att

$$\frac{1}{\Gamma(s)} = \Gamma(1-s)\frac{\sin \pi s}{\pi}. \tag{4.6}$$

Vi vet att $\Gamma(s)$ har enkelpoler vid $s = 0, -1, -2, \ldots$ vilket ger oss att $\Gamma(1-s)$ har poler vid $s = 1, 2, 3, \ldots$. Vi vet även att $\sin(\pi s)$ har enkla nollställen vid alla heltal, så alla positiva nollställen kancellerar enkelpolerna för $\Gamma(1-s)$. Detta ger att $1/\Gamma$ har enkla nollställen vid $s = 0, -1, -2, \ldots$.

(ii) Vi utgår från Definition 4.1 för Γ som för $\mathrm{Re}(s) > 0$ ger att

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\,\mathrm{d}t = \int_0^1 e^{-t}t^{s-1}\,\mathrm{d}t + \int_1^\infty e^{-t}t^{s-1}\,\mathrm{d}t.$$

Genom att potensserieutveckla e^{-t} och integrera termvis får vi att

$$\int_0^1 e^{-t}t^{s-1}\,\mathrm{d}t = \sum_{n=1}^{\infty}\frac{(-1)^n}{n!(n+s)}, \quad \text{för } \mathrm{Re}(s) > 0,$$

vilket ger

$$\Gamma(s) = \sum_{n=1}^{\infty}\frac{(-1)^n}{n!(n+s)} + \int_1^\infty e^{-t}t^{s-1}\,\mathrm{d}t.$$

Sätter vi in detta i (4.6) får vi att

$$\frac{1}{\Gamma(s)} = \left(\sum_{n=1}^{\infty}\frac{(-1)^n}{n!(n+1-s)}\right)\frac{\sin \pi s}{\pi} + \left(\int_1^\infty e^{-t}t^{-s}\,\mathrm{d}t\right)\frac{\sin \pi s}{\pi}, \quad \text{för } s \in \mathbb{C}. \tag{4.7}$$

Vi visar först att för $\sigma = \mathrm{Re}(s)$ har vi att

$$\int_1^\infty e^{-t}t^{\sigma}\,\mathrm{d}t \le e^{(\sigma+1)\log(\sigma+1)}.$$

Välj n så att $\sigma \le n \le \sigma + 1$. Detta ger att

$$\begin{aligned}\int_1^\infty e^{-t}t^{\sigma}\,\mathrm{d}t \le \int_0^\infty e^{-t}t^{n}\,\mathrm{d}t = \Gamma(n+1) = n! \le \\ \le n^n = e^{n\log n} \le e^{(\sigma+1)\log(\sigma+1)}.\end{aligned}$$

Vi använder nu detta för att uppskatta integralen

$$\left|\int_1^\infty e^{-t}t^{-s}\,\mathrm{d}t\right| \le \int_1^\infty e^{-t}t^{|\sigma|}\,\mathrm{d}t \le e^{(|\sigma|+1)\log(|\sigma|+1)}.$$

Från Eulers formel fås att $|\sin \pi s| \le e^{\pi|s|}$, vilket tillsammans med uppskattningen ovan ger att den andra termen i (4.7) kan uppskattas som

$$\left|\left(\int_1^\infty e^{-t}t^{-s}\,\mathrm{d}t\right)\frac{\sin \pi s}{\pi}\right| \le c_1 e^{(|s|+1)\log(|s|+1)}e^{\pi|s|} \le c_1 e^{c_2|s|\log|s|}. \tag{4.8}$$

Nu återstår det att begränsa termen

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n!(n+1-s)}\frac{\sin \pi s}{\pi}, \tag{4.9}$$

i (4.7). Problemet här är när vi i summan får noll i nämnaren, det vill säga när $(n+1-s)=0$, vilket sker när vi är nära ett heltal. Det finns alltså två fall att betrakta, ett där $|\text{Im}(s)|>1$ och ett där $|\text{Im}(s)|\leq 1$. I det första fallet när $|\text{Im}(s)|>1$ har vi inga problem och uttrycket till belopp domineras av sinustermen, vilket ger att uttrycket är begränsat av $e^{\pi|s|}$.

För att undersöka det andra fallet när vi befinner oss nära realaxeln väljer vi k till att vara ett heltal så att $k-1/2\leq \text{Re}(s)<k+1/2$. För $k\geq 1$ kan vi ta ut termen som kan ge att nämnaren är noll i summan, alltså

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n!(n+1-s)}\frac{\sin\pi s}{\pi}=(-1)^k\frac{\sin\pi s}{(k-1)!(k-s)}+\sum_{n\neq k-1}\frac{(-1)^n}{n!(n+1-s)}\frac{\sin\pi s}{\pi}.$$

För den första termen konstaterar vi att singulariteten i $s=k$ är hävbar, då $\sin\pi s$ försvinner vid alla heltal k. I den andra termen är summan begränsad av $e^{\pi|s|}$.

För $k\leq 0$ får vi från vårt antagande att $\text{Re}(s)<1/2$ där summan återigen är begränsad av $e^{\pi|s|}$. Vi har därmed bevisat att (4.9) är begränsad av $e^{c_2|s|}$ och beviset är klart. □

I Kapitel 3 visade vi att hela funktioner kan skrivas som en oändlig produkt. I och med att $1/\Gamma(s)$ är en hel funktion med tillväxtordning 1 får vi följande sats.

Sats 4.8. *För alla $s\in\mathbb{C}$ gäller att*

$$\frac{1}{\Gamma(s)}=e^{\gamma s}s\prod_{n=1}^{\infty}\left(1+\frac{s}{n}\right)e^{-s/n},$$

där γ kallas Eulers konstant och är definierad som

$$\gamma=\lim_{N\to\infty}\sum_{n=1}^{N}\frac{1}{n}-\log N.$$

Detta följer av Hadamards faktoriseringssats som vi introducerade i Kapitel 3.

4.3 Riemanns zetafunktion

Definition 4.2. *För $s>1$ definieras Riemanns zetafunktion som*

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\,.$$

Som vi tidigare har nämnt är denna funktion fundamental inom analytisk talteori i allmänhet och primtalssatsen i synnerhet.

Egenskaperna hos zetafunktionen hänger nära samman med gammafunktionen och, precis som för gammafunktionen, finns det en analytisk fortsättning i det komplexa talplanet. Vi kommer även se att funktionen är symmetrisk runt linjen $\text{Re}(s)=1/2$ och studera hur $\zeta(s)$ växer kring $\text{Re}(s)=1$.

Proposition 4.9. *Serien som definierar $\zeta(s)$ konvergerar för $Re(s)>1$, och funktionen ζ är holomorf i detta halvplan.*

Bevis. Låt $s = \sigma + it$, där $\sigma, t \in \mathbb{R}$. Då gäller att

$$|n^{-s}| = |e^{-s \log n}| = e^{-\sigma \log n} = n^{-\sigma}.$$

Om vi nu har att $\sigma > 1 + \delta > 1$ så kommer serien som definierar ζ att vara likformigt begränsad av den konvergenta serien $\sum_{n=1}^{\infty} 1/n^{1+\delta}$. Detta medför att serien $\sum 1/n^s$ konvergerar likformigt på varje halvplan $\mathrm{Re}(s) > 1 + \delta > 1$, vilket ger en holomorf funktion i halvplanet $\mathrm{Re}(s) > 1$. □

Som nämnts i introduktionen så relaterar ζ till primtalen via Eulers produktformel, vars bevis görs i mer allmänhet för Dirichlets L-funktioner i Proposition 10.6.

Sats 4.10 (Eulers produktformel)**.** *För $Re(s) > 1$ gäller*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

där produkten löper över alla primtal.

För att studera den analytiska fortsättningen av zetafunktionen introducerar vi ännu en viktig funktion, nämligen thetafunktionen.

Definition 4.3. *Thetafunktionen betecknas med $\vartheta(t)$ och definieras som*

$$\vartheta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}, \quad \textit{för } t > 0.$$

Vi kommer bland annat att använda oss av denna thetafunktions så kallade funktionalekvation

$$\vartheta(t) = t^{-1/2} \vartheta(1/t), \quad \text{för } t > 0, \tag{4.10}$$

vilken är en följd av Poissons summationsformel, se Sats 2.2. Vi ser detta genom att tillämpa Poissons summationsformel på funktionerna

$$f(x) = e^{-\pi t (x+a)^2} \quad \text{och} \quad \hat{f}(\xi) = t^{-1/2} e^{-\pi \xi^2 / t} e^{2\pi i a \xi},$$

vilket ger oss

$$\sum_{n=-\infty}^{\infty} e^{-\pi t (n+a)^2} = \sum_{n=-\infty}^{\infty} t^{-1/2} e^{-\pi n^2 / t} e^{2\pi i n a}.$$

Då $a = 0$ får vi precis funktionalekvationen i (4.10).

Vi kommer vidare att ha användning av thetafunktionens tillväxt och avtagande

$$\vartheta(t) \leq C t^{-1/2} \text{ då } t \to 0, \tag{4.11}$$

$$|\vartheta(t) - 1| \leq C e^{-\pi t} \text{ för något } C > 0 \text{ och alla } t \geq 1. \tag{4.12}$$

Olikheten i (4.11) följer från funktionalekvationen (4.10) medan (4.12) följer från att

$$\sum_{n \geq 1} e^{-\pi n^2 t} \leq \sum_{n \geq 1} e^{-\pi n t} = e^{-\pi t} \sum_{n=0}^{\infty} e^{-\pi n t} \leq e^{\pi t} \sum_{n=0}^{\infty} e^{-\pi n} = C e^{-\pi t}, \text{ för } t \geq 1.$$

Vi är nu redo att bevisa ett viktigt samband mellan ζ, Γ och ϑ.

Sats 4.11. *För* $\mathrm{Re}(s) > 1$ *gäller att*

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta\left(s\right) = \frac{1}{2}\int_0^\infty u^{\frac{s}{2}-1}[\vartheta(u)-1]\,\mathrm{d}u\,.$$

Bevis. Vi börjar med att notera att

$$\int_0^\infty e^{-\pi n^2 u}u^{(s/2)-1}\,\mathrm{d}u = \pi^{-s/2}\Gamma(s/2)n^{-s},\ \text{då } n \geq 1, \tag{4.13}$$

vilket följer av variabelbytet $u = t/\pi n^2$. Observera nu att

$$\frac{\vartheta(u)-1}{2} = \sum_{n=1}^\infty e^{-\pi n^2 u}.$$

Detta ser vi genom att notera att $\vartheta(u) = \sum_{n=-\infty}^\infty e^{-\pi n^2 u}$ är en jämn funktion, det vill säga att

$$\vartheta(u) = \sum_{n=-\infty}^\infty e^{-\pi n^2 u} = 2\sum_{n=1}^\infty e^{-\pi n^2 u} + 1.$$

Uppskattningarna (4.11) och (4.12) tillåter oss att byta plats på den oändliga summan och integralen, vilket ger oss:

$$\begin{aligned}\frac{1}{2}\int_0^\infty u^{(s/2)-1}[\vartheta(u)-1]\,\mathrm{d}u &= \sum_{n=1}^\infty\int_0^\infty u^{(s/2)-1}e^{-\pi n^2 u}\,\mathrm{d}u\\ &= \pi^{-s/2}\Gamma(s/2)\sum_{n=1}^\infty n^{-s}\\ &= \pi^{-s/2}\Gamma(s/2)\zeta(s)\,.\end{aligned}$$

□

Låt oss nu betrakta en lite modifierad zetafunktion som kallas för xi-funktionen.

Definition 4.4. *För* $\mathrm{Re}(s) > 1$ *definierar vi xi-funktionen enligt*

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s). \tag{4.14}$$

Sats 4.12. *Funktionen* $\xi(s)$ *är holomorf för* $\mathrm{Re}(s) > 1$ *och har en analytisk fortsättning i hela* $\mathbb{C}$ *som en meromorf funktion med enkelpoler i* $s = 0$ *och* $s = 1$*. Dessutom gäller att*

$$\xi(s) = \xi(1-s) \text{ för alla } s \in \mathbb{C}.$$

Bevis. Låt $\psi(u) := [\vartheta(u)-1]/2$. Funktionalekvationen (4.10) ger att

$$\psi(u) = u^{-1/2}\psi(1/u) + \frac{1}{2u^{1/2}} - \frac{1}{2}.$$

Enligt Sats 4.11 har vi för $\mathrm{Re}(s) > 1$ att

$$\begin{aligned}
\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) &= \int_0^\infty u^{(s/2)-1}\psi(u)\,\mathrm{d}u = \\
&= \int_0^1 u^{(s/2)-1}\psi(u)\,\mathrm{d}u + \int_1^\infty u^{(s/2)-1}\psi(u)\,\mathrm{d}u = \\
&= \int_0^1 u^{(s/2)-1}\left[u^{-1/2}\psi(1/u) + \frac{1}{2u^{1/2}} - \frac{1}{2}\right]\mathrm{d}u + \\
&+ \int_1^\infty u^{(s/2)-1}\psi(u)\,\mathrm{d}u = \\
&= \frac{1}{s-1} - \frac{1}{s} + \int_0^1 u^{(s/2)-3/2}\psi\left(\frac{1}{u}\right)\mathrm{d}u + \int_1^\infty u^{(s/2)-1}\psi(u)\,\mathrm{d}u = \\
&= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \left(u^{(-s/2)-1/2} + u^{(s/2)-1}\right)\psi(u)\,\mathrm{d}u.
\end{aligned}$$

I ekvationen ovan kommer sista likheten från variabelbytet $u = 1/t$. Vidare noterar vi att $\vartheta - 1$ avtar exponentiellt vid oändligheten, vilket innebär att även ψ gör det enligt (4.12). Detta i sin tur medför att integralen ovan definierar en hel funktion, vilket medför att ξ har en analytisk fortsättning i hela $\mathbb{C}$ med enkelpoler vid $s = 0$ och $s = 1$. Slutligen observerar vi att integralen inte påverkas av att byta ut s mot $1 - s$, vilket även håller för summan av de två termerna $1/(s-1) - 1/s$. Därmed ser vi att $\xi(s) = \xi(1-s)$. □

Vi ska nu gå över till att visa att zetafunktionen kan utvidgas till en meromorf funktion i hela det komplexa talplanet.

Sats 4.13. *Zetafunktionen har en meromorf fortsättning i hela $\mathbb{C}$ vars enda pol är en enkelpol vid $s = 1$.*

Bevis. Från (4.14) fås att ζ kan skrivas på formen

$$\zeta(s) = \pi^{s/2}\frac{\xi(s)}{\Gamma(s/2)}\,.$$

Vi vet att $1/\Gamma(s)$ är en hel funktion och vi har även i Sats 4.7 visat att $1/\Gamma(s/2)$ har nollställen i $s = 0, -2, -4, \ldots$. Vidare vet vi från Sats 4.12 att $\xi(s)$ har enkelpoler i $s = 0$ och $s = 1$. Men eftersom $1/\Gamma(s/2) = 0$ för $s = 0$ blir $\zeta(s)$ holomorf i $s = 0$, och därmed blir den enda polen för $\zeta(s)$ i $s = 1$. □

Sats 4.14. *De enda nollställena till ζ utanför remsan $0 \leq \mathrm{Re}(s) \leq 1$ är de jämna negativa heltalen $-2, -4, -6, \ldots$ och kallas de triviala nollställena.*

Bevis. Enligt Proposition 3.1 har vi för $\mathrm{Re}(s) > 1$ att zetafunktionen på dess produktframställning är noll om och endast om en av termerna i produkten är noll. Detta ger att ζ inte har några nollställen.

Vi vet sedan tidigare att vi kan skriva xi-funktionen som

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)\,.$$

Från Sats 4.12, som säger att $\xi(s) = \xi(1-s)$, får vi då att

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left((1-s)/2\right)\zeta(1-s)\,.$$

Från detta kan vi skriva zetafunktionen som

$$\zeta(s) = \pi^{s-1/2} \frac{\Gamma\left((1-s)/2\right)}{\Gamma\left(s/2\right)} \zeta(1-s)\,.$$

Här ser vi att för $\mathrm{Re}(s) < 0$ har zetafunktionen följande egenskaper

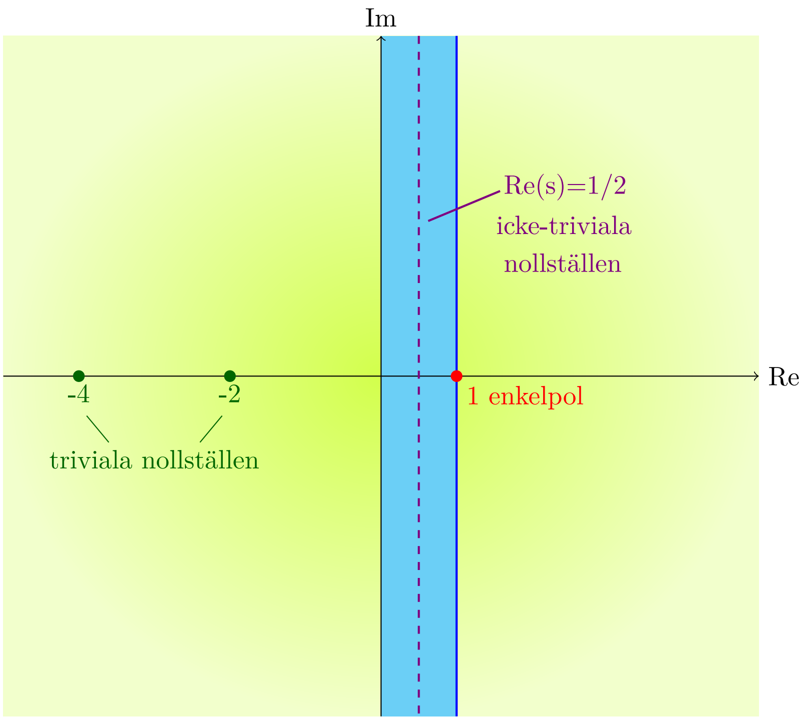
(i) $\zeta(1-s)$ har inga nollställen eftersom $\mathrm{Re}(1-s) > 1$.

(ii) $\Gamma((1-s)/2)$ har inga nollställen.

(iii) $1/\Gamma(s/2)$ har nollställen vid alla jämna negativa heltal eftersom $1/\Gamma(s)$ har nollställen vid alla negativa heltal för $\mathrm{Re}(s) < 0$.

Vi har nu visat att zetafunktionen inte har några nollställen för $\mathrm{Re}(s) > 1$ och för $\mathrm{Re}(s) < 0$ har den nollställen i alla negativa jämna heltal . □

Nu har vi visat att zetafunktionen har nollställen vid alla negativa jämna heltal utanför remsan $0 \leq \mathrm{Re}(s) \leq 1$ och man brukar kalla dessa för zetafunktionens triviala nollställen. Resten av zetafunktionens nollställen kan man visa ligger innanför denna kritiska remsa och dessa kallas de icke-triviala nollställena. Det är här Riemannhypotesen, ett av de sju millenieproblemen, kommer in. Hypotesen säger att alla nollställen tilll Riemanns zetafunktion, utom de triviala, kommer ligga på linjen $\mathrm{Re}(s) = 1/2$. Man har redan hittat flera icke-triviala nollställen, vilka alla har visat sig ligga på denna linje, men hypotesen är inte bevisad ännu.



Figur 4.1: *Illustration över zetafunktionens trivila och icke-triviala nollställen samt enkelpolen och den kritiska remsan.*

Vi kommer nu att behandla en mer elegant metod för att visa den analytiska fortsättningen av zetafunktionen, vilken enkelt ger oss funktionens utvidgning i halvplanet $\mathrm{Re}(s) > 0$. Fördelen med denna metod kommer vi att se när vi diskuterar zetafunktionens tillväxt nära linjen $\mathrm{Re}(s) = 1$, vilket är något vi kommer att behöva längre fram. Den generella idén är att jämföra summan $\sum_{n=1}^{\infty} 1/n^s$ med integralen $\int_1^{\infty} 1/x^s \, \mathrm{d}x$.

Proposition 4.15. *Det existerar en sekvens av hela funktioner* $\{f_n\}_{n=1}^{\infty}$ *som uppfyller uppskattningen* $|f_n(s)| \leq |s|/n^{\sigma+1}$ *där* $s = \sigma + it$*, och sådana att*

$$\sum_{1 \leq n < N} \frac{1}{n^s} - \int_1^N \frac{\mathrm{d}x}{x^s} = \sum_{1 \leq n < N} f_n(s) \,, \quad \textit{för alla } N \in \mathbb{N}\backslash\{1\} \,. \tag{4.15}$$

Denna proposition ger oss följande följdsats.

Följdsats 4.16. *För* $\mathrm{Re}(s) > 0$ *gäller att*

$$\zeta(s) - \frac{1}{s-1} = H(s) \,, \tag{4.16}$$

där $H(s) = \sum_{n=1}^{\infty} f_n(s)$ *är en holomorf funktion i halvplanet* $\mathrm{Re}(s) > 0$*, med* $\{f_n\}$ *som i Proposition 4.15.*

Bevis av Proposition 4.15. Vi börjar med att jämföra summan

$$\sum_{1 \leq n < N} 1/n^s \,,$$

med

$$\sum_{1 \leq n < N} \int_n^{n+1} 1/x^s \, \mathrm{d}x \,.$$

Låt

$$f_n(s) = \int_n^{n+1} \left[\frac{1}{n^s} - \frac{1}{x^s} \, \mathrm{d}x \right] . \tag{4.17}$$

Tillämpar vi nu medelvärdessatsen på funktionen $g(x) = 1/x^s$ får vi att

$$\left| \frac{1}{n^s} - \frac{1}{x^s} \right| \leq \frac{|s|}{n^{\sigma+1}} , \quad \text{för } n \leq x \leq n+1.$$

Detta medför att $|f_n(s)| \leq |s|/n^{\sigma+1}$, och beviset är klart. □

Bevis av följdsats 4.16. Vi börjar med att anta att $\mathrm{Re}(s) > 1$, och låter N gå mot oändligheten i (4.15). Observera att $|f_n(s)| \leq |s|/n^{\sigma+1}$ ger oss likformig konvergens av serien $\sum f_n(s)$ i varje halvplan $\mathrm{Re}(s) > \delta$ då $\delta > 0$. Eftersom $\mathrm{Re}(s) > 1$ konvergerar $\sum 1/n^s$ likformigt mot $\zeta(s)$, vilket bevisar påståendet för $\mathrm{Re}(s) > 1$. Men den likformiga konvergensen visar också att $\sum f_n(s)$ är holomorf för $\mathrm{Re}(s) > 0$, vilket därmed visar att $\zeta(s)$ går att utvidga till detta halvplan och att identiteten i (4.16) även håller här. □

Med hjälp av Proposition 4.15 kan vi visa att zetafunktionen inte växer "allt för snabbt" nära linjen $\mathrm{Re}(s) = 1$. Vi erinrar oss om att $|\zeta(s)| \leq \sum 1/n^{\sigma}$ då $\mathrm{Re}(s) > 1$, och att $\zeta(s)$ därmed är begränsad i varje halvplan $\mathrm{Re}(s) \geq 1 + \delta > 1$. Vi vänder oss nu till en proposition som säger att $|\zeta(s)|$ domineras av termen $|t|^{\varepsilon}$ för alla $\varepsilon > 0$ på linjen $\mathrm{Re}(s) = 1$, och att funktionens tillväxt nära linjen nästan är densamma.

Proposition 4.17. *Antag att* $s = \sigma + it$, $\sigma, t \in \mathbb{R}$. *Då gäller det att för varje* $\sigma_0 : 0 \leq \sigma_0 \leq 1$ *och varje* $\varepsilon > 0$ *existerar det en konstant* c_ε *sådan att*

$$\begin{aligned} &(i) \quad |\zeta(s)| \leq c_\epsilon |t|^{1-\sigma_0+\varepsilon}, \text{ då } \sigma_0 \leq \sigma \text{ och } |t| \geq 1 \\ &(ii) \quad |\zeta'(s)| \leq c_\epsilon |t|^{\varepsilon}, \text{ då } \sigma \geq 1 \text{ och } |t| \geq 1. \end{aligned}$$

Propositionen medför speciellt att $\zeta(1+it) = O(|t|^\varepsilon)$ då t går mot oändligheten, och samma uppskattning håller för ζ'.

Bevis. Vi använder oss av Proposition 4.15 där vi observerade att $|f_n(s)| \leq |s|/n^{\sigma+1}$. Dessutom har vi att $|f_n(s)| \leq 2/n^\sigma$, vilket följer av uttrycket från (4.17) och det faktum att $|1/n^s| = n^{-\sigma}$ och $|1/x^s| \leq n^{-\sigma}$ då $x \geq n$. Kombinerar vi nu dessa två uppskattningar av $|f_n(s)|$ får vi att

$$|f_n(s)| \leq \left(\frac{|s|}{n^{\sigma_0+1}}\right)^\delta \left(\frac{2}{n^{\sigma_0}}\right)^{1-\delta} \leq \frac{2|s|^\delta}{n^{\sigma_0+\delta}}, \text{ då } \delta \geq 0.$$

Välj nu $\delta = 1 - \sigma_0 + \varepsilon$ och använd identiteten från (4.16). Då har vi att

$$|\zeta(s)| \leq \left|\frac{1}{s-1}\right| + 2|s|^{1-\sigma_0+\varepsilon} \sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}} \qquad \text{då } \sigma = \mathrm{Re}(s) \geq \sigma_0,$$

vilket bevisar (i). Den andra slutsatsen visar vi genom att använda Cauchys integralformel

$$\zeta'(s) = \frac{1}{2\pi r} \int_0^{2\pi} \zeta(s + re^{i\theta}) e^{i\theta} \, \mathrm{d}\theta,$$

där vi integrerar över en cirkel med radien r centrerad kring punkten s. Väljer vi nu $r = \varepsilon$ och noterar att denna cirkel befinner sig i halvplanet $\mathrm{Re}(s) \geq 1 - \varepsilon$ så följer (ii) som en konsekvens av (i) genom att byta ut 2ε mot ε i sista steget, det vill säga

$$\begin{aligned} |\zeta'(s)| = \frac{1}{2\pi\varepsilon} \left| \int_0^{2\pi} \zeta(s + \varepsilon e^{i\theta}) e^{i\theta} \, \mathrm{d}\theta \right| &\leq \frac{1}{2\pi\varepsilon} \int_0^{2\pi} |\zeta((\sigma + \varepsilon\cos\theta) + i(t + \varepsilon \sin\theta))| \, \mathrm{d}\theta \\ &\overset{(i)}{\leq} c_{2\varepsilon} |t + \varepsilon \sin\theta|^{1-\sigma_0+\varepsilon} \leq c_\varepsilon |t|^{1-(1-\varepsilon)+\varepsilon} = c_{2\varepsilon}|t|^{2\varepsilon}. \end{aligned}$$

Vi har alltså att $|\zeta'(s)| \leq c_\varepsilon |t|^\varepsilon$. $\square$

Kapitel 5

Fourieranalys på ändliga abelska grupper

I detta kapitel kommer vi att studera Fourieranalys för funktioner definierade på så kallade ändliga abelska grupper. Denna teori kommer vi behöva bland annat för att bevisa Dirichlets sats om primtal i aritmetiska följder.

Den del av teorin som berör själva Fourieranalysen är inte speciellt invecklad. Innan vi kan formulera den måste vi dock först introducera en hel del begrepp från gruppteori, vilket kommer att uppta huvuddelen av kapitlet. Denna gruppteori kommer bland annat innefatta att definera vad en abelsk grupp är samt gå igenom begreppet karaktär, där karaktärer är huvudnyckeln för att kunna applicera Fourieranalys på ändliga abelska grupper.

5.1 Ändliga abelska grupper

En grupp G är en mängd element som tillsammans med en gruppoperator uppfyller fyra egenskaper.

Definition 5.1. *En grupp $(G, \cdot)$ där $\cdot$ betecknar gruppoperationen, definieras av följande egenskaper.*

(i) Slutenhet: Om $a, b \in G$, så gäller att $a \cdot b \in G$.

(ii) Associativitet: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ för alla a, b och c som tillhör G.

(iii) Identitetselement: Det finns ett element u som tillhör G så att $a \cdot u = u \cdot a = a$ för alla a som tillhör G.

(iv) Inverselement: För alla a som tillhör G finns det ett element a^{-1} som tillhör G, så att $a \cdot a^{-1} = a^{-1} \cdot a = u$, där u är identitetselementet.

Ett enkelt exempel på en grupp är mängden av alla heltal under addition, $(\mathbb{Z}, +)$. Denna grupp kommer uppfylla alla egenskaper i definitionen ovan.

Definition 5.2. *En grupp $(G, \cdot)$ är abelsk om även*

(v) Kommutativitet: $a \cdot b = b \cdot a$ för alla a och b som tillhör G.

Exempel på abelska grupper.

- Mängden av alla reella tal, $\mathbb{R}$, bildar en abelsk grupp under addition. Identitetselementet är 0 och inversen till a är $-a$. Dock bildar gruppen $\mathbb{R}$ inte en abelsk grupp under multiplikation, då inverselementkravet inte är uppfyllt för elementet $a = 0$.
- Enhetscirkeln S^1 i det komplexa talplanet är en abelsk grupp. Om S^1 ses som mängden av alla punkter $\{e^{i\theta}; \theta \in \mathbb{R}\}$ så är operationen vanlig multiplikation av komplexa tal.
- Gruppen $\mathbb{Z}(N)$, bestående av de N:te enhetsrötterna, är en abelsk grupp under multiplikation av komplexa tal, vilket vi kommer visa tydligare senare.

För funktioner mellan grupper har vi de viktiga begreppen homomorfism och isomorfism.

Definition 5.3. *Låt G och H vara två grupper och låt $f : G \to H$. Avbildningen f kallas för en homomorfism om*

$$f(a \cdot b) = f(a) \cdot f(b), \text{ för alla } a, b \in G.$$

Här är operationen i vänsterledet operationen från gruppen G, och operationen i högerledet är operationen från gruppen H.

Definition 5.4. *Avbildningen $f : G \to H$ kallas för en isomorfism om den är en bijektiv homomorfism. Detta innebär att det existerar $\tilde{f} : H \to G$ så att*

$$(\tilde{f} \circ f)(a) = a \text{ och } (f \circ \tilde{f})(b) = b, \text{ för alla } a \in G \text{ och } b \in H.$$

Vi kallar två grupper G och H för isomorfa om det existerar en isomorfism mellan dem, och betecknar detta $G \approx H$. Man kan säga att två isomorfa grupper i grund och botten beskriver samma typ av objekt, men att de skiljer sig åt i representation, det vill säga att man har två olika mängder med två olika operationer som har samma egenskaper.

Exempel. Exponentialfunktionen $f = e^x$ avbildar alla reella tal på alla positiva reella tal, det vill säga $f : \mathbb{R} \to \mathbb{R}^+$. Vi ser att f är en homomorfism om $(\mathbb{R}, +)$ är en abelsk grupp under addition och $(\mathbb{R}^+, \cdot)$ under multiplikation. Det finns en invers homomorfism till exponentialfunktionen, nämligen logarimen $\tilde{f} = \ln x$, där $\tilde{f} : \mathbb{R}^+ \to \mathbb{R}$. Från definitionerna ovan ser vi att f är en isomorfism, vilket innebär att grupperna $\mathbb{R}$ och $\mathbb{R}^+$ är isomorfa, det vill säga $(\mathbb{R}, +) \approx (\mathbb{R}^+, \cdot)$.

Vi kommer främst att behandla ändliga abelska grupper där vi betecknar antalet element i en sådan grupp med $|G|$, och kallar detta tal för gruppens ordning. Exempelvis har gruppen $\mathbb{Z}(N)$ ordningen N.

5.2 Gruppen $\mathbb{Z}(N)$

Vi går nu vidare med att studera en av de enklaste abelska grupperna, $\mathbb{Z}(N)$. Denna grupp kan definieras på två olika sätt, dels som mängden av de N:te enhetsrötterna, och dels som mängden av heltal modulo N. Här lämpar sig det första fallet bättre för komplexanalys, medan det andra fallet passar bättre vid talteori. Gruppen är viktig för den diskreta Fouriertransformen, och i det här avsnittet kommer vi att definiera och studera båda dessa sätt att betrakta $\mathbb{Z}(N)$.

För att kunna studera det andra sättet behöver vi definiera begreppet kongruens.

Definition 5.5. *Två heltal x och y är kongruenta modulo N om skillnaden mellan dem är en heltalsmultipel av N, det vill säga om x-y är delbart med N. Vi skriver detta som $x \equiv y \bmod N$.*

5.2.1 Gruppen $\mathbb{Z}(N)$ som mängden av N:te enhetsrötter

Vi börjar med att definiera gruppen $\mathbb{Z}(N)$ som alla komplexa tal z som är N:te enhetsrötter, där N är ett heltal. Dessa enhetsrötter är jämt fördelade på enhetscirkeln och när N går mot oändligheten kommer $\mathbb{Z}(N)$ täcka hela enhetscirkeln. Med andra ord är $\mathbb{Z}(N)$ alla tal sådana att $z^N = 1$, och på polär form har vi att

$$\mathbb{Z}(N) = \left\{1, e^{2\pi i/N}, e^{2\pi i2/N}, ..., e^{2\pi i(N-1)/N}\right\} .$$

Om vi låter $\zeta = e^{2\pi i/N}$ kan varje element i $\mathbb{Z}(N)$ skrivas på formen ζ^k där k är ett heltal. För $k = N$ gäller det att $\zeta^N = 1$, vilket ger att

$$\zeta^m = \zeta^n \quad \text{om och endast om } n - m \text{ är delbart med } N .$$

Man kan enkelt visa att $\mathbb{Z}(N)$ är en abelsk grupp under komplex multiplikation utifrån Definition 5.1 och 5.2.

Exempel. Vi vill nu visa ett exempel för att få en känsla för hur grupper fungerar. Vi har att

$$\mathbb{Z}(3) = \{1, e^{2\pi i/3}, e^{4\pi i/3}\} .$$

Vi börjar med att räkna ut den multiplikativa tabellen för gruppen genom att applicera gruppoperationen på varje kombination av elementen i gruppen. Till exempel för $e^{4\pi i/3}$ multiplicerat med $e^{4\pi i/3}$ får vi $e^{8\pi i/3}$, och tar vi sedan bort en period $2\pi i$ landar vi på $e^{2\pi i/3}$, som är en del av mängden $\mathbb{Z}(3)$.

$(\mathbb{Z}(3), \cdot)$	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
1	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
$e^{2\pi i/3}$	$e^{2\pi i/3}$	$e^{4\pi i/3}$	1
$e^{4\pi i/3}$	$e^{4\pi i/3}$	1	$e^{2\pi i/3}$

Tabell 5.1: *Multiplikativ tabell för $\mathbb{Z}(3)$.*

Från Tabell 5.1 kan vi se att $\mathbb{Z}(3)$ är sluten under multiplikation, eftersom oavsett vilken kombination av element från gruppen vi opererar på kommer vi alltid att vara kvar i gruppen.

5.2.2 Gruppen $\mathbb{Z}(N)$ som mängden av heltal modulo N

Denna definition av $\mathbb{Z}(N)$ är som nämnts gruppen av heltal modulo N och vi kommer hädanefter beteckna denna grupp som $\mathbb{Z}/N\mathbb{Z}$, uttalas $\mathbb{Z}$ mod N. Lite enklare beskrivet består gruppen av alla heltal mellan 0 och $N - 1$ med addition som gruppoperation, alltså

$$\mathbb{Z}/N\mathbb{Z} = \{0, 1, 2, \ldots, N - 1\} .$$

Vi ser här att om vi tar ett tal större än $N - 1$ och tar modulo N kommer vi hamna på ett tal mellan just 0 och $N-1$, vilket alltså ger att gruppen är sluten under addition av heltal modulo N. Man kan visa att denna grupp också är en abelsk grupp genom att visa egenskaperna $(i) - (v)$ i Definition 5.1 och 5.2. Man får att 0 är indentitetselementet och att inversen till a är $-a$ mod N, för alla $a \in \mathbb{Z}/N\mathbb{Z}$.

Exempel. På liknande sätt som exemplet för $\mathbb{Z}(3)$ vill vi nu studera gruppen $\mathbb{Z}/3\mathbb{Z}$. Vi har att

$$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}\,.$$

Denna grupp är abelsk under addition av heltal modulo 3 och Tabell 5.2 visar dess additiva tabell. Här har vi till exempel att $2+2=4$ och då $4 \equiv 1 \bmod 3$ får vi alltså att $2+2=1$ i $\mathbb{Z}/3\mathbb{Z}$.

$(\mathbb{Z}/3\mathbb{Z}, +)$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabell 5.2: Additiv tabell för $\mathbb{Z}/3\mathbb{Z}$.

Om vi betraktar den multiplikativa tabellen för $\mathbb{Z}(3)$, Tabell 5.1, och den additiva tabellen för $\mathbb{Z}/3\mathbb{Z}$, Tabell 5.2, ser vi att det finns en del likheter i strukturen. Det första elementet i båda grupperna befinner sig på samma plats i båda tabellerna. Samma sak gäller även för andra och tredje elementet i grupperna. Vi ser alltså att dessa två grupper med helt olika mängder och helt olika operationer faktiskt beskriver samma sak. Det är just detta som en isomorfism mellan två grupper innebär och slutsatsen blir alltså att $\mathbb{Z}(3)$ och $\mathbb{Z}/3\mathbb{Z}$ är isomorfa. Det visar sig att detta även gäller för ett godtyckligt heltal N. Isomorfismen ges av

$$k \longleftrightarrow e^{2\pi i k/N}\,. \tag{5.1}$$

Hädanefter betecknar vi både gruppen av heltal modulo N och gruppen av N:te enhetsrötter som $\mathbb{Z}(N)$.

Vi vänder oss nu till ett annat exempel på en ändlig abelsk grupp. Denna kommer att vara viktigt för beviset av Dirichlets sats.

5.3 Gruppen $\mathbb{Z}^*(q)$

Vi skall här definiera vad vi menar med gruppen $\mathbb{Z}^*(q)$, men dessförinnan går vi igenom ytterligare ett begrepp som vi behöver i vår arsenal, nämligen enhet.

Definition 5.6. *Låt q vara ett positivt heltal. Ett heltal $n \in \mathbb{Z}(q)$ kallas för en enhet om det existerar ett heltal $m \in \mathbb{Z}(q)$ sådant att $nm \equiv 1 \bmod q$.*

Vi låter $\mathbb{Z}^*(q)$ beteckna mängden av alla enheter i $\mathbb{Z}(q)$. Det är inte svårt att visa att $\mathbb{Z}^*(q)$ är en abelsk grupp med operationen multiplikation modulo q. Man kan även visa att elementen i $\mathbb{Z}^*(q)$ är precis de element som är relativt prima q, det vill säga att största gemensamma delaren mellan elementen och q är 1.

Exempel. Gruppen som bildas av enheterna i $\mathbb{Z}(4) = \{0, 1, 2, 3\}$ är $\mathbb{Z}^*(4) = \{1, 3\}$. Om vi betraktar avbildningen mellan $\mathbb{Z}^*(4)$ och $\mathbb{Z}(2)$, som ges av

$$\begin{array}{ccc} \mathbb{Z}^*(4) & & \mathbb{Z}(2) \\ 1 & \longleftrightarrow & 0 \\ 3 & \longleftrightarrow & 1\,, \end{array}$$

är det inte svårt att visa att multiplikation i $\mathbb{Z}^*(4)$ är samma sak som addition i $\mathbb{Z}(2)$. Alltså har vi att $\mathbb{Z}^*(4) \approx \mathbb{Z}(2)$. Detta kan även ses från deras multiplikativa respektive additiva tabeller som i exemplet för $\mathbb{Z}(3)$.

5.4 Karaktärer

För att kunna applicera Fourieranalys på ändliga abelska grupper spelar karaktärer en viktig roll och vi börjar med att definiera vad en karaktär är.

Definition 5.7. *Låt S^1 beteckna enhetscirkeln i $\mathbb{C}$ och låt $(G, \cdot)$ vara en ändlig abelsk grupp. Då är en karaktär på G en komplexvärd funktion $e : G \to S^1$ som uppfyller*

$$e(a \cdot b) = e(a)e(b)\,, \text{ för alla } a, b \in G\,, \tag{5.2}$$

där operationen i vänsterledet är operationen i gruppen G och operationen i högerledet är operationen för S^1, vilken är multiplikation.

Med andra ord är en karaktär e en homomorfism från G till enhetscirkeln S^1. Vi kommer strax se att karaktärer spelar samma roll för Fourieranalys på ändliga abelska grupper, som $\{e^{2\pi inx}\}$ inom "vanlig" Fourieranalys.

Definition 5.8. *Den triviala karaktären, också kallad enhetskaraktären, definieras enligt*

$$e(a) := 1\,, \text{ för alla } a \in G\,.$$

Låt nu $\hat{G}$ beteckna mängden av alla karaktärer i G. Då kommer gruppen av karaktärer också att bilda en abelsk grupp. Vi formulerar detta i följande lemma.

Lemma 5.1. *Mängden $(\hat{G}, \cdot)$ är en abelsk grupp definierad av*

$$(e_1 \cdot e_2)(a) = e_1(a)e_2(a)\,, \text{ för alla } a \in G\,.$$

Vi kallar $\hat{G}$ för den duala gruppen av G. Att hitta karaktärerna för en specifik grupp är i allmänhet inte lätt. Här är ett par exempel.

Exempel. Man kan visa att karaktärerna på $\mathbb{R}$ ges av

$$e_\xi(x) = e^{2\pi i\xi x}\,, \quad \text{där } \xi \in \mathbb{R}\,.$$

Eftersom vi tidigare har konstaterat att $e^x : \mathbb{R} \to \mathbb{R}^+$ är en isomorfism får vi från karaktärerna på $\mathbb{R}$ att karaktärerna på $\mathbb{R}^+$ ges av

$$e_\xi(x) = x^{2\pi i\xi} = e^{2\pi i\xi \log x}\,, \quad \text{där } \xi \in \mathbb{R}\,.$$

Exempel. Man kan visa att karaktärerna på $\mathbb{Z}(N)$ är av formen

$$e_n(k) = \zeta_N^{nk} = e^{2\pi ink/N}\,, \quad \zeta_N = e^{2\pi i/N}\,,$$

där $n \in \{0, \dots, N-1\}$.

Nu ska vi se att det räcker att karaktärerna e avbildas från gruppen G till det komplexa talplanet istället för till enhetscirkeln.

Lemma 5.2. *Låt G vara en ändlig abelsk grupp och $e : G \to \mathbb{C}\backslash\{0\}$ en homomorfism. Då är e en karaktär.*

Bevis. Att en funktion e är en karaktär innebär att den avbildas på enhetscirkeln, vilket i sin tur innebär att normen måste vara 1. Vi börjar med att konstatera att eftersom G är ändlig kommer $|e(a)|$ ha en övre och nedre begränsning då a varierar i G. Vidare ser vi att

$$|e(b^n)| = |e(b)|^n .$$

Då detta ska vara begränsat för alla $b \in G$ måste $|e(b)| = 1$, vilket ger att e avbildas till enhetscirkeln och enligt definitionen måste e vara en karaktär. □

5.4.1 Ortogonalitet hos karaktärer

Vi vill nu visa att karaktärer $e : G \to S^1$ utgör en ortonormerad bas till V, där V är vektorrummet av alla komplexvärda funktioner på G och där $\dim(V) = |G|$. Man kan göra detta på flera sätt. Ett sätt är att först visa att karaktärerna är ortonormala och därefter visa att $|\hat{G}| = |G|$, det vill säga att de spänner upp hela vektorrummet. Ett annat sätt är att hitta en bas till vektorrummet och därefter visa att basvektorerna är homomorfismer, vilket medför att vektorerna måste vara karaktärerna. Det är den senare bevisidén vi kommer att använda oss av.

Vi börjar med följande lemma.

Lemma 5.3. *Om e inte är enhetskaraktären till en ändlig abelsk grupp G gäller att*

$$\sum_{a \in G} e(a) = 0 .$$

Bevis. Välj $b \in G$ sådant att $e(b) \neq 1$. Eftersom e är en karaktär får vi att

$$e(b) \sum_{a \in G} e(a) = \sum_{a \in G} e(b)e(a) = \sum_{a \in G} e(ab) = \sum_{a \in G} e(a) .$$

Den sista likheten gäller för att då a går igenom alla element i G kommer också ab att gå igenom alla element i G. Detta ger att

$$(e(b) - 1) \sum_{a \in G} e(a) = 0 ,$$

och då $e(b) \neq 1$ får vi att $\sum_{a \in G} e(a) = 0$. □

Vi är nu redo att visa att karaktärerna är ortonormala.

Sats 5.4. *Karaktärerna till G är ortonormala med avseende på den inre produkten*

$$(f, g) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)} , \quad \text{där } f, g \in V. \tag{5.3}$$

Bevis. Vi vill visa att

$$(e, e') = \begin{cases} 1 \text{ om } e = e' \\ 0 \text{ om } e \neq e' \end{cases} . \tag{5.4}$$

För fallet då $e = e'$ får vi att

$$(e, e) = \frac{1}{|G|} \sum_{a \in G} e(a)\overline{e(a)} = \frac{1}{|G|} \sum_{a \in G} |e(a)|^2 = 1 ,$$

där sista likheten kommer av att normen av alla karaktärer är 1 då de avbildas på enhetscirkeln. För fallet då $e \neq e'$ har vi att

$$(e, e') = \frac{1}{|G|} \sum_{a \in G} e(a)\overline{e'(a)} = \frac{1}{|G|} \sum_{a \in G} e(a)(e'(a))^{-1} = \frac{1}{|G|} \sum_{a \in G} (e(e')^{-1})(a)\,,$$

där den andra likheten följer av att $1 = |e'(a)|^2 = e'(a)\overline{e'(a)}$. Då $e \neq e'$ får vi att $e(e')^{-1}$ ej är enhetskaraktären. Därför kan vi använda oss av Lemma 5.3 som säger att den sista summan är lika med noll, vilket ger att $(e\,,e') = 0$. $\square$

Vi har nu visat att karaktärerna är ortonormala och därmed linjärt oberoende. Vi ska nu visa att karaktärerna utgör en bas.

Sats 5.5. *Karaktärerna till en ändlig abelsk grupp G utgör en bas i vektorrummet av funktioner på G.*

Innan vi går igenom beviset behöver vi införa ett par begrepp. Antag att V är ett vektorrum av dimension d med den inre produkten $(\cdot, \cdot)$. En linjär transformation $T : V \to V$ kallas för unitär om den bevarar den inre produkten. Med andra ord kallas transformationen unitär om $(Tv, Tw) = (v, w)$ för alla $v, w \in V$. Från spektralsatsen i linjär algebra får vi att unitära transformer är diagonaliserbara. Vad detta betyder är att det existerar en bas $\{v_1, \ldots, v_d\}$ för V sådan att $T(v_i) = \lambda_i v_i$, där $\lambda_i \in \mathbb{C}$ är ett egenvärde till egenvektorn v_i.

Vi presenterar nu ett lemma som kommer hjälpa oss med beviset.

Lemma 5.6. *Antag att $\{T_1, \ldots, T_k\}$ är en kommuterande familj av unitära transformer på det ändligt dimensionella inre produkt-rummet V. Med andra ord är*

$$T_i T_j = T_j T_i\,, \quad \textit{för alla } i, j\,.$$

Då gäller att $T_1, \ldots, T_k$ är simultant diagonaliserbara. Det vill säga, det existerar en bas för V som består av egenvektorer för alla T_i, $i = 1, \ldots, k$.

Bevis. Vi visar detta med hjälp av induktion. Fallet då $k = 1$ är spektralsatsen. Antag att lemmat håller för alla familjer av $k - 1$ kommuterande unitära transformer. Vi applicerar spektralsatsen på T_k, vilken ger oss att V är en direkt summa av sina egenrum,

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}\,,$$

där V_{λ_i} betecknar delrummet av alla egenvektorer med egenvärde λ_i. Vi hävdar att varje T_j, $j = 1, \ldots, k - 1$ avbildar varje egenrum V_{λ_i} på sig själv. Om $v \in V_{\lambda_i}$ och $1 \leq j \leq k - 1$ så ser vi att

$$T_k T_j(v) = T_j T_k(v) = T_j(\lambda_i v) = \lambda_i T_j(v)\,,$$

vilket innebär att $T_j(v) \in V_{\lambda_i}$. Vidare ser vi att om vi begränsar $T_1, \ldots, T_{k-1}$ till V_{λ_i} så bildar de en kommuterande unitär linjärtransformation, och då får vi från induktionsantagandet att dessa är simultant diagonaliserbara på varje delrum V_{λ_i}. Denna diagonalisering ger oss den önskade basen för varje V_{λ_i}, och på så sätt även för V. $\square$

Bevis av Sats 5.5. Vi erinrar oss själva om att vektorrummet $V = \{f : G \to \mathbb{C}\}$ är av dimension $|G|$. För varje $a \in G$ definierar vi således en linjärtransformation $T_a : V \to V$ enligt

$$(T_a f)(x) = f(a \cdot x) \qquad \text{för } x \in G.$$

Eftersom G är abelsk följer att $T_aT_b = T_bT_a$ för alla $a, b \in G$. Vidare kan man även visa att T_a är unitär med avseende på den inre produkten (5.3). Vi anropar nu Lemma 5.6, vilken ger oss att familjen $\{T_a\}_{a\in G}$ är simultant diagonaliserbar. Med andra ord existerar det en bas $\{v_b(x)\}_{b\in G}$ för V sådan att varje $v_b(x)$ är en egenfunktion för T_a för alla $a \in G$. Vi låter nu v vara en av dessa baselement och 1 vara enhetselementet i G. Vi har att $v(1) \neq 0$ ty annars är

$$v(a) = v(a \cdot 1) = (T_a v)(1) = \lambda_a v(1) = 0\,,$$

där λ_a är egenvärdet till v för T_a. Alltså är $v = 0$, vilket är en motsägelse. Vi hävdar vidare att funktionen som definieras av $w(x) = \lambda_x = v(x)/v(1)$ är en karaktär till G. Med samma argument som för v ovan ser vi att $w(x) \neq 0$ för alla x. Vidare får vi att

$$w(a \cdot b) = \frac{v(a \cdot b)}{v(1)} = \frac{\lambda_a v(b)}{v(1)} = \lambda_a\lambda_b = w(a)w(b)\,.$$

Enligt Lemma 5.2 är beviset således klart. □

5.5 Fouriers inversionssats och Plancherels sats

Vi har visat att karaktärerna till en ändlig abelsk grupp G utgör en bas för vektorrummet V av alla komplexvärda funktioner på G. Härmed har vi allt som krävs för att kunna utföra Fourieranalys på funktionerna i V.

Låt f var en funktion i V. Eftersom karaktärerna formar en bas vet vi att f kan skrivas som en linjärkombination av karaktärerna,

$$f = \sum_{e\in\hat{G}} c_e e\,, \tag{5.5}$$

för några konstanter c_e. För att få fram dessa konstanter använder vi oss av att vi vet att karaktärerna är en ortonormal familj. Detta innebär att den inre produkten av två karaktärer antingen är ett eller noll, som vi ser i ekvation (5.4). Tar vi skalärprodukt med karaktären e' på båda sidor i ekvation (5.5) får vi att

$$(f, e') = \sum_{e\in\hat{G}} c_e(e, e') = c_{e_1}(e_1, e') + c_{e_2}(e_2, e') + \ldots + c_{e'}(e', e') + \ldots = c_{e'}\,.$$

Den sista likheten kommer från ortonormaliteten där det bara finns ett fall då $e_i = e'$ i summan, resten av termerna i summan blir då noll. Vi har nu fått fram koefficienterna $c_e = (f, e)$ och detta definierar vi som Fourierkoefficienterna av f med avseende på e.

Definition 5.9. *Givet en funktion $f \in V$ och en karaktär e på G definierar vi Fourierkoefficienten av f med avseende på e som*

$$\hat{f}(e) = (f, e) = \frac{1}{|G|}\sum_{a\in G} f(a)\overline{e(a)}\,.$$

Vi sammanfattar nu räkningarna ovan som Fouriers inversionssats.

Sats 5.7 (Fouriers inversionssats)**.** *För alla funktionern $f \in V$ gäller att*

$$f = \sum_{e\in\hat{G}} \hat{f}(e)e\,.$$

Vi kan nu visa Plancherels sats.

Sats 5.8 (Plancherels sats)**.** *För alla $f \in V$ gäller att*

$$||f||^2 = (f, f) = \sum_{e \in \hat{G}} |\hat{f}(e)|^2 .$$

Bevis. Eftersom karaktärerna i G utgör en ortonormal bas i vektorrummet V, och $(f, e) = \hat{f}(e)$, får vi genom att först använda Fouriers inversionssats och sedan den inre produkten från (5.3) att

$$\|f\|^2 = (f, f) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{f(a)} = \frac{1}{|G|} \sum_{a \in G} f(a) \sum_{e \in \hat{G}} \overline{\hat{f}(e)}\overline{e(a)} =$$
$$= \frac{1}{|G|} \sum_{a \in G} \left(\sum_{e \in \hat{G}} f(a)\overline{e(a)} \right) \overline{\hat{f}(e)} = \frac{|G|}{|G|} \sum_{a \in G} (f,e)\overline{\hat{f}(e)} = \sum_{e \in \hat{G}} |\hat{f}(e)|^2 .$$

□

Vi avslutar detta kapitel med att applicera dessa två satser på gruppen $\mathbb{Z}(N)$ och vi kommer att se att detta resulterar i den "vanliga" diskreta Fouriertransformen.

5.5.1 Fouriers inversionssats och Plancherels indentitet på $\mathbb{Z}(N)$

Eftersom vi redan har konstaterat att $\mathbb{Z}(N)$ är en abelsk grupp kan vi därmed applicera Fourieranalys på gruppen. Vi vet från grundläggande kurser i Fourieranalys att inversionssatsen för $\mathbb{Z}(N)$ ser ut som

$$f(k) = \sum_{n=0}^{N-1} a_n e^{2\pi i nk/N} , \tag{5.6}$$

där konstanterna a_n ges av

$$a_n = \frac{1}{N} \sum_{k=0}^{N-1} f(k) e^{-2\pi i kn/N} . \tag{5.7}$$

Detta kan man härleda på liknande sätt som det generella fallet ovan. Vi ska nu se att vi enklare kan komma fram till samma formler genom att använda oss av den generella inversionsformeln med $G = \mathbb{Z}(N)$. Vi har tidigare konstaterat att karaktärerna på $\mathbb{Z}(N)$ ges av $e_n(k) = e^{2\pi i nk/N}$ där $n \in \{0, N-1\}$. Eftersom vi vet att $|\hat{G}| = |G|$, och att $|\mathbb{Z}(N)| = N$ får vi att även antalet karaktärer är N stycken.

Lägger vi in karaktärerna i ekvationen från Sats 5.7 får vi

$$f(k) = \sum_{e \in \hat{G}} \hat{f}(e) e(k) = \sum_{n=0}^{N-1} a_n e^{2\pi i nk/N} ,$$

där $a_n = \hat{f}(e)$ är Fourierkoefficienten. Enligt Definition 5.9 gäller att

$$a_n = \hat{f}(e) = (f, e) = \frac{1}{N} \sum_{k=0}^{N-1} f(k)\overline{e(k)} = \frac{1}{N} f(k) e^{-2\pi i nk/N} ,$$

vilket ger oss Fouriers inversionssats på $\mathbb{Z}(N)$.

Även Plancherels identitet på $\mathbb{Z}(N)$ kan fås från den generella formeln. På $\mathbb{Z}(N)$ ser identiteten ut som

$$\frac{1}{N}\sum_{k=0}^{N-1}|f(k)|^2=\sum_{n=0}^{N-1}|a_n|^2\,.$$

Även denna formel kan härledas på liknande sätt som i det generella fallet. För att visa att vi istället kan använda oss av den generella formeln börjar vi med att observera att vänsterledet kan skrivas om med hjälp av den inre produkten (5.3) enligt

$$\|f\|^2=(f,f)=\frac{1}{N}\sum_{k=0}^{N-1}f(k)\overline{f(k)}=\frac{1}{N}\sum_{k=0}^{N-1}|f(k)|^2\,.$$

Vidare kan vi använda Plancherels sats från Sats 5.8 och får att

$$\|f\|^2=\sum_{e\in\hat{G}}|\hat{f}(e)|^2=\sum_{n=0}^{N-1}|\hat{f}(e)|^2=\sum_{n=0}^{N-1}|a_n|^2\,,$$

vilket ger oss identiteten på $\mathbb{Z}(N)$.

Vi har nu lyckats visa att det är betydligt enklare att använda den generella formeln för Fourieranalys på ändliga abelska grupper på en specifik grupp, nämligen $\mathbb{Z}(N)$, än att härleda allt från början. Det faktum att det är enkelt att applicera Fourieranalys på ändliga abelska grupper är det som gör teorin användbar, vilket vi bland annat även kommer att se senare i beviset av Dirichlets sats.

Kapitel 6

Elliptiska funktioner

En elliptisk funktion är en meromorf funktion med två linjärt oberoende komplexa perioder ω_1 och ω_2, det vill säga att $f(z+\omega_1) = f(z)$, och $f(z+\omega_2) = f(z)$. Begreppet elliptisk funktion introducerades på 1800-talet av den norske matematikern Niels Henrik Abel, som inversen till en elliptisk integral. En elliptisk integral är en integral på formen

$$\int \mathrm{R}(x,\sqrt{P(x)})\,\mathrm{d}x, \tag{6.1}$$

där R betecknar ett rationellt uttryck, och $P(x)$ är ett polynom av grad 3 eller 4. Anledningen till att dessa integraler kallas för elliptiska integraler är av historiska skäl, då integraler på denna form uppstod när man försökte beräkna omkretsen på ellipser med hjälp av integralkalkyl. Som bekant kan man räkna ut längden av en i planet parametriserad kurva $r(t) = (x(t),y(t))$ med hjälp av integralen

$$\int_{t_0}^{t_1} \sqrt{(x'(t))^2 + (y'(t))^2}\,\mathrm{d}t.$$

En ellips med halvaxellängderna a och b parametriseras som $x(\theta) = a\cos\theta$, $y(t) = b\sin\theta$. Bågens längd från ett argument θ_0 till ett annat θ_1 ges då utav integralen

$$\int_{\theta_0}^{\theta_1} \sqrt{a^2\sin^2\theta + b^2\cos^2\theta}\,\mathrm{d}\theta,$$

som efter variabelbytet $x = a\cos\theta$ och under antagandet att $b > a$ ger oss integralen

$$\int_{x_0}^{x_1} \sqrt{\frac{a^2}{a^2-x^2} + (b^2-a^2)}\,\mathrm{d}x.$$

Som kuriosa kan vi notera att om $b = a = r$, det vill säga att vår ellips är en cirkel med radien r, så är integralen analytiskt lösbar och integranden har en primitiv funktion $F(x_1) = r\arcsin(x_1/r)$. Här har vi satt $x_0 = 0$ för enkelhetens skull. I likhet med de elliptiska funktionerna har vi även här en periodisk invers till integralen, men med enbart en period, nämligen $r\sin(F/r)$. När polynomet i nämnaren blir av högre grad, som en följd av att $b \neq a$, uppstår integraler utan elementärt uttryckbara lösningar. Det är inversen till dessa lösningar som är de elliptiska funktionerna, som till skillnad från de trigonometriska och hyberboliska funktionerna har två perioder, och inte en.

Efter Abels insatser i studerandet av dessa funktioner utvecklade Carl Gustav Jacob Jacobi resultaten och introducerade thetafunktionerna, vilka kom att spela en stor roll och som vi framför allt kommer ha användning för när vi bevisar två- och fyrkvadratssatsen. Därefter var det Weierstraß som vidareutvecklade teorin och införde den elliptiska $\wp$-funktionen ($\wp$ uttalas Weierstraß-p), vilken vi huvudsakligen kommer att studera i detta kapitel. Vi kommer att snudda vid kopplingarna till talteori genom att vidare studera Eisensteinserier, som är nära sammankopplade till elliptiska funktioner. Värt att nämna är att namnet elliptisk funktion hänger kvar av ovan redogjorda historiska skäl, och syftar egentligen till vilken dubbelperiodisk funktion som helst.

6.1 Introduktion till elliptiska funktioner

I det här avsnittet kommer vi att behandla elliptiska funktioner och deras egenskaper. Vi börjar med att definiera elliptiska funktioner.

Definition 6.1. *En tvåperiodisk meromorf funktion som inte är konstant kallas en elliptisk funktion.*

Att en funktion f är tvåperiodisk innebär att det finns två komplexa tal ω_1 och ω_2 skilda från noll sådana att

$$f(z+\omega_1) = f(z) \quad \text{och} \quad f(z+\omega_2) = f(z) \quad \text{för alla } z \in \mathbb{C}\,.$$

De två perioderna ω_1 och ω_2 kan antingen vara linjärt beroende eller linjärt oberoende. Då de är linjärt beroende, det vill säga då $\omega_2/\omega_1 \in \mathbb{R}$ har vi två fall. Antingen är kvoten rationell och då är f enkelperiodisk eller så är kvoten irrationell och då är f konstant. Båda dessa fall då perioderna är linjärt beroende är ointressanta för oss, eftersom en elliptisk funktion är dubbelperiodisk och icke-konstant. Vi kommer därför att anta att ω_1 och ω_2 är linjärt oberoende, det vill säga att $\omega_2/\omega_1 \in \mathbb{C}\backslash\mathbb{R}$.

Om vi låter $\tau = \omega_2/\omega_1$ och noterar att τ och $1/\tau$ har olika tecken på sina imaginärdelar så kan vi anta att $\mathrm{Im}(\tau){>}0$. Vi observerar nu att om funktionen f har perioderna w_1 och w_2 så är detta ekvivalent med att funktionen $F(z) = f(\omega_1 z)$ har perioderna 1 och τ. Dessutom gäller att f är meromorf om och endast om F är meromorf. Utöver detta kan alla f:s egenskaper direkt appliceras på F och därför kan vi utan inskränkning anta att f är en funktion i $\mathbb{C}$ med perioderna 1 och τ, där $\mathrm{Im}(\tau) > 0$.
Tillämpar vi periodiciteten upprepade gånger får vi således att

$$f(z+n+m\tau) = f(z) \quad \text{för alla } n,m \in \mathbb{Z} \text{ och alla } z \in \mathbb{C}\,.$$

Vi ska nu konstruera ett gitter enligt

$$\Lambda = \{n + m\tau : n,m \in \mathbb{Z}\}\,.$$

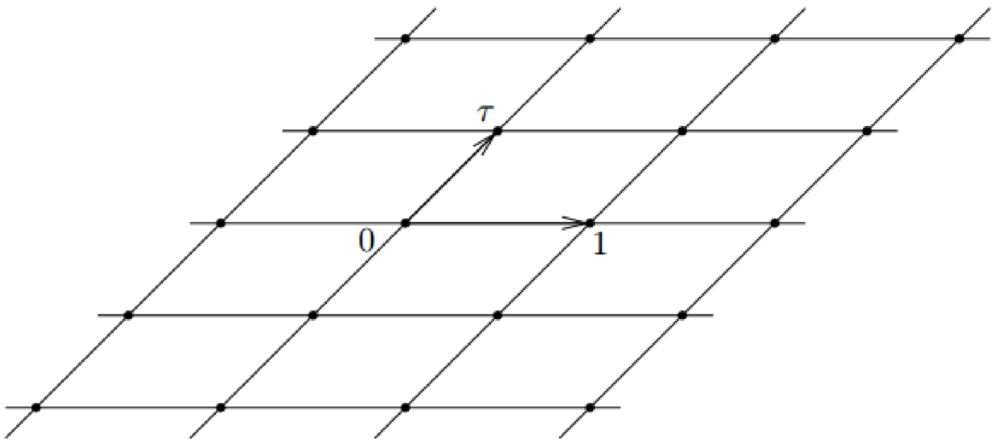
Detta gitter kan ses i Figur 6.1. Vi säger att 1 och τ genererar Λ. Vi definierar även det fundamentala parallellogrammet som

$$P_0 = \{z \in \mathbb{C} : z = a + b\tau \text{ där } 0 \le a < 1 \text{ och } 0 \le b < 1\}\,.$$

Det fundamentala parallellogrammet innefattar området mellan 0, 1, τ och $1{+}\tau$, enligt Figur 6.1. Syftet med det fundamentala parallellogrammet kommer från att man kan visa att en elliptisk funktion f med perioderna 1 och τ helt kan bestämmas utifrån dess beteende på P_0. För att se detta räcker det med att visa att varje punkt i det komplexa talplanet är kongruent med en unik punkt i P_0.

Vi får då att Λ och P_0 tillsammans täcker hela det komplexa talplanet enligt

$$\mathbb{C} = \bigcup_{n,m\in\mathbb{Z}} (n + m\tau + P_0)\,. \tag{6.2}$$



Figur 6.1: Gittret som perioderna 1 och τ genererar.

Från det fundamentala parallellogrammet kan vi definiera det periodiska parallellogrammet. Ett periodiskt parallellogram P är en translation av det fundamentala parallellogrammet, det vill säga vi definierar P som

$$P = P_0 + h \quad \text{för något } h \in \mathbb{C}\,.$$

Vi har att varje punkt i det komplexa planet är kongruent med en unik punkt i varje periodiskt parallellogram. Vi kan därmed säga att en elliptisk funktion f unikt bestäms av sitt beteende i ett periodiskt parallellogram.

Vi sammanfattar det vi hittills har gått igenom i en proposition.

Proposition 6.1. *Antag att f är en elliptisk funktion med perioderna, 1 och τ, som genererar gittret Λ. Då gäller att*

(i) varje punkt i $\mathbb{C}$ är kongruent med en unik punkt i det fundamentala parallellogrammet

(ii) varje punkt i $\mathbb{C}$ är kongruent med en unik punkt i varje givet periodiskt parallellogram

(iii) gittret Λ och P_0 täcker hela det komplexa talplanet, enligt (6.2)

(iv) funktionen f bestäms av sina värden i något periodiskt parallellogram.

6.2 Liouvilles satser

Liouvilles satser beskriver grundläggande egenskaper hos dubbelperiodiska funktioner, däribland elliptiska funktioner.

Sats 6.2. *En hel dubbelperiodisk funktion är konstant.*

Bevis. En funktion f bestäms av dess värden på P_0 och eftersom P_0 är begränsad får vi att f är begränsad på $\mathbb{C}$. Från Liouvilles sats får vi att f måste vara konstant. $\square$

Som vi nämnde tidigare är en elliptisk funktion dubbelperiodisk, meromorf och icke-konstant. Man kan visa att en sådan funktion har ett begränsat antal nollsällen och poler i ett område där polerna kan ligga på randen till området. Nästa sats handlar om antalet poler hos en elliptisk funktion. (När vi räknar antalet poler och antalet nollställen till en funktion räknar vi alltid med multiplicitet.)

Sats 6.3. *En elliptisk funktion f har totalt alltid minst två poler, räknat med multiplicitet.*

Bevis. Vi börjar med att anta att f inte har några poler på randen till det fundamentala parallellogrammet, ∂P_0. Enligt residysatsen har vi då att

$$\int_{\partial P_0} f(z)\,\mathrm{d}z = 2\pi i \sum \mathrm{Res} f\,.$$

Vi kan beräkna integralen genom att integrera längs randen enligt

$$\int_{\partial P_0} f(z)\,\mathrm{d}z = \int_0^1 f(z)\,\mathrm{d}z + \int_1^{1+\tau} f(z)\,\mathrm{d}z + \int_{1+\tau}^{\tau} f(z)\,\mathrm{d}z + \int_{\tau}^{0} f(z)\,\mathrm{d}z\,.$$

I och med periodiciteten får vi att integralerna över motstående sidor tar ut varandra. Detta ger att $\int_{\partial P_0} f(z)\,\mathrm{d}z = 0$ och enligt residysatsen måste då även $\sum \mathrm{res} f = 0$. Enligt Sats 6.2 har f minst en pol, men för att $\sum \mathrm{res}(f) = 0$ skall kunna gälla måste det då finnas minst två poler.

Om f har poler på randen, ∂P_0, så låter vi $P = h + P_0$, där $h \in \mathbb{C}$ sådan att f saknar poler på ∂P. På samma sätt som ovan kan man konstatera att f måste ha minst två poler i P. Antalet poler i P är lika med antalet poler i P_0 oavsett h. □

Definition 6.2. *Det totala antalet poler hos en elliptisk funktion kallas för funktionens ordning.*

Sats 6.4. *Varje elliptisk funktion av ordning m har m nollställen i P_0.*

Bevis. Vi börjar med att anta att f inte har några poler på randen ∂P_0. Från argumentprincipen har vi att

$$\int_{\partial P_0} \frac{f'(z)}{f(z)}\,\mathrm{d}z = 2\pi i(\mathcal{N}_\zeta - \mathcal{N}_p)\,,$$

där $\mathcal{N}_\zeta$ och $\mathcal{N}_p$ är antalet nollställen respektive antalet poler till f i P_0. Integration längs randen, ∂P_0, blir på samma sätt som i föregående sats noll, då f'/f är periodisk. Detta ger att $\mathcal{N}_\zeta = \mathcal{N}_p$, det vill säga antalet nollställen och antalet poler till f är lika många.

Om f har poler på randen till P_0 så gör vi en translation av området (som i Sats 6.3) och resonerar på samma sätt som tidigare. □

Nu har vi behandlat några egenskaper hos elliptiska funktioner men vi har ännu inte visat att en funktion som uppfyller dessa egenskaper överhuvudtaget existerar. Vårt nästa mål är att konstruera en elliptisk funktion.

6.3 Weierstraß elliptiska funktion

Weierstraß elliptiska funktion brukar betecknas med $\wp$ och visar sig vara av stor vikt då alla elliptiska funktioner kan skrivas i termer av $\wp$ och dess derivata. Detta påstående kommer att bevisas senare i detta avsnitt. Tidigare nämndes att varje sådan funktion måste ha minst två poler och vi börjar därför med att konstruera en funktion vars enda singularitet är en dubbelpol i de punkter på gittret som genereras av perioderna.

Den naturliga ansatsen vore ett uttryck på formen

$$\sum_{\omega\in\Lambda} \frac{1}{(z+\omega)^2},$$

med $\omega = (n+m\tau)$. Detta är dock en serie som inte är absolutkonvergent och vi väljer att dela upp funktionen så att summeringen inte inkluderar origo. Låt således Λ^* beteckna hela gittret utom origo, det vill säga

$$\Lambda^* = \Lambda - \{(0,0)\},$$

och betrakta

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda^*} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right],$$

där vi valt att subtrahera ut $\frac{1}{\omega^2}$ för att få summan att konvergera. Om vi utvecklar uttrycket innanför hakparenteserna får vi att

$$\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = \frac{-z^2-2z\omega}{(z+\omega)^2\omega^2},$$

som är av storleksordning $O(\frac{1}{\omega^3})$. För att visa att serien är en meromorf funktion med våra önskade poler behöver vi följande lemma.

Lemma 6.5. *Serierna*

$$\sum_{(m,n)\neq(0,0)} \frac{1}{(|n|+|m|)^r} \quad \textit{och} \quad \sum_{n+m\tau\in\Lambda^*} \frac{1}{|n+m\tau|^r},$$

konvergerar då $r > 2$.

Beviset av detta lemma är relativt långt och tekniskt, och den nödvändiga teorin hittar man i Complex Analysis av Stein & Shakarchi s. 197-199, och det faktiska beviset av lemmat finner vi på s. 268-269. Vi är nu redo att definiera Weierstraß elliptiska funktion $\wp$, den fundamentala byggstenen i teorin för elliptiska funktioner.

Definition 6.3. *Låt*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda^*} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right] = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left[\frac{1}{(z+n+m\tau)^2} - \frac{1}{(n+m\tau)^2}\right]. \tag{6.3}$$

$\wp$ kallas för Weierstraß elliptiska funktion.

För att visa att $\wp$ är en meromorf funktion med dubbelpoler i gitterpunkterna antar vi först att $|z| < R$ och skriver

$$\wp(z) = \frac{1}{z^2} + \sum_{|\omega|\le 2R} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right] + \frac{1}{z^2} + \sum_{|\omega|>2R} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right].$$

Innanför hakparenteserna i den andra summan har vi ett uttryck som är av storleksordning $O(\frac{1}{|\omega|^3})$ då $|z| < R$, vilket ger att hela summan är holomorf enligt Lemma 6.5. Vi har även att den första summan har dubbelpoler i gitterpunkterna på disken $|z| < R$.

Det återstår att visa att $\wp$ är dubbelperiodisk.

Sats 6.6. *$\wp$ är en elliptisk funktion med perioderna 1 och τ, och har dubbelpoler vid gitterpunkterna.*

Bevis. Om vi deriverar $\wp$ i (6.3) termvis får vi att

$$\wp'(z) = \frac{-2}{z^3} - 2 \sum_{(n,m)\neq(0,0)} \frac{1}{(z+n+m\tau)^3} = -2 \sum_{(n,m)\in\mathbb{Z}} \frac{1}{(z+n+m\tau)^3} \,.$$

Från Lemma 6.5 får vi att serien ovan är absolutkonvergent när z inte är en av gitterpunkterna. Vi ser även att deriveringen eliminerar termen $-1/\omega^2$ vilket ger att $\wp'$ inte ändras när vi ersätter z med $z+1$ och $z+\tau$. Detta ger att $\wp'$ är periodisk med perioderna 1 och τ och det finns två konstanter a och b sådana att

$$\wp(z+1) = \wp(z) + a \quad \text{och} \quad \wp(z+\tau) = \wp(z) + b \,. \tag{6.4}$$

Från definitionen av $\wp$ i (6.3) ser vi att $\wp$ är en jämn funktion. Detta fås av att serien har kvadratiska termer i nämnaren vilket gör att när vi ersätter z med $-z$ får vi att summan över $\omega \in \Lambda^*$ kan ersättas med summan över $-\omega \in \Lambda^*$. Vi kan alltså skriva $\wp(-z) = \wp(z)$ och får att

$$\wp(-1/2) = \wp(1/2) \quad \text{och} \quad \wp(-\tau/2) = \wp(\tau/2) \,.$$

Om vi sätter in uttrycken ovan i ekvation (6.4) får vi att $a = b = 0$, vilket ger att $\wp$ är dubbelperiodisk med perioderna 1 och τ. $\square$

6.4 Egenskaper för $\wp$

Tidigare så har vi konstaterat att $\wp$ är en jämn funktion vilket ger att $\wp'$ är en udda funktion. Vi vet även att $\wp'$ är periodisk med 1 och τ. Exempelvis gäller det för $z = 1/2$ att

$$\wp'(1/2) = -\wp'(-1/2) = -\wp'(-1/2+1) = -\wp'(1/2) \,,$$

vilket ger att $\wp'(1/2) = 0$. Samma gäller för $\wp'(\tau/2)$ och för $\wp'((1+\tau)/2)$ och vi får att

$$\wp'(1/2) = \wp'(\tau/2) = \wp'\left(\frac{1+\tau}{2}\right) = 0 \,,$$

där dessa tre punkter kallas för halvperioder. Eftersom $\wp'$ är elliptisk med ordning 3 är de tre punkterna de enda rötterna till $\wp$ i det fundamentala parallelogrammet och de har multiplicitet 1. Vi kan definiera punkterna som

$$\wp(1/2) = e_1, \quad \wp(\tau/2) = e_2 \quad \text{och} \quad \wp\left(\frac{1+\tau}{2}\right) = e_3 \,,$$

där ekvationen $\wp(z) = e_1$ har en dubbelrot i $1/2$. Eftersom $\wp$ har ordning 2 så finns det inga andra lösningar till $\wp(z) = e_1$ i det fundamentala parallelogrammet. På samma sätt får vi att ekvationerna $\wp(z) = e_2$ och $\wp(z) = e_3$ endast har dubbelrötter vid $1/2$ respektive $\tau/2$. Vi observerar att e_1, e_2 och e_3 är distinkta eftersom annars skulle $\wp$ ha fyra rötter i det fundamentala parallelogrammet, vilket motsäger att $\wp$ har ordning 2. Från detta kan vi nu bevisa följande sats.

Sats 6.7. *Funktionen $(\wp')^2$ är det kubiska polynomet i $\wp$*

$$(\wp')^2(z) = (\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3) \,.$$

Bevis. Låt $F(z) = (\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$. Som vi visade tidigare ges de enda lösningarna till ekvationerna $\wp(z) = e_1$, $\wp(z) = e_2$ och $\wp(z) = e_3$ i det fundamentala parallelogrammet av $1/2$, $\tau/2$ och $(1+\tau)/2$. Alltså ges de enda rötterna till $F(z)$ av $1/2$, $\tau/2$ och $(1+\tau)/2$ med multiplicitet 2. Men vi noterar att $\wp'$ har poler av ordning 3 i gitterpunkterna, och därför har $F(z)$ poler av ordning 6 i samma punkter. Vidare är kvoten $(\wp')^2/F$ holomorf och dubbelperiodisk, vilket ger att kvoten är konstant enligt Sats 6.2. Det återstår nu att visa att kvoten är lika med 4. Vi har för z nära origo att

$$\wp(z) = \frac{1}{z^2} + \sum \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right],$$

vilket ger att

$$\wp'(z) = -\frac{2}{z^3} + \dots .$$

Division med F ger då att kvoten är $(\wp')^2/F = 4$. □

Vi påstod tidigare att en viktig egenskap med Weierstraß elliptiska funktion $\wp$ är att varje elliptisk funktion kan skrivas i termer av $\wp$ och $\wp'$. Detta demonstreras av följande lemma och sats.

Lemma 6.8. *Varje jämn elliptisk funktion F med perioderna 1 och τ är en rationell funktion av $\wp$.*

En konsekvens av detta lemma är följande sats.

Sats 6.9. *Varje elliptisk funktion f med perioderna 1 och τ är en rationell funktion av $\wp$ och $\wp'$.*

Vi bevisar nu Lemma 6.8 ovan och ger därefter ett bevis till Sats 6.9.

Bevis. Vårt mål är att konstruera en elliptisk funktion med $\wp$ som har exakt samma nollställen och poler som F. Vi börjar med att anta att F inte har några nollställen eller poler på Λ. Detta eftersom om F har ett nollställe eller en pol i origo, så måste ordningen av nollstället eller polen vara av jämn ordning eftersom F är en jämn funktion. En konsekvens av detta är då att det finns ett heltal m sådant att $F\wp^m$ har inga nollställen eller poler i Λ. Vi försöker nu konstruera F utifrån $\wp$.

Låt $a \in \mathbb{C}$ vara en konstant. Det gäller då att $\wp(z) - \wp(a)$ har endast ett nollställe av ordning 2 om och endast om a är en halv period, annars har $\wp(z) - \wp(a)$ två distinkta nollställen i punkterna $\pm a$. Vi måste nu försöka räkna nollställena och polerna till F eftersom vår representation av F i termer av $\wp$ måste stämma överens exakt.

Om a är ett nollställe till F så är också $-a$ ett nollställe till F eftersom F är jämn. Vidare är a kongruent till $-a$ om och endast om a är en halv period, och i detta fall är a ett nollställe av jämn ordning. Det följer därför att om följden $\pm a_1, \pm a_2, \dots, \pm a_m$ medräknat multiplicitet betecknar alla nollställen till F så gäller att

$$[\wp(z) - \wp(a_1)]\dots[\wp(z) - \wp(a_m)],$$

har exakt samma rötter som F. Med liknande resonemang som ovan följer att polerna $(\pm b_1, \dots, \pm b_m)$ till F medräknat multipliciteten visar att

$$G(z) = \frac{[\wp(z) - \wp(a_1)]\dots[\wp(z) - \wp(a_m)]}{[\wp(z) - \wp(b_1)]\dots[\wp(z) - \wp(b_m)]},$$

är periodisk och har exakt samma nollställen och poler som F. Därmed bildar vi kvoten F/G som är elliptisk och holomorf, och som en konsekvens av detta följer av Sats 6.2 att F/G är konstant. Därmed följer lemmat. □

Bevis av Sats 6.9. Vi påminner om att $\wp$ är jämn och är $\wp'$ udda. Vi skriver då funktionen f som en summa av en jämn och udda funktion, det vill säga

$$f(z) = f_{\text{jämn}}(z) + f_{\text{udda}}(z) : \ f_{\text{jämn}}(z) = \frac{f(z)+f(-z)}{2}\,, \quad f_{\text{udda}}(z) = \frac{f(z)-f(-z)}{2}\,.$$

Då gäller att $f_{\text{udda}}/\wp'$ är jämn. Lemma 6.8 applicerad på $f_{\text{udda}}/\wp'$ och $f_{\text{jämn}}$ ger oss då att funktionen f kan skrivas som en rationell funktion i termer av $\wp$ och $\wp'$. $\square$

6.5 Eisensteinserier

Tidigare i detta avsnitt definierades parametern $\tau = \omega_2/\omega_1$ där ω_1 och ω_2 är perioderna till någon elliptisk funktion f, så att $\mathrm{Im}(\tau) > 0$. Vi antog sedan att de två perioderna är 1 respektive τ och konstruerade $\wp$ utifrån detta val av τ. Detta leder då till den naturliga frågan hur $\wp$ påverkas av valet av parametern τ. Vi kan alltså betrakta $\wp(z)$ som en funktion av τ, det vill säga $\wp_\tau(z)$.

Exempelvis ses att $\wp_{\tau+1}$ och $\wp_\tau$ har exakt samma perioder, och faktum är att dessa två funktioner är identiska. På ett analogt sätt kan man härleda funktionalekvationen $\wp_{-1/\tau}(z) = \tau^2\wp_\tau(\tau z)$ genom att sätta $-1/\tau = -\omega_1/\omega_2$ med $\mathrm{Im}(-1/\tau) > 0$.

Detta leder oss nu till att betrakta gruppen av transformationer av övre halvplanet av $\mathbb{C}$ som genereras av transformationerna $\tau \to \tau + 1$ och $\tau \to -1/\tau$. Denna grupp kallas för den modulära gruppen och leder oss då till att studera de så kallade Eisensteinserierna, för att få en bättre förståelse över hur dessa byten av τ påverkar $\wp(z)$.

Definition 6.4. *Eisensteinserien av ordning k definieras som*

$$E_k(\tau) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n+m\tau)^k}\,, \tag{6.5}$$

där $k \geq 3$ är ett heltal och τ är ett komplext tal med positiv imaginärdel.

Sats 6.10. *Eisensteinserier konvergerar om $k \geq 3$, och de är holomorfa i övre halvplanet. Om k är udda, är $E_k(\tau) = 0$. Eisensteinserier uppfyller följande relationer:*

$$E_k(\tau) = E_k(\tau+1) = \tau^{-k}E_k(-1/\tau)\,. \tag{6.6}$$

Bevis. Enligt Lemma 6.5 är $E_k(\tau)$ både absolut och likformigt konvergent då $k \geq 3$ så länge $\mathrm{Im}(\tau)\geq \delta > 0$, vilket gör $E_k(\tau)$ holomorf i övre halvplanet. Genom att ersätta n samt m med $-n$ respektive $-m$ ser man av symmetriskäl att $E_k(\tau)$ är identiskt 0 då k är udda. Till sist så motiverar vi Eisensteinseriernas periodicitet med följande argument: $n + (m+1)\tau = n + m + m\tau = n' + m\tau$, då n går över alla heltal, och $n + m = n'$ är ett heltal. Betrakta

$$(n + m(-1/\tau))^k = \tau^{-k}(n\tau - m)^k\,,$$

notera att vi fritt kan byta ut talparet (n, m) mot $(-m, n)$, då vi fortfarande summerar över alla heltal. Detta bevisar sista påståendet i satsen om Eisensteinseriernas egenskaper. $\square$

Vi skall nu knyta samman Eisensteinserierna med $\wp$, då Eisensteinserier uppstår i $\wp$-funktionens Laurentserieutveckling runt origo.

Sats 6.11. *För z nära noll gäller*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) E_{2k+2} z^{2k} . \tag{6.7}$$

Bevis. Vi ersätter ω mot $-\omega$ i definitionen av $\wp$, vilket ej ändrar summan

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] ,$$

och betraktar det sista uttrycket med hjälp av identiteten

$$\frac{1}{(1-w)^2} = \sum_{\ell=0}^{\infty} (\ell+1) w^\ell ,$$

för $|w| < 1$. För mycket små z kan vi dra slutsatsen

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2} \sum_{\ell=0}^{\infty} (\ell+1) \left(\frac{z}{\omega}\right)^\ell = \frac{1}{\omega^2} + \sum_{\ell=1}^{\infty} (\ell+1) \frac{z^\ell}{\omega^{\ell+2}} .$$

Kombinerat med den första ekvationen, och på grund av likformig konvergens, kan man nu kasta om summatecken för att erhålla det önskade resultatet

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \sum_{\ell=1}^{\infty} (\ell+1) \frac{z^\ell}{\omega^{\ell+2}} = \frac{1}{z^2} + \sum_{\ell=1}^{\infty} (\ell+1) z^\ell \sum_{\omega \in \Lambda^*} \frac{1}{\omega^{\ell+2}} ,$$

där den sista summan är ett annat uttryck för $E_{\ell+2}(\tau)$. Med observationen att detta är lika med 0 då ℓ är jämnt, kan man nu istället välja att summera över $\ell = 2k$ för att erhålla uttrycket i satsen. □

Genom att derivera Laurentserieutvecklingen i Sats 6.7 erhåller vi följande identiteter

$$\wp'(z) = \frac{-2}{z^3} + 6E_4 z + 20E_6 z^3 \dots$$

$$(\wp'(z))^2 = \frac{4}{z^6} - \frac{24E_4}{z^4} - 80E_6 \dots$$

$$(\wp(z))^3 = \frac{1}{z^6} + \frac{9E_4}{z^4} + 15E_6 \dots$$

Härur erhålles att differensen $(\wp'(z))^2 - 4(\wp(z))^3 + 60E_4\wp(z) + 140E_6$ är holomorf nära 0. Eftersom denna differens är en dubbelperiodisk funktion får vi enligt Sats 6.2 att den måste vara konstant, och då differensen är 0 då $z = 0$ måste den vara identiskt lika med 0. Vi får då, med $g_2 = 60E_4$ och $g_3 = 140E_6$ att

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3 \tag{6.8}$$

vilket gör att vi nu har en direkt relation mellan uttrycket (6.4) och Eisensteinserierna.

6.6 Eisensteinserier och delarfunktioner

Vi har nu sakta men säkert närmat oss kopplingen mellan komplexanalysen och talteori, och fokuserar nu på Eisensteinserierna som vi använder oss av för att förena dessa två områden. Vi kommer att betrakta Fourierkofficienterna i Fourierutvecklingen av den periodiska funktionen $E_k(\tau)$. Vi betecknar $\mathcal{E}(z) = E_k(\tau)$, där $z = e^{2\pi i\tau}$ och börjar med att studera Laurentserieutvecklingen av $\mathcal{E}$ som en funktion av z.

Lemma 6.12. *Antag att $k \geq 2$ och att $\mathrm{Im}(\tau) > 0$. Då gäller att*

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+\tau)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i\tau l} .$$

Bevis. Genom att använda Poissons summationsformel på $f(z) = 1/(z+\tau)^k$ kommer vi att få ovanstående identitet. Ett alternativt bevis består av att notera att det först räcker med att visa att identiteten gäller för fallet $k = 2$, eftersom alla andra fall följer genom att termvis derivera, vilket är tillåtet för likformigt konvergerande summor. För att visa fallet då $k = 2$ börjar vi med att derivera formeln för cotangens, nämligen

$$\sum_{n=-\infty}^{\infty} \frac{1}{n+\tau} = \pi \cot \pi\tau .$$

Termvis derivering ger således att

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+\tau)^2} = \frac{\pi^2}{\sin^2(\pi\tau)} .$$

Vi utvecklar nu högerledet med hjälp av $\sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$ och får att

$$\begin{aligned} \frac{\pi^2}{\sin^2(\pi\tau)} &= \frac{-4\pi^2}{(e^{\pi\tau i} - e^{-\pi\tau i})^2} = \frac{-4\pi^2}{e^{2\pi\tau i} + e^{-2\pi\tau i} - 2} = \\ &= \frac{-4\pi^2}{e^{-2\pi\tau i}\underbrace{(1 + e^{4\pi\tau i} - 2e^{2\pi\tau i})}_{=(1-e^{2\pi\tau i})^2}} = \frac{-4\pi^2 e^{2\pi\tau i}}{(1-e^{2\pi\tau i})^2} . \end{aligned}$$

Genom att nu tillämpa det faktum att

$$\sum_{r=1}^{\infty} r w^r = \frac{w}{(1-w)^2} \quad \text{med } w = e^{2\pi i\tau} ,$$

fås att

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+\tau)^2} = -4\pi^2 \sum_{r=1}^{\infty} r e^{2\pi\tau i r} ,$$

vilket skulle visas. □

Som en konsekvens av detta lemma kan vi hitta ett samband mellan Eisensteinserier, zetafunktionen och delarfunktionerna. Vi illustrerar detta samband i en sats, men definierar först delarfunktionerna.

Definition 6.5. *Delarfunktionerna $\sigma_l(r)$ definieras som summan av den l:e potensen av delare till r, det vill säga*

$$\sigma_l(r) = \sum_{d|r} d^l.$$

Sats 6.13. *Om $k \geq 4$ är ett jämnt tal och $\operatorname{Im}(\tau) > 0$ får vi att*

$$E_k(\tau) = 2\zeta(k) + \frac{2(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{r=1}^{\infty} \sigma^{k-1}(r) e^{2\pi i \tau r}. \tag{6.9}$$

Bevis. Vi börjar med att notera att

$$\sigma^{k-1}(r) \leq r r^{k-1} = r^k, \tag{6.10}$$

och om $\operatorname{Im}(\tau) = t$ och $t \geq t_0$ har vi att

$$|e^{2\pi i \tau r}| \leq e^{-2\pi r t_0}. \tag{6.11}$$

Från detta får vi att serien i (6.9) kan uppskattas som

$$\left| \sum_{r=1}^{\infty} \sigma^{k-1}(r) e^{2\pi i \tau r} \right| \leq \sum_{r=1}^{\infty} r^k e^{-2\pi r t_0}, \tag{6.12}$$

vilket ger att serien är absolutkonvergent för $t \geq t_0$. För att fastställa formeln i satsen så använder vi definitionen för E_k, att k är ett jämnt tal samt definitionen för ζ som ger att

$$E_k(\tau) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n+m\tau)^k} = \sum_{n\neq 0} \frac{1}{n^k} + \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{(n+m\tau)^k} =$$

$$= 2\zeta(k) + \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{(n+m\tau)^k} = 2\zeta(k) + 2\sum_{m>0} \sum_{n=-\infty}^{\infty} \frac{1}{(n+m\tau)^k}.$$

Från Lemma 6.12, där vi har ersatt τ med $m\tau$, får vi att vi kan skriva om uttrycket ovan som

$$E_k(\tau) = 2\zeta(k) + 2\sum_{m>0} \frac{(-2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i \tau m l} =$$

$$= 2\zeta(k) + \frac{2(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{m>0} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i \tau m l} =$$

$$= 2\zeta(k) + \frac{2(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{r=1}^{\infty} \sigma^{k-1}(r) e^{2\pi i \tau r},$$

vilket visar formeln i satsen. □

Om vi nu betraktar fallet då $k = 2$,

$$E_2(\tau) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n+m\tau)^2},$$

har vi att serien inte längre är absolutkonvergent. För att ändå kunna analysera fallet då $k = 2$ definierar vi

$$F(\tau) = \sum_m \left(\sum_n \frac{1}{(n+m\tau)^2} \right),$$

där vi summerar enligt den angivna ordningen och $(n,m) \neq (0,0)$. Om vi använder samma argument som i satsen ovan, från (6.10) och (6.11), får vi att dubbelsumman konvergerar och kan formuleras enligt Sats 6.13. Från detta kan vi nu få nästa följdsats.

Följdsats 6.14. *Dubbelsumman F definierad som ovan konvergerar i den angivna ordningen och kan skrivas som*

$$F(\tau) = 2\zeta(2) - 8\pi^2 \sum_{r=1}^{\infty} \sigma(r) e^{2\pi i r\tau}\,,$$

där $\sigma(r)$ är den tidigare definierade delarfunktionen med $l = 1$ och $\zeta(2) = \pi^2/6$.

Kapitel 7

Thetafunktionen

Vi går nu djupare in i teorin för thetafunktionen som utgör en central roll i beviset av två- och fyrkvadratssatsen. I beviset använder vi oss av genererande funktioner för att koppla komplexa-nalysen till talteorin. I det här kapitlet kommer vi att studera thetafunktionens egenskaper och även gå igenom trippelprodukten och dess egenskaper.

7.1 Jacobis thetafunktion

Tidigare har vi definierat thetafunktionen som

$$\vartheta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}\,, \quad t > 0\,.$$

Med hjälp av dess funktionalekvation skrev vi om zetafunktionen på ett sådant sätt att vi med analytisk fortsättning kunde utvidga $\zeta(s)$ till hela det komplexa talplanet. Men egentligen är ϑ bara en variant av Jacobis ursprungliga thetafunktion, Θ, vilken är definierad som

$$\Theta(z|\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} e^{2\pi i n z}\,,$$

där $z \in \mathbb{C}$ och $\tau \in \mathbb{H}$ där $\mathbb{H}$ betecknar det övre komplexa halvplanet. Relationen mellan Θ och dess variant ϑ ges av $\vartheta(t) = \Theta(0|it)$.

Ännu en variant av thetafunktionen, vilken är intressant i bevisen av två- och fyrkvadratssatsen, är

$$\theta(\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}\,,$$

där $\tau \in \mathbb{H}$. Relationen mellan denna variant och den Jacobis ursprungliga thetafunktion ges av $\theta(\tau) = \Theta(0|\tau)$.

Vi ska nu studera egenskaperna hos den ursprungliga thetafunktionen.

Proposition 7.1. *Funktionen Θ har följande egenskaper*

(i) Θ är hel för $z \in \mathbb{C}$ och holomorf då $\tau \in \mathbb{H}$

(ii) $\Theta(z+1|\tau) = \Theta(z|\tau)$

(iii) $\Theta(z+\tau|\tau) = \Theta(z|\tau)e^{-\pi i\tau}e^{-2\pi iz}$

(iv) $\Theta(z|\tau) = 0$ *då* $z = 1/2 + \tau/2 + n + m\tau$ *och* $n, m \in \mathbb{Z}$ *.*

Bevis. För att visa (i) börjar vi med att anta att $\mathrm{Im}(\tau) = t \geq t_0 > 0$ och att $|z| \leq M$. Vi får då att

$$\sum_{n=-\infty}^{\infty} |e^{\pi i n^2 \tau} e^{2\pi i n z}| \leq C \sum_{n \geq 0} e^{-\pi n^2 t_0} e^{2\pi n M} < \infty \,,$$

vilket ger att Θ både är absolutkonvergent och likformigt konvergent. Det här ger att för varje fixt $\tau \in \mathbb{H}$ så är Θ hel och för varje fixt $z \in \mathbb{C}$ är funktionen Θ holomorf i det övre halvplanet.

Från definitionen av Θ för fixt τ kan (ii) fås direkt genom att notera att $e^{2\pi i n z}$ är periodisk med perioden 1.

För att visa (iii) observerar vi att

$$\begin{aligned}\Theta(z+\tau|\tau) &= \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} e^{2\pi i n(z+\tau)} = \\ &= \sum_{n=-\infty}^{\infty} e^{\pi i (n^2+2n)\tau} e^{2\pi i n z} \,.\end{aligned}$$

Kvadratkomplettering i exponenten ger vidare att

$$\begin{aligned}\Theta(z+\tau|\tau) &= \sum_{n=-\infty}^{\infty} e^{\pi i (n+1)^2 \tau} e^{-\pi i \tau} e^{2\pi i n z} = \\ &= \sum_{n=-\infty}^{\infty} e^{\pi i (n+1)^2 \tau} e^{-\pi i \tau} e^{2\pi i (n+1) z} e^{-2\pi i z} = \\ &= e^{-\pi i \tau} e^{-2\pi i z} \sum_{n=-\infty}^{\infty} e^{\pi i (n+1)^2 \tau} e^{2\pi i (n+1) z} = \\ &= e^{-\pi i \tau} e^{-2\pi i z} \Theta(z|\tau) \,,\end{aligned}$$

och egenskapen är visad.

För att visa (iv) räcker det att visa att $\Theta(1/2 + \tau/2|\tau) = 0$ och resten följer från tidigare egenskaper. Vi har att

$$\begin{aligned}
\Theta(1/2+\tau/2|\tau) &= \sum_{n=-\infty}^{\infty} e^{\pi i n^2\tau} e^{2\pi i n(1/2+\tau/2)} = \\
&= \sum_{n=-\infty}^{\infty} e^{\pi i(n^2+n)\tau} e^{\pi i n} = \\
&= \sum_{n=-\infty}^{\infty} (-1)^n e^{\pi i(n^2+n)\tau} = \\
&= 1 + \sum_{n=1}^{\infty}(-1)^n e^{\pi i(n^2+n)\tau} + \sum_{n=-1}^{-\infty}(-1)^n e^{\pi i(n^2+n)\tau} = \\
&= 1 + \sum_{n=1}^{\infty}(-1)^n e^{\pi i(n^2+n)\tau} + \sum_{n=1}^{\infty}(-1)^n e^{\pi i(n^2-n)\tau}\,.
\end{aligned}$$

Om vi gör variabelbytet $k = n-1$ på andra summan får vi

$$\begin{aligned}
\sum_{n=1}^{\infty}(-1)^n e^{\pi i(n^2-n)\tau} &= \sum_{k=0}^{\infty}(-1)^{k+1} e^{\pi i\big((k+1)^2-(k+1)\big)\tau} = \\
&= \sum_{k=0}^{\infty}(-1)^{k+1} e^{\pi i(k^2+k)\tau} = \\
&= -1 - \sum_{k=1}^{\infty}(-1)^k e^{\pi i(k^2+k)\tau}\,.
\end{aligned}$$

Från detta får vi att

$$\Theta(1/2+\tau/2|\tau) = 1 + \sum_{n=1}^{\infty}(-1)^n e^{\pi i(n^2+n)\tau} - 1 - \sum_{k=1}^{\infty}(-1)^k e^{\pi i(k^2+k)\tau} = 0\,.$$

□

7.2 Trippelprodukten

Vi kommer nu betrakta den så kallade trippelprodukten, $\Pi(z|\tau)$.

Definition 7.1. *Vi har att för $z \in \mathbb{Z}$, $\tau \in \mathbb{H}$ och $q = e^{\pi i\tau}$ så är trippelprodukten definierad som*

$$\Pi(z|\tau) = \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz})\,.$$

Detta är en funktion som uppfyller liknande egenskaper som $\Theta(z|\tau)$ och dessa formulerar vi i följande proposition.

Proposition 7.2. *Funktionen $\Pi(z|\tau)$ har följande egenskaper:*

(i) $\Pi(z|\tau)$ *är hel för $z \in \mathbb{C}$ och holomorf då $\tau \in \mathbb{H}$*

(ii) $\Pi(z+1|\tau) = \Pi(z|\tau)$

(iii) $\Pi(z+\tau|\tau) = \Pi(z|\tau)e^{-\pi i\tau}e^{-2\pi iz}$

(iv) $\Pi(z|\tau) = 0$ *då* $z = 1/2+\tau/2+n+m\tau$ *och* $n, m \in \mathbb{Z}$ *. Dessa punkter är även enkla nollställen, och de enda nollställena, till* $\Pi(\cdot|\tau)$*.*

Bevis. Vi låter Im(τ)= $t \geq t_0 > 0$, vilket ger att

$$|q| = |e^{\pi i\tau}| \leq e^{-\pi t_0} < 1\,.$$

Vi har även att faktorerna från trippelprodukten kan utvecklas enligt

$$(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz}) = 1 + O(|q|^{2n-1}e^{2\pi|z|})\,.$$

Eftersom att summan $\sum |q|^{2n-1}$ konvergerar kommer även $\Pi(z|\tau)$ konvergera enligt propositionen om oändliga produkters konvergens, se (3.1). Det här gör att $\Pi(z|\tau)$ definierar en hel funktion av z med fixt $\tau \in \mathbb{H}$ och en holomorf funktion av τ med fixt $z \in \mathbb{C}$, vilket ger att (i) gäller.

Från definitionen av $\Pi(z|\tau)$ fås (ii) genom att observera att funktionen är periodisk med perioden 1 för z.

För att bevisa (iii) observerar vi först att

$$\begin{aligned}\Pi(z+\tau|\tau) &= \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi i(z+\tau)})(1+q^{2n-1}e^{-2\pi i(z+\tau)}) = \\ &= \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n+1}e^{2\pi iz})(1+q^{2n-3}e^{-2\pi iz})\,,\end{aligned}$$

där vi har använt oss av att $q = e^{\pi i\tau}$. Om vi först betraktar andra faktorn i vår produkt har vi att

$$\prod_{n=1}^{\infty}(1+q^{2n+1}e^{2\pi iz})\frac{(1+qe^{2\pi iz})}{(1+qe^{2\pi iz})} = \prod_{n=1}^{\infty}(1+q^{2n-1}e^{2\pi iz})\frac{1}{(1+qe^{2\pi iz})}\,,$$

där vi i första produkten förlänger och förkortar med faktorn för $n = 0$, vilket gör att vi genom en omskrivning låter exponenten för q börja ett index tidigare. Om vi sedan betraktar den tredje faktorn i vår produkt har vi att

$$\prod_{n=1}^{\infty}(1+q^{2n-3}e^{-2\pi iz}) = \prod_{n=1}^{\infty}(1+q^{2n-1}e^{-2\pi iz})(1+q^{-1}e^{-2\pi iz})\,,$$

där vi har brutit ut faktorn för $n = 1$. Det här ger oss att

$$\begin{aligned}\Pi(z+\tau|\tau) &= \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz})\left(\frac{1+q^{-1}e^{-2\pi iz}}{1+qe^{2\pi iz}}\right) = \\ &= \Pi(z|\tau)\left(\frac{1+q^{-1}e^{-2\pi iz}}{1+qe^{2\pi iz}}\right)\,.\end{aligned}$$

Vi vet även att då $x \neq -1$ så är

$$\frac{1+x}{1+x^{-1}} = x\,,$$

vilket tillsammans med utvecklingen av $\Pi(z+\tau|\tau)$ ger oss att (iii) gäller.

För visa (*iv*) vill vi hitta alla nollställen till $\Pi(z|\tau)$. Vi minns först att en konvergent produkt endast har nollställen om minst en av dess faktorer är noll. Eftersom att $|q| < 1$ så kan aldrig faktorn $(1-q^n)$ vara noll. För att faktorn $(1+q^{2n-1}e^{2\pi iz})$ ska vara noll måste $q^{2n-1}e^{2\pi iz} = -1 = e^{\pi i}$. Vi har att $q = e^{\pi i\tau}$, och om vi då jämför exponenter får vi att

$$(2n-1)\tau + 2z = 1 \pmod 2\,,$$

där modulus 2 kommer från att e^z är periodisk med perioden $2\pi i$. Det här ger att

$$z = 1/2 + \tau/2 - n\tau \pmod 1\,,$$

vilket ger oss alla nollställen på formen $z = 1/2 + \tau/2 - n\tau + m$ för $n \geq 1$ och $m \in \mathbb{Z}$.

Den tredje faktorn i produkten blir på samma sätt noll om

$$(2n-1)\tau - 2z = 1 \pmod 2\,,$$

vilket ger att

$$\begin{aligned} z &= -1/2 - \tau/2 + n\tau \pmod 1 \\ &= 1/2 + \tau/2 + n'\tau \pmod 1\,, \end{aligned}$$

där $n' \geq 0$. Det här ger oss nollställena till $\Pi(\cdot|\tau)$ och eftersom vi vet att $1 - e^w$ har ett enkelt nollställe i $w = 0$ vet vi även att våra nollställen måste vara enkla. □

Vi har nu bevisat egenskaperna för både $\Theta(z|\tau)$ och $\Pi(z|\tau)$ och vi ser att funktionernas egenskaper påminner om varandra väldigt mycket. Det här gör att man kan misstänka att funktionerna också har en nära koppling, vilket vi kommer se i nästa sats.

Sats 7.3. *För alla $z \in \mathbb{C}$ och $\tau \in \mathbb{H}$ så gäller att*

$$\Theta(z|\tau) = \Pi(z|\tau)\,.$$

Bevis. Låt $\tau \in \mathbb{H}$ vara fixt och betrakta kvoten

$$F(z) = \frac{\Theta(z|\tau)}{\Pi(z|\tau)}\,.$$

Notera att med hjälp av de två senaste propositionerna så får vi att F är hel och dubbelperiodisk med perioderna 1 och τ. Enligt Liouvilles första sats, se Sats 6.2, betyder det här att F måste vara konstant i z. Detta ger att det existerar en funktion $c(\tau)$ så att

$$\Theta(z|\tau) = c(\tau)\Pi(z|\tau)\,. \tag{7.1}$$

Det återstår att visa att $c(\tau) = 1$ för alla τ. Vi börjar med att sätta $z = 1/2$ i ekvationen ovan så att $e^{2\pi iz} = -1$ och får att

$$\begin{aligned} \Theta(1/2|\tau) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} &= c(\tau)\prod_{n=1}^{\infty}(1-q^{2n})(1-q^{2n-1})(1-q^{2n-1}) = \\ &= c(\tau)\prod_{n=1}^{\infty}[(1-q^{2n-1})(1-q^{2n})](1-q^{2n-1}) = \\ &= c(\tau)\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n-1})\,. \end{aligned}$$

Sista steget följer av att de första två faktorerna tillsammans går över alla heltal. Detta ger att

$$c(\tau) = \frac{\sum_{n=-\infty}^{\infty}(-1)^n q^{n^2}}{\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n-1})} \,. \tag{7.2}$$

Om vi nu låter $z = 1/4$ i (7.1), så att $e^{2\pi i z} = i$, får vi att

$$\Theta(1/4|\tau) = \sum_{n=-\infty}^{\infty} q^{n^2} i^n \,.$$

Genom att utveckla summan i högerledet ser vi att alla termer där n är udda kommer att cancelleras, vilket ger att vi kan sätta $n = 2m$ och får å ena sidan att

$$\Theta(1/4|\tau) = \sum_{m=-\infty}^{\infty} q^{4m^2}(-1)^m \,.$$

Å andra sidan har vi att

$$\begin{aligned}\Pi(1/4|\tau) &= \prod_{m=1}^{\infty}(1-q^{2m})(1+iq^{2m-1})(1-iq^{2m-1}) = \\ &= \prod_{m=1}^{\infty}(1-q^{2m})(1+q^{4m-2}) \,.\end{aligned}$$

Vi delar nu upp produkten och använder oss av att vi kan låta $2m = 4n$ och $2m = 4n-2$. Det här ger oss att

$$\begin{aligned}\Pi(1/4|\tau) &= \prod_{n=1}^{\infty}(1-q^{4n})(1-q^{4n-2}) \prod_{m=1}^{\infty}(1+q^{4m-2}) = \\ &= \prod_{n=1}^{\infty}(1-q^{4n})(1-q^{4n-2})(1+q^{4n-2}) = \\ &= \prod_{n=1}^{\infty}(1-q^{4n})(1-q^{8n-4}) \,.\end{aligned}$$

Vi har alltså att

$$c(\tau) = \frac{\sum_{n=-\infty}^{\infty}(-1)^n q^{4n^2}}{\prod_{n=1}^{\infty}(1-q^{4n})(1-q^{8n-4})} \,. \tag{7.3}$$

Kombinerar vi nu (7.2) och (7.3) får vi att $c(\tau) = c(4\tau)$ och upprepar vi denna likhet får vi att $c(\tau) = c(4^k\tau)$. Vi har att $q^{4^k} = e^{i\pi 4^k \tau}$ går mot 0 då k går mot oändligheten och ser då att $\Pi(0|\tau)$ och $\Theta(0|\tau)$ går mot 1 då $\mathrm{Im}(\tau)$ går oändligheten, vilket i sin tur ger att $c(\tau) = 1$. $\square$

Om vi använder oss av Sats 7.3 med $z = 0$ får vi $\theta(\tau) = \Theta(0|\tau)$. Med hjälp av detta kan vi formulera nästa följdsats, där vi får att θ inte har några nollställen i det övre halvplanet. Denna följdsats är viktig för beviset av två- och fyrkvadratssatsen.

Följdsats 7.4. *För $Im(\tau) > 0$ och $q = e^{\pi i \tau}$ gäller att*

$$\theta(\tau) = \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1})^2 \,,$$

vilket ger att $\theta(\tau) \neq 0$ för $\tau \in \mathbb{H}$.

Del III

De tre satserna

Kapitel 8

Primtalssatsen

> "No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. Now we know that the theorem is roughly equivalent to a theorem about an analytic function, the theorem that Riemann's zeta function has no roots on a certain line. A proof of such a theorem, not fundamentally dependent on the theory of functions, seems to me extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say 'lie deep' and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten." - P.H Hardy, 1921

Inom talteori beskriver primtalssatsen den asymptotiska fördelningen av primtal för positiva heltal. Låt oss börja med att definiera funktionen $\pi(x)$.

$$\pi(x) = \text{ antalet primtal mindre än eller lika med } x \ .$$

Primtalen är både oändliga till antalet och irreguljära i sin fördelning, vilket inger lite hopp om att hitta ett slutet uttryck för $\pi(x)$ i elementära funktioner. Istället har man valt att studera det asymptotiska beteendet för $\pi(x)$, det vill säga beteendet som $\pi(x)$ antar när man låter x växa obegränsat. Flera sådana uttryck har hittats genom historien, bland annat de två nedanstående uttrycken.

$$\pi(x) \sim \frac{x}{\log(x)} \qquad \text{när } x \to \infty \,, \tag{8.1}$$

$$\pi(x) \sim \int_2^x \frac{1}{\log t}\,\mathrm{d}t \qquad \text{när } x \to \infty \,. \tag{8.2}$$

Här betyder det asymptotiska förhållandet $f(x) \sim g(x)$ när x går mot oändligheten att

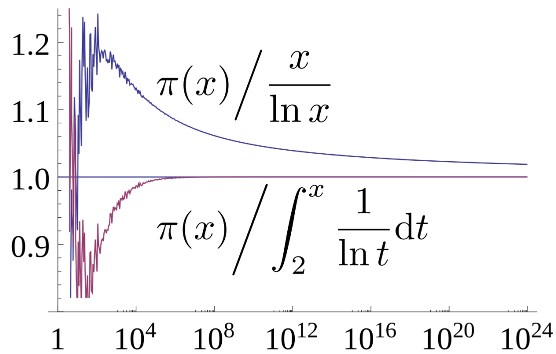
$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1 \,.$$

Det första uttrycket bygger på begåvade gissningar som formulerades av Legendre och Gauss i slutet av 1700-talet. Det andra uttrycket kom Dirichlet fram till 1838, men även det utan rigoröst bevis. Ungefär 100 år efter Legendre och Gauss insatser så bevisade Hadamard och de la Valleé Poussin oberoende av varandra förhållandet i ekvation (8.1), även kallad primtalssatsen.

Sats 8.1 (Primtalssatsen)**.** *Låt $\pi(x)$ beteckna antalet primtal mindre än eller lika med x. Då får vi det asymptotiska förhållandet*

$$\pi(x) \sim \frac{x}{\log x}\,, \text{ när } x \to \infty\,.$$

Primtalsatsen ger oss en bild av hur tätt primtalen ligger och säger att primtalen blir mindre vanliga då de blir större. Det är alltså denna relationen vi kommer att bevisa, även om det inte



Figur 8.1: *Kvoten av $\pi(x)$ och dess två nämnda uppskattningar, med logaritmisk skala på x-axeln. Bild tagen ifrån Wikimedia Commons.*

är den som konvergerar snabbast, vilket vi kan se i Figur 8.1.

För att bevisa primtalssatsen kommer vi, liksom originalbeviset, använda oss av komplexanalys. År 1949 kom Paul Erdös och Atle Selberg med det första elementära beviset, till den i början av kapitlet citerade G.H. Hardys stora besvikelse. Vårt bevis bygger på att man introducerar två hjälpfunktioner, som i förhållande till $\pi(x)$ är relativt lätta att arbeta med. De kallas för Tchebychev's ψ-funktioner och definieras som följande

$$\psi(x) = \sum_{p^m \leq x} \log p\,,$$

samt

$$\psi_1(x) = \int_1^x \psi(u)\,\mathrm{d}u\,.$$

Som vi ser så definieras $\psi(x)$ som en summa över logaritmer av primtal, vilket gör den direkt relaterbar till påståendet om $\pi(x)$ asymptotiska beteende. Beviset i sig bygger nu på en effektiv trestegsraket.

1. Visa att om $\psi(x) \sim x$ för obegränsat växande x, så gäller att $\pi(x) \sim x/\log x$ för ett obegränsat växande x.
2. Att $\psi(x) \sim x$ följer om $\psi_1(x) \sim x^2/2$, för ett obegränsat växande x.
3. Att rigoröst bevisa att $\psi_1(x) \sim x^2/2$ och ur detta följer sedan påståenden ovan.

För att bevisa det tredje steget krävs vissa manipulationer av Riemanns ζ-funktion nära linjen $s = 1 + it$, $t \in \mathbb{R}$, där den är nollskild för alla t. Således inleder vi vårt bevis med att utveckla en verktygslåda för manipulation av ζ-funktionen, för att sedan visa de tre påståendena beskrivna ovan.

8.1 Nollställen till zetafunktionen

Vi studerade nollställena till zetafunktionen i Kapitel 4 där vi bland annat kom fram till att $\zeta(s)$ har nollställen i alla negativa jämna heltal. Dessa nollställen kallas för de triviala nollställena, och är i sig ointressanta för vår fortsatta studie. Resten av zetafunktionens nollställen har vi bevisat ligger innanför den kritiska remsan $0 < \mathrm{Re}(s) < 1$ och kallas de icke-triviala nollställena. Här kommer den berömda Riemannhypotesen in som behandlas i större detalj i slutet av Kapitel 4. Riemannhypotesen är inte det absolut centrala för beviset av primtalsatsen, men vad som däremot är centralt är påståendet att zetafunktionen är nollskild på linjen $s = 1 + it$, $t \in \mathbb{R}$. För att kunna bevisa detta kommer vi först och främst behöva Eulers produktformel för zetafunktionen, som vi nämnde redan i introduktionen. Formeln säger att om $\mathrm{Re}(s) > 1$ har vi att zetafunktionen kan skrivas som den oändliga produkten

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}} . \tag{8.3}$$

För att bevisa att zetafunktionen är nollskiljd på $\mathrm{Re}(s) = 1$ har vi även samlat de nödvändiga komponenterna i följande lemman.

Lemma 8.2. *Om $Re(s) > 1$ har vi att*

$$\log \zeta(s) = \sum_{p,\, m} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} c_n n^{-s} ,$$

för något $c_n \geq 0$.

Bevis. Beviset av denna sats bygger på några fundamentala egenskaper hos logaritmen samt Taylorutvecklingen för logaritmen. Vi börjar med att notera att

$$\log \frac{1}{1-x} = \sum_{m=1}^{\infty} \frac{x^m}{m} ,$$

för $0 < x < 1$. Ur detta och produktformeln för zetafunktionen följer att

$$\log \zeta(s) = \log \prod_p \frac{1}{1-p^{-s}} = \sum_p \log \frac{1}{1-p^{-s}} = \sum_{p,\, m} \frac{p^{-ms}}{m} .$$

Dubbelsumman är absolutkonvergent vilket gör att man fritt kan välja summationsordning. Analytisk fortsättning ger nu att den här formeln håller för $\mathrm{Re}(s) > 1$. Värt att notera är att för $\mathrm{Re}(s) > 1$ kan $\log \zeta(s)$ definieras holomorft, då $\zeta(s)$ saknar nollställen i detta område. Till sist får vi att

$$\sum_{p,\, m} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} c_n n^{-s} ,$$

där

$$c_n = \begin{cases} \frac{1}{m} & \text{om } n = p^m \\ 0 & \text{annars} . \end{cases}$$

□

Lemma 8.3. *Om* $\theta \in \mathbb{R}$ *har vi att*

$$3 + 4\cos\theta + \cos 2\theta \geq 0\,.$$

Bevis. Lemmat följer från att vi med hjälp av dubbla vinkeln för cosinus kan skriva om uttrycket som

$$3 + 4\cos\theta + \cos 2\theta = 3 + 4\cos\theta + 2\cos^2\theta - 1 = 2(1+\cos\theta)^2\,,$$

som vi vet är större än noll för reella θ. □

Följdsats 8.4. *Om* $\sigma > 1$ *och* t *är reellt har vi att*

$$\log|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geq 0\,.$$

Bevis. Låt $s = \sigma + it$ och notera att

$$\mathrm{Re}(n^{-s}) = \mathrm{Re}(e^{(\sigma+it)\log n}) = e^{-\sigma\log n}\cos t\log n = n^{-\sigma}\cos t\log n\,. \tag{8.4}$$

Notera även att

$$\log z = \log|z| + i\mathrm{Arg}(z) \to \mathrm{Re}(\log z) = \log|z|.$$

Därför får vi att

$$\log|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| = 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+2it)|\,,$$

vilket i sin tur är lika med

$$3\mathrm{Re}(\log\zeta(\sigma)) + 4\mathrm{Re}(\log\zeta(\sigma+it)) + \mathrm{Re}(\log\zeta(\sigma+2it))\,.$$

Här noterar vi uttrycket för logaritmer utav zetafunktionen från Lemma 8.2 och använder oss av ekvation (8.4). Slutligen landar vi på att

$$\log|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| = \sum_{n=1}^{\infty} c_n n^{-\sigma}(3 + 4\cos(t\log n) + \cos(2t\log n))\,.$$

Att detta uttryck är ickenegativt följer ur Lemma 8.3 och att c_n är ickenegativt. □

Nu när vi har alla verktyg så kan vi formulera och bevisa satsen som säger att zetafunktionen inte har några nollställen på linjen $\mathrm{Re}(s) = 1$. För att göra detta kommer vi anta motsatsen, det vill säga att den har nollställen på $\mathrm{Re}(s) = 1$, och sen kommer vi se att detta strider mot följdsatsen ovan.

Sats 8.5. *Zetafunktionen har inga nollställen på linjen* $\mathrm{Re}(s) = 1$.

Bevis. Vi börjar med att konstatera att vi vet att ζ har en pol i punkten 1, vilket ger att den inte har några nollställen i ett närområde till denna punkt. Det vi vill visa är då att

$$\zeta(1+it) \neq 0\,,$$

för alla $t \in \mathbb{R}$. Antag motsatsen, det vill säga att

$$\zeta(1+it_0) = 0\,,$$

för något $t_0 \neq 0$. För att motbevisa detta kommer vi använda oss av uttrycket i Följdsats 8.4. Vi vet att ζ är en holomorf funktion vid $s_0 = 1 + it_0$ och att den därför försvinner i denna punkt med en ordning av minst ett. Detta ger att det finns en holomorf funktion g som inte försvinner nära $1 + it_0$ och ett $n \geq 1$ så att

$$\zeta(s) = (s - s_0)^n g(s) .$$

Från detta får vi med $s_0 = 1 + it_0$ att det finns ett $C_1 > 0$ så att

$$|\zeta(\sigma + it_0)|^4 \leq C_1(\sigma - 1)^4, \text{ när } \sigma \to 1 . \tag{8.5}$$

Liknande vet vi att ζ har en enkelpol vid $s_0 = 1$ och vi får att det finns en holomorf funktion h som inte försvinner nära s_0 så att

$$\zeta(s) = (s - s_0)^{-1} h(s) .$$

Detta ger att det finns ett $C_2 > 0$ sådan att

$$|\zeta(\sigma)|^3 \leq C_2(\sigma - 1)^{-3} \text{ när } \sigma \to 1 . \tag{8.6}$$

Eftersom ζ är holomorf vid $\sigma + it_0$ för alla σ får vi att $|\zeta(\sigma + 2it_0)|$ är begränsad när σ närmar sig 1. Om vi nu lägger ihop våra uppskattningar ser vi att

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \to 0 , \text{ när } \sigma \to 1 ,$$

där nollstället i detta uttryck är av högre ordning än polen. Eftersom logaritmen av ett tal mellan noll och ett är negativt motsäger detta Följdsats 8.4. Detta bevisar att ζ inte kan ha några nollställen på linjen $\mathrm{Re}(s) = 1$.

□

8.2 Uppskattningar av zetafunktionen

En annan viktig del för beviset av primtalssatsen är att undersöka hur zetafunktionen beter sig nära linjen $\mathrm{Re}(s) = 1$. Den termen som kommer ha en stor roll i beviset är den logaritmiska derivatan $\zeta'(s)/\zeta(s)$ och vi kommer behöva kunna uppskatta denna. Därför behöver vi veta hur $\zeta'(s)$ och $1/\zeta(s)$ växer. Uppskattningen för ζ' togs upp i kapitel 4 om zetafunktionen, men vi upprepar propositionen här igen för tydlighetens skull.

Proposition 8.6. *Antag att $s = \sigma + it$, $\sigma, t \in \mathbb{R}$. Då gäller det att för varje $\sigma_0 : 0 \leq \sigma_0 \leq 1$ och varje $\epsilon > 0$ existerar det en konstant c_ϵ sådan att*

(i) $|\zeta(s)| \leq c_\epsilon |t|^{1-\sigma_0+\epsilon}$, *då* $\sigma_0 \leq \sigma$ *och* $|t| \geq 1$.

(ii) $|\zeta'(s)| \leq c_\epsilon |t|^\epsilon$, *då* $\sigma \geq 1$ *och* $|t| \geq 1$.

I propositionen ovan ser vi i den andra punkten uppskattningen för ζ' och vi kommer nu undersöka uppskattningen av $1/\zeta$.

Proposition 8.7. *För varje $\epsilon > 0$ har vi att*

$$\frac{1}{|\zeta(s)|} \leq c_\epsilon |t|^\epsilon ,$$

där $s = \sigma + it$ med $\sigma \geq 1$ och $|t| \geq 1$.

Bevis. Från tidigare har vi sett att

$$|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geq 1\,,$$

för $\sigma \geq 1$. Från detta och från den första uppskattningen av Proposition 8.6 får vi att

$$|\zeta^4(\sigma+it)| \geq |\zeta^{-3}(\sigma)||\zeta^{-1}(\sigma+2it)| \geq c|\zeta^{-3}(\sigma)||t|^{-\epsilon} \geq c'(\sigma-1)^3|t|^{-\epsilon}\,,$$

för alla $\sigma \geq 1$ och $|t| \geq 1$. Argumentet för den sista olikheten kommer från ekvation 8.6 i satsen om att zetafunktionen inte har några nollställen i $\mathrm{Re}(s) = 1$. Om vi nu tar fjärderoten ur detta får vi

$$|\zeta(\sigma+it)| \geq c'(\sigma-1)^{3/4}|t|^{-\epsilon/4}\,, \tag{8.7}$$

för $\sigma \geq 1$ och $|t| \geq 1$. Vi behöver nu hantera två separata fall, utifrån om olikheten $\sigma - 1 \geq A|t|^{-5\epsilon}$ håller eller ej för ett lämpligt val av A, som bestäms senare. Om den här olikheten håller så följer det direkt av ovanstående ekvation att

$$|\zeta(\sigma+it)| \geq A'|t|^{-\varepsilon/4}\,,$$

och att byta ut ϵ mot 4ϵ ger oss exakt den uppskattning som vi söker. Om $\sigma - 1 < A|t|^{-5\epsilon}$ så kan vi gå runt detta genom att ansätta en punkt $\sigma' > \sigma$ där $\sigma' - 1 = A|t|^{-5\epsilon}$. Triangelolikheten ger oss nu att

$$|\zeta(\sigma+it)| \geq |\zeta(\sigma'+it)| - |\zeta(\sigma'+it) - \zeta(\sigma+it)|\,.$$

Integralkalkylens medelvärdesats tillsammans med den tidigare erhållna uppskattningen $|\zeta'(s)| \leq c_\epsilon|t|^\epsilon$ leder oss nu till

$$|\zeta(\sigma'+it) - \zeta(\sigma+it)| = |\zeta'(s)(\sigma'-\sigma)| \leq c''|\sigma'-\sigma||t|^\varepsilon \leq c''|\sigma'-1||t|^\varepsilon\,.$$

Efter dessa observationer kan vi sätta $\sigma = \sigma'$ i uttrycket från ekvation (8.7) och får då

$$\begin{aligned}|\zeta(\sigma+it)| &\geq |\zeta(\sigma'+it)| - |\zeta(\sigma'+it) - \zeta(\sigma+it)| \geq \\ &\geq c'(\sigma'-1)^{3/4}|t|^{-\varepsilon/4} - c''(\sigma'-1)|t|^\varepsilon\,.\end{aligned}$$

Kom ihåg att $\sigma' - 1 = A|t|^{-5\epsilon}$, och sätt $A = (c'/(2c''))^4$. Detta ger oss att den första termen ovan kan skrivas

$$c'(\sigma'-1)^{3/4}|t|^{-\varepsilon/4} = 2c''(\sigma'-1)|t|^\varepsilon\,,$$

och där ur följer

$$|\zeta(\sigma+it)| \geq c''(\sigma'-1)|t|^\varepsilon = c''A|t|^{-5\varepsilon}|t|^\varepsilon = A''|t|^{-4\epsilon}\,.$$

Genom att byta ut 4ε mot ε får vi vår önskade relation. □

Det som är viktigt att komma ihåg om zetafunktionen för att bevisa primtalssatsen är att zetafunktionen inte har några nollställen på linjen $\mathrm{Re}(s) = 1$ och att den kan uppskattas enligt Proposition 8.6 och 8.7.

8.3 Funktionerna ψ och ψ_1

Nu har vi studerat zetafunktionen till den nivå som beviset av primtalssatsen kräver. Beviset bygger dock inte bara på egenskaper hos zetafunktionen. I det här avsnittet introducerar vi två nya funktioner som är centrala för beviset. Dessa två funktioner kallas Tchebychev's ψ-funktioner och är förhållandevis enkla att hantera. Överraskande nog hittar man många likheter i deras beteende jämfört med primtalsfunktionen $\pi(x)$.

8.3.1 Funktionen ψ

Definition 8.1. *Tchebychevs ψ-funktion skrivs*

$$\psi(x) = \sum_{p^m \leq x} \log p \,,$$

där p är ett primtal och m är ett positivt heltal. Summan går över alla heltal på formen p^m som är mindre än eller lika med x.

Det vi nu ska göra är att hitta varianter för att skriva ψ-funktionen ovan och för detta definierar vi först von Mangoldt-funktionen.

Definition 8.2 (von Mangoldt-funktionen $\Lambda(n)$)**.**

$$\Lambda(n) = \begin{cases} \log p \,, & \textit{om } n = p^m, \textit{ för något primtal } p \textit{ och något } m \geq 1 \\ 0 \,, & \textit{annars.} \end{cases}$$

Från definitionen ovan får vi att vi kan skriva ψ som

$$\psi(x) = \sum_{p^m \leq x} \log p = \sum_{n=1}^{x} \Lambda(n) \,.$$

Vi noterar att om $p^m \leq x$ får vi att $m \leq \log x / \log p$ och vi kan skriva

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \,, \tag{8.8}$$

där $\lfloor u \rfloor$ är det största heltalet som är mindre än eller lika med u. Samtliga av dessa tre sätt att skriva $\psi(x)$ kommer att komma till användning i beviset.

Efter att nu ha introducerat ψ vill vi koppla denna till $\pi(x)$. Faktumet är att vi kan förenkla primtalssatsen till ett liknande asymptotiskt förhållande för ψ, vilket motiveras i propositionen nedan.

Proposition 8.8. *Om $\psi(x) \sim x$ när x går mot oändligheten har vi att $\pi(x) \sim x/\log x$ när x går mot oändligheten, det vill säga*

$$\lim_{x \to \infty} \pi(x) \frac{\log x}{x} = \lim_{x \to \infty} \frac{\psi(x)}{x} \,. \tag{8.9}$$

Bevis. För att bevisa den här utsagan behöver vi visa följande två olikheter:

$$1 \leq \liminf_{x \to \infty} \pi(x) \frac{\log x}{x} \,; \tag{8.10}$$

$$\limsup_{x \to \infty} \pi(x) \frac{\log x}{x} \leq 1 \,. \tag{8.11}$$

För den första olikheten räcker en grov uppskattning som bygger på den tredje formuleringen av $\psi(x)$ från ekvation (8.8),

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \leq \sum_{p \leq x} \frac{\log x}{\log p} \log p = \pi(x) \log x \,.$$

Efter division med x erhåller vi

$$\limsup_{x\to\infty} \frac{\psi(x)}{x} \leq \liminf_{x\to\infty} \frac{\pi(x)\log x}{x}\,, \tag{8.12}$$

och vi ser nu att *om* $\psi(x) \sim x$, så gäller ekvation (8.10). Den övre uppskattningen i ekvation (8.11) är mer komplex. Fixera ett tal α så att $0 < \alpha < 1$ och uppskatta ψ utifrån Definition 8.1. Detta ger oss att

$$\begin{aligned}\psi(x) = \sum_{p^m \leq x} \log p \geq \sum_{p\leq x} \log p \geq \sum_{x^\alpha < p \leq x} \log p \geq \\ \geq \log x^\alpha \sum_{x^\alpha < p \leq x} 1 \geq \alpha \log x (\pi(x) - \pi(x^\alpha))\,.\end{aligned}$$

Om vi noterar att $\pi(x^\alpha) \leq x^\alpha$ för $\alpha < 1$ får vi följande uppskattning av ψ,

$$\psi(x) \geq \alpha\pi(x)\log x - \alpha x^\alpha \log x\,.$$

Delar vi båda sidor med x får vi

$$\frac{\psi(x)}{x} \geq \alpha\pi(x)\frac{\log x}{x} - \alpha x^{\alpha-1}\log x\,,$$

där den andra termen kommer gå mot noll när vi låter x växa och får därmed att

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq \alpha \limsup_{x\to\infty} \pi(x)\frac{\log x}{x}\,. \tag{8.13}$$

Vi vet att $\psi(x) \sim x$ när x går mot oändligheten och låter vi α närma sig 1 får vi att den övre uppskattningen i ekvation (8.11) håller. Kombinerar vi våra två resultat i ekvation (8.12) och (8.13) får vi slutsatsen

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq \limsup_{x\to\infty} \frac{\pi(x)\log x}{x} \geq \liminf_{x\to\infty} \frac{\pi(x)\log x}{x} \geq \limsup_{x\to\infty} \frac{\psi(x)}{x}\,,$$

vilket ger oss likheten i ekvation (8.9).

□

8.3.2 Funktionen ψ_1

För att kunna visa Proposition 8.8 ovan introducerar vi en ny funktion som går att betrakta som ”primitiva funktion” till ψ, nämligen ψ_1.

Definition 8.3. *Tchebychev's ψ_1-funktion skrivs*

$$\psi_1(x) = \int_1^x \psi(u)\,\mathrm{d}u\,.$$

Det vi nu ska visa är att asymptoten $\psi \sim x$ när x går mot oändligheten följer av det asymptotiskta förhållandet $\psi_1 \sim x^2/2$. Likt i Proposition 8.8 kommer den dock vara en obevisad utsaga i beviset som nu följer.

Proposition 8.9. *Om $\psi_1(x) \sim x^2/2$ när x går mot oändligheten gäller att $\psi(x) \sim x$ när x går mot oändligheten, det vill säga*

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = \lim_{x\to\infty} \frac{\psi_1(x)}{x^2/2}\,.$$

Bevis. Vi kommer att behöva två godtyckliga α, β så att $\alpha < 1 < \beta$, observera att

$$\frac{1}{(1-\alpha)x}\int_{\alpha x}^{x}\psi(u)\,\mathrm{d}u \leq \psi(x) \leq \frac{1}{(\beta-1)x}\int_{x}^{\beta x}\psi(u)\,\mathrm{d}u\,,$$

vilket gäller då $\psi(x)$ är en strikt växande funktion. Precis som i Proposition 8.8 vill vi nu visa att motsvarande olikheter för limsup och liminf gäller, se ekvation (8.10) och (8.11). En direkt konsekvens av den senare olikheten i vår observation ovan är att

$$\psi(x) \leq \frac{1}{(\beta-1)x}[\psi_1(\beta x) - \psi_1(x)]\,.$$

Efter division med x erhåller vi

$$\frac{\psi(x)}{x} \leq \frac{1}{(\beta-1)}\left[\frac{\psi_1(\beta x)}{(\beta x)^2}\beta^2 - \frac{\psi_1(x)}{(x)^2}\right].$$

Om vi nu utgår ifrån att $\psi_1(x) \sim x^2/2$ gäller, får vi när x går mot oändligheten att

$$\limsup_{x\to\infty}\frac{\psi(x)}{x} \leq \frac{\beta^2-1}{(\beta-1)}\liminf_{x\to\infty}\frac{\psi_1(x)}{x^2/2}\,,$$

vilket gäller för alla $\beta > 1$. Eftersom β kan röra sig godtyckligt nära 1 följer det att olikheten för liminf i ekvation (8.10) gäller,

$$\limsup_{x\to\infty}\frac{\psi(x)}{x} \leq \liminf_{x\to\infty}\frac{\psi_1(x)}{x^2/2}$$

Exakt samma typ av beräkning visar att

$$\liminf_{x\to\infty}\frac{\psi(x)}{x} \geq \limsup_{x\to\infty}\frac{\psi_1(x)}{x^2/2}$$

och propositionen är nu bevisad. □

8.4 Förhållandet mellan ψ_1 och ζ

Det är nu dags att visa hur ψ_1 och ζ hänger ihop, med hjälp av en rad överraskande identiteter. I Lemma 8.2 fick vi för $\mathrm{Re}(s) > 1$ uttrycket

$$\log\zeta(s) = \sum_{p,m}\frac{p^{-ms}}{m}\,.$$

Deriverar vi båda sidor med avseende på s i uttrycket ovan får vi att

$$\frac{1}{\zeta(s)}\zeta'(s) = -\sum_{p,m}(\log p)p^{-ms} = -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\,,$$

där sista steget fås från Definition 8.2. Vi har då att

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\,, \tag{8.14}$$

för $\mathrm{Re}(s) > 1$. Efter detta följer en integralidentitet som är en alternativ representation av $\psi_1(x)$, och som ytterligare knyter samman zetafunktionen och $\psi_1(x)$.

Proposition 8.10. *För alla $c > 1$ har vi att*

$$\psi_1(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) \mathrm{d}s \,. \tag{8.15}$$

För att kunna bevisa uttrycket för ψ_1 ovan så noterar vi först att vi redan har utvecklat ett nytt uttryck för $-\zeta'/\zeta$ i ekvation (8.14). Kvar har vi alltså att undersöka den resterande integralen och detta gör vi med hjälp av följande lemma.

Lemma 8.11. *Om $c > 0$ har vi att*

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{a^s}{s(s+1)} \mathrm{d}s = \begin{cases} 0\,, & \text{om } 0 < a \leq 1 \\ 1 - 1/a\,, & \text{om } 1 \leq a\,, \end{cases}$$

där integralen går över linjen $Re(s) = c$.

Bevis. Notera först att eftersom $|a^s| = a^c$ så konvergerar integralen. Antag fallet då $1 \leq a$ och beteckna $a = e^\beta$, där $\beta = \log a \geq 0$. Låt då $f(s)$ vara

$$f(s) = \frac{a^s}{s(s+1)} = \frac{e^{\beta s}}{s(s+1)}\,,$$

med poler i $s_0 = 0$ och i $s_1 = -1$. Residyn i dessa punkter är då

$$\begin{aligned} \mathrm{Res}(f, s_0) &= \lim_{s \to s_0} (s - s_0) \frac{a^s}{s(s+1)} = 1\,, \\ \mathrm{Res}(f, s_1) &= \lim_{s \to s_1} (s - s_1) \frac{a^s}{s(s+1)} = -\frac{1}{a}\,. \end{aligned}$$

Betrakta nu kurvan $\Gamma_1(T)$ för $T > 0$. Kurvan består av den vertikala linjen $S(t)$ som går från $c - iT$ till $c + iT$ och halvcirkeln $C(S)$ med centrum i c med radie T, se Figur 8.2. Här väljer vi T stort nog så att konturen innesluter polerna för f som är i punkterna 0 och -1. Från residysatsen får vi att

$$\frac{1}{2\pi i} \int_{\Gamma_1(T)} f(s)\, \mathrm{d}s = \sum_{i=0}^{1} res_{s=s_i} f(s) = 1 - \frac{1}{a}\,,$$

och vi vet att

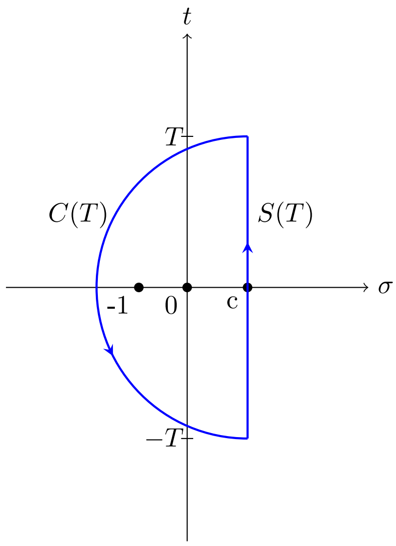
$$\int_{\Gamma_1(T)} f(s)\, \mathrm{d}s = \int_{S(T)} f(s)\, \mathrm{d}s + \int_{C(T)} f(s)\, \mathrm{d}s\,.$$

Om vi nu kan visa att integralen över halvcirkeln $C(T)$ går mot noll när T går mot oändligheten har vi bevisat satsen i fallet $a \geq 1$. Notera att för s på halvcirkeln får vi att

$$|s(s+1)| \geq \frac{T^2}{2}\,,$$

för stora T. Eftersom $\sigma \leq c$ får vi tillslut att

$$\begin{aligned} \left| \int_{C(T)} f(s)\, \mathrm{d}s \right| &= \left| \int_{C(T)} \frac{e^{\beta s}}{s(s+1)} \right| \mathrm{d}s \leq \int_{C(T)} \frac{|e^{\beta s}|}{|s(s+1)|} \mathrm{d}s \leq \\ &\leq \int_{C(T)} \frac{e^{\beta c}}{T^2/2} \mathrm{d}s \leq \frac{2C}{T^2} \int_{C(T)} \mathrm{d}s = \frac{2C}{T^2} \pi T\,, \end{aligned}$$

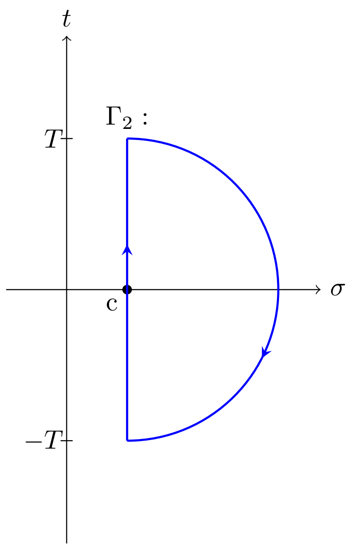


Figur 8.2: *Konturen $\Gamma_1(T)$ bestående av linjen $S(T)$ och halvcirkeln $C(T)$ med polerna $s_0 = 0$ och $s_1 = -1$ utritade.*

som går mot noll när T går mot oändligheten. Detta ger för $1 \leq a$ att

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{a^s}{s(s+1)}\,\mathrm{d}s = 1 - \frac{1}{a}\,.$$

För $0 < a \leq 1$ betraktar vi en liknande kurva, $\Gamma_2(T)$, fast här ligger halvcirkeln till höger om linjen $Re(s) = c$, se Figur 8.3. Vi ser att kurvan inte innesluter några poler, vilket enligt residysatsen



Figur 8.3: *Konturen $\Gamma_2(T)$ där halvcirkeln nu är placerad till höger om $Re(s) = c$.*

ger att integralen över Γ_2 är lika med noll. Liknande argument som i fallet $a \geq 1$ används nu för att visa att integralen över halvcirkeln går mot noll när T går mot oändligheten och beviset är klart. $\square$

Vi har nu samlat på oss tillräckligt med information för att bevisa ekvationen som kopplar samman ψ_1 och zetafunktionen.

Bevis av Proposition 8.10. För att visa uttrycket för ψ_1 i ekvation (8.15) observerar vi från von Mangoldt-funktionen i Definition 8.2 att vi kan skriva

$$\psi(u) = \sum_{n=1}^{\infty} \Lambda(n) f_n(u)\,,$$

där f_n ges av

$$f_n(u) = \begin{cases} 1\,, & \text{om } n \leq u \\ 0\,, & \text{annars} \end{cases}.$$

Använder vi detta får vi att

$$\psi_1(x) = \int_1^x \psi(u)\,\mathrm{d}u = \sum_{n=1}^{\infty} \int_1^x \Lambda(n) f_n(u)\,\mathrm{d}u = \sum_{n\leq x} \Lambda(n) \int_n^x \mathrm{d}u = \sum_{n \leq x} \Lambda(n)(x-n)\,.$$

Från ekvation (8.14) får vi att

$$\begin{aligned} \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\mathrm{d}s &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)}\left(\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\right)\mathrm{d}s = \\ &= x\sum_{n=1}^{\infty}\Lambda(n)\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{(x/n)^s}{s(s+1)}\,\mathrm{d}s\,, \end{aligned}$$

och från Lemma 8.11 där $a = x/n$ får vi att

$$x\sum_{n=1}^{\infty}\Lambda(n)\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{(x/n)^s}{s(s+1)}\,\mathrm{d}s = x\sum_{n=1}^{\infty}\Lambda(n)\left(1-\frac{n}{x}\right) = \psi_1(x)\,.$$

$\square$

8.5 Bevis av asymptoten för ψ_1

För att kunna bevisa primtalssatsen vill vi visa det asymptotiska förhållandet för ψ_1, det vill säga

$$\psi_1(x) \sim \frac{x^2}{2}\,,\ \text{när } x \to \infty\,.$$

Om detta gäller så säger Proposition 8.8 och Proposition 8.9 att

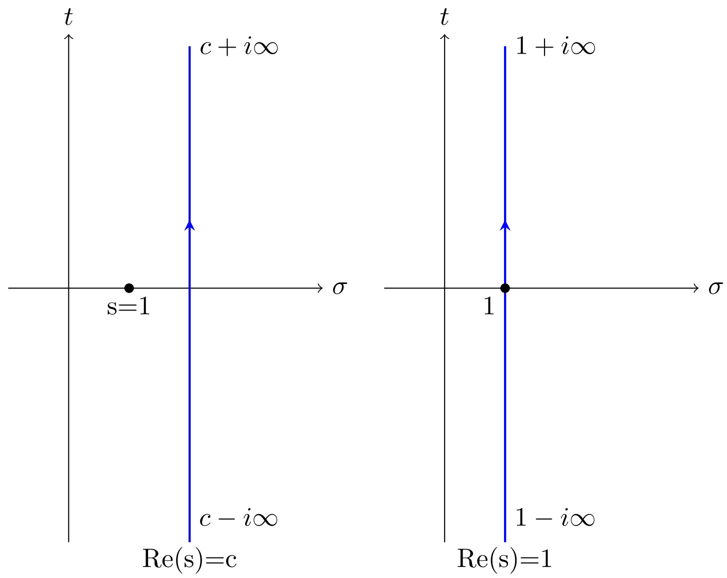
$$\pi(x) \sim \frac{x}{\log x}\,,\ \text{när } x \to \infty\,,$$

vilket visar primtalssatsen, Sats 8.1.

Bevis av Sats 8.1. Som vi konstaterat tidigare vill vi visa att $\psi \sim x^2/2$ när x går mot oändligheten. För att visa detta kommer vi huvudsakligen behöva använda oss utav följande tre argument.

1. Formeln från Proposition 8.10 som kopplar samman ψ_1 och ζ, det vill säga för $c > 1$ har vi att
$$\psi_1(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\,\mathrm{d}s\,.$$
2. Att zetafunktionen enligt Sats 8.5 inte har några nollställen på $\mathrm{Re}(s) = 1$, det vill säga
$$\zeta(1+it) \neq 0, \text{ för alla } t \in \mathbb{R}\,.$$
3. Uppskattningarna av zetafunktionen nära linjen $\mathrm{Re}(s) = 1$ från Proposition 8.7 tillsammans med Proposition 8.6, alltså att
$$\frac{1}{|\zeta(s)|} \leq c_\varepsilon |t|^\varepsilon \quad \text{och} \quad |\zeta'(s)| \leq c'_\varepsilon |t|^\varepsilon\,,$$
för $\sigma \geq 1$ och $|t| \geq 1$.

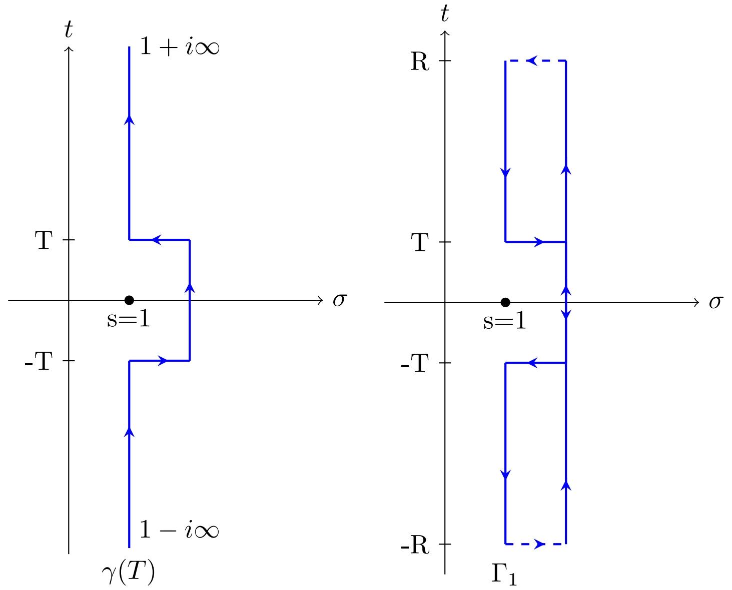
Vår strategi är att i integralen för ψ_1 ändra linjen från $Re(s) = c$ till $Re(s) = 1$, se Figur 8.4. Detta skulle göra att faktorn x^{s+1} i integralen skulle få ordningen x^2, vilket påminner om det vi vill visa. Däremot skulle vi då stöta på problemet att polen till ζ vid $s = 1$ kommer ge oss termen $x^2/2$, vilket är precis asymptoten till ψ_1. Alltså måste vi visa att det som är kvar av ψ_1 måste vara betydligt mindre än termen $x^2/2$. Vi måste därför hitta en grov uppskattning av ordning x^2 när vi integrerar över linjen $Re(s) = 1$.



Figur 8.4: *Till vänster har vi linjen $Re(s) = c$ som ska flyttas till linjen $Re(s) = 1$, till höger.*

Börja med att fixera $c > 1$, låt säga att $c = 2$, och antag att x är fixt med $x \geq 2$. Låt sedan $F(s)$ beteckna
$$F(s) = \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\,.$$

För att kunna flytta linjen till $\mathrm{Re}(s) = 1$ kommer vi behöva göra detta i två steg där vi flyttar linjen en bit i taget. Gör först om den vertikala linjen $Re(s) = c$ till kurvan $\gamma(T)$, se Figur 8.5. Här är den del som ligger på $Re(s) = 1$ när



Figur 8.5: *Till vänster linjen $\gamma(T)$ och till höger kurvan Γ_1 där vi har slagit ihop $Re(s) = c$ och $\gamma(T)$.*

$$\{T \leq t < \infty\} \quad \text{och} \quad \{-\infty < t \leq -T\}\,.$$

Vi har här satt $T \geq 3$, men den kommer väljas större senare. Slå nu upp ihop kurvorna för linjen $Re(s) = c$ och $\gamma(T)$ till kurvan Γ_1, se Figur 8.5. Från Cauchys sats ser vi att eftersom vi inte har några poler i området för Γ_1 får vi att

$$\int_{\Gamma_1} F(s)\,\mathrm{d}s = 0\,,$$

där Γ_1 kan delas upp enligt figuren ovan så att

$$\int_{\Gamma_1} F(s)\,\mathrm{d}s = \int_{c-iR}^{c+iR} F(s)\,\mathrm{d}s - \int_{\gamma(T)} F(s)\,\mathrm{d}s + \int_{c+iR}^{1+iR} F(s)\,\mathrm{d}s + \int_{1-iR}^{c-iR} F(s)\,\mathrm{d}s = 0\,.$$

Om vi kan visa att de två sista integralerna går mot noll när R går mot oändligheten får vi att

$$\psi_1(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(s)\,\mathrm{d}s = \frac{1}{2\pi i}\int_{\gamma(T)} F(s)\,\mathrm{d}s\,. \tag{8.16}$$

Detta kan bekräftas genom att vi från Proposition 8.7 och Proposition 8.6 får att

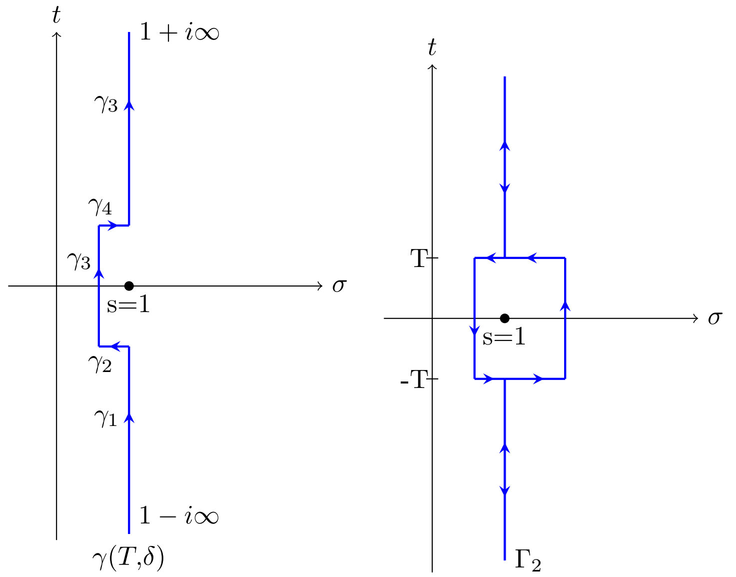
$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leq A|t|^{\eta}\,,\ \text{för något fixt } \eta > 0\,, \tag{8.17}$$

där $s = \sigma + it$ med $\sigma \geq 1$ och $|t| \geq 1$. Detta område innesluter de två rektanglarna som är begränsade av linjen $(c - i\infty, c + i\infty)$ och γ , se Figur 8.5. Vilket ger att

$$|F(s)| \leq A'|t|^{\eta-2}\,,$$

i de två rektanglarna. Eftersom F är holomorf i dessa områden och avtar fort nog när s går mot oändligheten får vi att påståendet i ekvation (8.16) håller.

I nästa steg flyttar vi konturen åter ett steg där vi konstruerar konturen $\gamma(T,\delta)$, se Figur 8.6.



Figur 8.6: *Till vänster har vi konturen $\gamma(T,\delta)$ och till höger kurvan Γ_2 där vi har slagit ihop $\gamma(T)$ och $\gamma(T,\delta)$.*

I konturen $\gamma(T,\delta)$ befinner vi oss nu innanför den kritiska remsan där vi inte vet hur zetafunktionens nollställen beter sig. Men från Sats 8.5, som säger att zetafunktionen inte försvinner på linjen $\mathrm{Re}(s) = 1$, får vi att den inte heller försvinner i ett område väldigt nära linjen heller. För $|t| \leq T$, där T är fixt, väljer vi alltså ett tillräckligt litet $\delta > 0$ så att ζ inte har några nollställen i lådan

$$\{s = \sigma + it, 1 - \delta \leq \sigma \leq 1, |t| \leq T\}.$$

Återigen kombinerar vi två konturer och låter Γ_2 vara kurvan över både $\gamma(T)$ och $\gamma(T,\delta)$ enligt Figur 8.6. Vi konstaterar nu att $F(s)$ endast har en enkelpol vid $s = 1$, vilket kan ses från Följdsats 4.16 i kapitel 4 som säger att

$$\zeta(s) = \frac{1}{s-1} + H(s),$$

där H är holomorf nära $s = 1$. Detta ger att

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s-1} + h(s),$$

där även h är holomorf nära 1. Med uttrycket ovan får vi att residyn av F vid polen $s = 1$ är

$$res_{s=1}F(s) = \lim_{s\to 1}(s-1)\frac{x^{s+1}}{s(s+1)}\left(\frac{1}{s-1} + h(s)\right) = \frac{x^2}{2},$$

och residysatsen ger då att

$$\frac{1}{2\pi i}\int_{\Gamma_2} F(s)\,\mathrm{d}s = \mathrm{Res}(F,1) = \frac{x^2}{2}.$$

Noter nu att Γ_2 kan delas upp i de två integralerna över $\gamma(T)$ och $\gamma(T,\delta)$,

$$\int_{\Gamma_2} F(s)\,\mathrm{d}s = \int_{\gamma(T)} F(s)\,\mathrm{d}s - \int_{\gamma(T,\delta)} F(s)\,\mathrm{d}s,$$

vilket tillsammans ger att

$$\frac{1}{2\pi i}\int_{\gamma(T)} F(s)\,\mathrm{d}s = \frac{x^2}{2} + \frac{1}{2\pi i}\int_{\gamma(T,\,\delta)} F(s)\,\mathrm{d}s\,. \tag{8.18}$$

Nu har vi flyttat integralen närmare $\mathrm{Re}(s) = 1$ och sammanfattningsvis har vi fått ett nytt uttryck för ψ_1. Från ekvationen (8.18) ovan och ekvation (8.16) får vi alltså att

$$\psi_1(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(s)\,\mathrm{d}s = \frac{1}{2\pi i}\int_{\gamma(T)} F(s)\,\mathrm{d}s = \frac{x^2}{2} + \frac{1}{2\pi i}\int_{\gamma(T,\,\delta)} F(s)\,\mathrm{d}s\,. \tag{8.19}$$

Vi ser nu att vi börjar närma oss asymptoten vi vill visa, men för att kunna analysera hur ψ_1 beter sig för stora x vill vi först uppskatta $\gamma(T,\delta)$ med termer av x^2. Detta görs genom att dela upp $\gamma(T,\delta)$ i $\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 + \gamma_5$ så som Figur 8.6 visar och därefter uppskatta varje integral

$$\int_{\gamma_j} F(s)\,\mathrm{d}s, \text{ för } j = 1, \dots, 5\,,$$

med termen x^2. För kurvan γ_1 noterar vi att $\sigma = 1$ vilket ger att

$$|x^{s+1}| = x^{1+\sigma} = x^2\,.$$

Från uppskattningen i ekvation (8.17) kan vi välja exponenten till ett tal mindre än ett, till exempel $\eta = 1/2$, och vi får att

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \le A|t|^{1/2}\,.$$

Använder vi detta får vi för $s = 1 + it$ att

$$\begin{aligned}\left|\int_{\gamma_1} F(s)\,\mathrm{d}s\right| &\le \left|\int_{\gamma_1} \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\mathrm{d}s\right| \le A\int_T^\infty \frac{x^2}{|(1+it)(2+it)|}|t|^{1/2}\,\mathrm{d}t \le \\ &\le Ax^2\int_T^\infty \frac{|t|^{1/2}}{t^2}\,\mathrm{d}t\,.\end{aligned}$$

Vi konstaterar först att integralen på högersidan konvergerar. Välj T stort nog så att

$$\int_T^\infty \frac{|t|^{1/2}}{t^2}\,\mathrm{d}t \le \frac{\varepsilon}{2A}\,,$$

vilket ger oss att

$$\left|\int_{\gamma_1} F(s)\,\mathrm{d}s\right| \le \frac{\varepsilon}{2}x^2\,.$$

Samma argument kan göras för γ_5 där vi också har att $\sigma = 1$ och vi får att

$$\left|\int_{\gamma_5} F(s)\,\mathrm{d}s\right| \le \frac{\varepsilon}{2}x^2\,.$$

På kurvan γ_3 har vi att $\sigma = 1 - \delta$ vilket ger att

$$|x^{s+1}| = x^{1+\sigma} = x^{1+1-\delta} = x^{2-\delta}\,.$$

Efter att nu ha fixerat T så väljer vi δ tillräckligt litet. Vi konstaterar nu att det finns ett C_T som beror av T så att

$$\left|\int_{\gamma_3} F(s)\,\mathrm{d}s\right| \le \int_{-T}^{T} \frac{x^{2-\delta}}{|(1-\delta+it)(2-\delta+it)|}\left|\frac{\zeta'(1-\delta+it)}{\zeta(1-\delta+it)}\right| \mathrm{d}t \le C_T x^{2-\delta}\,.$$

Till slut kommer vi till kurvorna γ_2 och γ_4 som beter sig väldigt liknande. För uppskattningen av γ_2 har vi att $s = \sigma - iT$ för ett fixt T och vi har att det finns ett C'_T vilket ger att

$$\begin{aligned}\left|\int_{\gamma_2} F(s)\,\mathrm{d}s\right| &\le \int_{1-\delta}^{1} \frac{x^{\sigma+1}}{|(\sigma-iT)(\sigma+1-iT)|}\left|\frac{\zeta'(\sigma-iT)}{\zeta(\sigma-iT)}\right| \mathrm{d}\sigma \le C'_T \int_{1-\delta}^{1} x^{\sigma+1}\,\mathrm{d}\sigma = \\ &= C'_T\left[\frac{x^{\sigma+1}}{\log x}\right]_{1-\delta}^{1} = C'_T\left(\frac{x^2}{\log x} - \frac{x^{2-\delta}}{\log x}\right) \le C'_T\frac{x^2}{\log x}\,.\end{aligned}$$

En liknande uppskattning kan göras även för γ_4. När vi nu har uppskattat alla integraler kan vi uppskatta hela integralen över $\gamma(T,\delta)$ och vi får från ekvation (8.19) att

$$\begin{aligned}\left|\psi_1(x) - \frac{x^2}{2}\right| &= \left|\frac{1}{2\pi i}\int_{\gamma(T,\delta)} \frac{x^{s+1}}{s(s+1)} F(s)\,\mathrm{d}s\right| \le \\ &\le \varepsilon x^2 + C_T x^{2-\delta} + 2C'_T\frac{x^2}{\log x}\,.\end{aligned}$$

Dela nu båda sidorna av uttrycket ovan med $x^2/2$ och vi får att

$$\left|\frac{2\psi_1(x)}{x^2} - 1\right| \le 2\varepsilon + 2C_T x^{-\delta} + 2C'_T\frac{1}{\log x}\,.$$

För stora x ser vi att de två sista termerna i högerledet kan uppskattas som mindre än ε, det vill säga för stora x har vi att

$$\left|\frac{\psi_1(x)2}{x^2} - 1\right| \le 2\varepsilon + \varepsilon + \varepsilon = 4\varepsilon\,.$$

Vi har nu visat att

$$\psi_1(x) \sim \frac{x^2}{2}\,,\ \text{när } x \to \infty\,,$$

och från Proposition 8.9 får vi att

$$\pi(x) \sim \frac{x}{\log x}\,,\ \text{när } x \to \infty\,.$$

□

Kapitel 9

Två- och fyrkvadratssatsen

I det här avsnittet kommer huvudfokus ligga på att studera summor av kvadrater. Själva intresset till det här uppkom på Pythagoras tid då man insåg att för rätvinkliga trianglar kommer kvadraten av hypotenusan, c, vara lika med summan av de kvadrerade kateterna, a och b, det vill säga att $c^2 = a^2 + b^2$. Låt säga att både a och b är heltal, då skulle detta medföra att även $c^2 = n$ är ett heltal. Frågan man då ställde sig var för vilka n detta gäller, alltså vilka heltal kan uttryckas som en summa av två kvadrater? Man ställde sig även frågan på hur många olika sätt detta kan göras för varje heltal? Det är precis dessa två frågor som gav upphov till de två kända satserna två- och fyrkvadratssatsen.

Rätt så snabbt insåg man att det inte går att uttrycka alla heltal som en summa av två kvadrater och inte heller som en summa av tre kvadrater. Frågan som då återstod var om alla positiva heltal kan uttryckas som en summa av fyra kvadrater, vilket verkade stämma då man inte hittade något positivt heltal där detta inte gäller. Men något egentligt bevis för detta fick man först långt senare då man hade börjat studera elliptiska funktioner, och framförallt fått teorin för Jacobis thetafunktion.

9.1 Bevisidé

Vi kommer märka att både två- och fyrkvadratssatsen i sig är ganska okomplicerade, men detta gäller inte för bevisen. Därför kommer vi punkta upp de huvudsakliga stegen man gör i bevisen, både för att få en idé över tankegången och för att inse vad vi kommer behöva för teori. Men först skriver vi upp formuleringarna av satserna och vi börjar med tvåkvadratssatsen.

Sats 9.1 (Tvåkvadratssatsen)**.** *Om $n \geq 1$ gäller att*

$$r_2(n) = 4(d_1(n) - d_3(n))\,. \tag{9.1}$$

Här betecknar $r_2(n)$ antalet gånger ett positivt heltal n kan skrivas som en summa av två kvadrater. Vi låter k vara ett positivt heltal eller noll och har att $d_1(n)$ definierar antalet delare till n på formen $4k + 1$ och att $d_3(n)$ definierar antalet delare till n på formen $4k + 3$. Vi går nu över till att formulera fyrkvadratssatsen.

Sats 9.2 (Fyrkvadratssatsen)**.** *Varje positivt heltal kan skrivas som en summa av fyra kvadrater och för alla $n \geq 1$ gäller att*

$$r_4(n) = 8\sigma_1^*(n)\,. \tag{9.2}$$

Här betecknar $r_4(n)$ antalet sätt n kan skrivas som en summa av fyra kvadrater och $\sigma_1^*(n)$ betecknar summan av delare till n som inte är delbara med 4.

Exempel. Vi väljer att betrakta Sats 9.1 för det positiva heltalet 1. Vi börjar med vänsterledet i (9.1) och sätter $n = 1$. Vi vet att talet 1 kan skrivas som en summa av två kvadrater enligt

$$(\pm 1)^2 + 0^2 = 1\,,$$

eller enligt

$$0^2 + (\pm 1)^2 = 1\,.$$

Således kommer $r_2(1) = 4$, eftersom vi kan uttrycka 1 som en summa av två kvadrater på fyra olika sätt. Om vi nu istället betraktar högerledet i (9.1) och sätter $n = 1$ får vi att

$$4(d_1(1) - d_3(1)) = 4(1 - 0) = 4\,.$$

Vi har nu fått att för $n = 1$ gäller (9.1), eftersom både vänster- och högerled är lika med 4.

Vi väljer nu att betrakta Sats 9.2 för det positiva heltalet 1. Vi börjar med vänsterledet i ekvation (9.2) och sätter $n = 1$. Vi vet att talet 1 kan skrivas som en summa av fyra kvadrater enligt

$$\begin{aligned}
(\pm 1)^2 + 0^2 + 0^2 + 0^2 &= 1\,,\\
0^2 + (\pm 1)^2 + 0^2 + 0^2 &= 1\,,\\
0^2 + 0^2 + (\pm 1)^2 + 0^2 &= 1\,,\\
0^2 + 0^2 + 0^2 + (\pm 1)^2 &= 1\,.
\end{aligned}$$

Således kommer $r_4(1) = 8$, eftersom vi kan uttrycka 1 som en summa av fyra kvadrater på åtta olika sätt. Om vi nu istället betraktar högerledet i ekvation (9.1) och sätter $n = 1$ får vi att

$$8\sigma_1^*(1) = 8 * 1 = 8\,.$$

Vi har nu fått att för $n = 1$ gäller ekvation (9.2), eftersom både vänster- och högerled är lika med 8.

I exemplet ovan har vi nu visat att både två- och fyrkvadratssatsen gäller för $n = 1$. För att visa att dessa satser gäller för alla positiva heltal n kommer vi behöva en annan tankegång och vi delar upp detta i ett antal steg.

1. Sekvenserna $r_2(n)$ och $r_4(n)$ är båda talföljder som är jobbiga att studera direkt. Därför vill vi skriva om dessa sekvenser till något vi kan jobba med analytiskt, så det första vi kommer behöva göra är att hitta en så kallad genererande funktion för $r_2(n)$ respektive $r_4(n)$. Det kommer visa sig att dessa genererande funktioner kommer båda vara en potens av thetafunktionen $\theta(\tau)$.

2. Vi vill nu hitta en ny identitet som är ekvivalent med den identitet vi har i satsen, alltså ekvivalent med (9.1) respektive (9.2). Denna nya identitet kommer bland annat innehålla vår generande funktion från steg 1.

3. När vi har lyckats visa att vår nya identitet är ekvivalent med den i satsen räcker det att visa att vår nya identitet håller. Vi delar upp beviset av den nya identiteten i två steg.

(a) Först måste vi visa att vänster- och högerled i vår nya identitet uppfyller samma strukturella egenskaper. För att kunna gå vidare till nästa steg kommer vi att visa att strukturella likheter räcker för att identiteten ska hålla. Detta kommer att följa analogt med Sats 6.2, men beviset är väsentligt mer invecklat.

(b) Nu återstår att visa att förhållandet mellan vänster- och högerled är konstant. Om detta gäller är beviset av två- respektive fyrkvadratssatsen färdigt.

9.2 Genererande funktioner

I steg 1 i vår steglista över två- och fyrkvadratssatsens bevis nämnde vi att sekvenserna $r_2(n)$ och $r_4(n)$ är jobbiga sekvenser att studera. Därför vill vi skriva om dessa sekvenser som genererande funktioner, vilka vi kommer kunna studera analytiskt. Att studera deras genererande funktioner kan i sin tur leda till nya insikter om sekvenserna. Det är detta som gör genererande funktioner till ett väldigt kraftfullt verktyg, vilket ofta används inom talteorin. I vårt fall så kommer vi definiera en genererande funktion enligt följande

Definition 9.1. *Givet en sekvens av tal $\{F_n\}_{n=0}^{\infty}$ så kan dess genererande funktion definieras som*

$$F(x) = \sum_{n=0}^{\infty} F_n x^n \,.$$

9.3 Egenskaper för $\theta(\tau)$

I steg 1 i vår steglista för beviset av två- och fyrkvadratssatsen vill vi koppla $r_2(n)$ respektive $r_4(n)$ till en genererande funktion. Denna genererande funktion kommer vara en potens av $\theta(\tau)$, $\tau \in \mathbb{H}$, och senare i steg 3a kommer vi studera de strukturella egenskaperna hos denna funktion. Därför formulerar vi nu en proposition med dessa egenskaper.

Proposition 9.3. *Funktionen θ som är definierad i det övre komplexa halvplanet uppfyller egenskaperna*

(i) $\theta(\tau+2) = \theta(\tau)$

(ii) $\theta(-1/\tau) = \sqrt{\tau/i}\theta(\tau)$

(iii) $\theta(\tau) \to 1$ *då* $Im(\tau) \to \infty$

(iv) $\theta(1-1/\tau) \approx \sqrt{\tau/i}2e^{\pi i\tau/4}$ *då* $Im(\tau) \to \infty$,

där vi låter $\sqrt{\tau/i}$ endast beteckna de positiva rötterna, alltså $\sqrt{\tau/i} \in \mathbb{H}$.

Bevis. Från definitionen av $\theta(\tau)$ får vi att (i) gäller, detta kan ses genom att lägga in $\tau + 2$ i θ.

För att bevisa (ii) kommer vi att använda oss av den ursprungliga Jacobis thetafunktion, Θ. Vi kommer först studera hur Θ beter sig under transformationen $\tau \to -1/\tau$ och använder därefter relationen mellan dem, det vill säga sätter $z = 0$. För att se vad som händer med Jacobis thetafunktion, Θ under transformationen formulerar vi följande sats.

Sats 9.4. *Om $\tau \in \mathbb{H}$ så har vi att*

$$\Theta(z|-1/\tau) = \sqrt{\frac{\tau}{i}} e^{\pi i \tau z^2} \Theta(z\tau|\tau) \,, \tag{9.3}$$

för alla $z \in \mathbb{C}$.

Bevis av Sats 9.4. Vi noterar att både vänster- och högerleden i ekvation (9.3) beskriver holomorfa funktioner i z och τ. Tack vare analytisk fortsättning vet vi då att de båda funktionerna kommer vara identiska i hela det komplexa talplanet om vi bevisar satsen för $z = a$ där a är reellt och för $\tau = it$ med $t > 0$.

Vi börjar med att betrakta högerledet i (9.3) med $z = a$ och $\tau = it$ och får att

$$\sqrt{\frac{\tau}{i}} e^{\pi i \tau z^2} \Theta(z\tau|\tau) = t^{1/2} e^{-\pi t a^2} \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} e^{-2\pi n a t} = t^{1/2} \sum_{n=-\infty}^{\infty} e^{-\pi t (n+a)^2} . \tag{9.4}$$

Vi vill nu visa att detta kommer vara lika med vårt vänsterled genom att använda Poissions summationsformel. För att kunna göra det studerar vi först funktionen $f(x) = e^{-\pi x^2}$. Vi vet sedan innan att den här funktionen är sin egen fouriertransform eftersom

$$\int_{-\infty}^{\infty} e^{-\pi x^2} e^{-2\pi i x \xi} \, \mathrm{d}x = e^{-\pi \xi^2} .$$

Vi fixerar värdena på $t > 0$ och $a \in \mathbb{R}$ och ser att om vi då ändrar i integralen så att $x \mapsto t^{1/2}(x+a)$ har vi att fouriertransformen av

$$f(x) = e^{-\pi t (x+a)^2} \quad \text{är} \quad \hat{f}(\xi) = t^{-1/2} e^{\frac{-\pi \xi^2}{t}} e^{2\pi i \xi a} .$$

Vi använder nu Poissons summationsformel och får att

$$t^{1/2} \sum_{n=-\infty}^{\infty} e^{-\pi t (n+a)^2} = t^{1/2} \sum_{n=-\infty}^{\infty} t^{-1/2} e^{\frac{-\pi n^2}{t}} e^{2\pi i n a} = \sum_{n=-\infty}^{\infty} e^{\frac{-\pi n^2}{t}} e^{2\pi i n a} ,$$

där vi vet att

$$\sum_{n=-\infty}^{\infty} e^{\frac{-\pi n^2}{t}} e^{2\pi i n a} = \Theta(a| - 1/it) .$$

□

Sätter vi nu $z = 0$ i denna sats får vi enligt relationen mellan Jacobis thetafunktion, Θ, och dess variant, θ, att (ii) i Proposition 9.3 gäller.

Egenskap (iii) från propositionen följer även den direkt från definitionen av θ, ty termen då $n = 0$ är 1 och de resterande termerna går mot noll då imaginärdelen av τ går mot oändligheten.

För att bevisa (iv) analyserar vi beteendet av $\theta(\tau)$ då τ går mot 1. För att visa detta kommer vi använda nästa följdsats och låta $\mathrm{Im}(\tau)$ gå mot oändligheten.

Följdsats 9.5. *Om $\tau \in \mathbb{H}$ gäller att*

$$\theta(1 - 1/\tau) = \sqrt{\frac{\tau}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i (n+1/2)^2 \tau} .$$

Bevis av Följdsats 9.5. Vi börjar beviset med att notera att n och n^2 båda antar varannan udda och vartannat jämnt tal och får att

$$\theta(1 + \tau) = \sum_{n=-\infty}^{\infty} (-1)^{n^2} e^{i\pi n^2 \tau} = \sum_{n=-\infty}^{\infty} (-1)^n e^{i\pi n^2 \tau} = \Theta(1/2|\tau) .$$

Om vi sätter $\tau = -1/\tau$ får vi att

$$\theta(1 - 1/\tau) = \Theta(1/2| - 1/\tau)\,.$$

Använd nu sats 9.4 med $z = 1/2$, vi får då att

$$\begin{aligned}\theta(1 - 1/\tau) = \Theta(1/2| - 1/\tau) &= \sqrt{\frac{\tau}{i}}e^{\pi i\tau/4}\Theta(\tau/2|\tau) = \\ &= \sqrt{\frac{\tau}{i}}e^{\pi i\tau/4}\sum_{n=-\infty}^{\infty} e^{\pi i n^2\tau}e^{\pi i n\tau} = \\ &= \sqrt{\frac{\tau}{i}}\sum_{n=-\infty}^{\infty} e^{\pi i(n+1/2)^2\tau}\,.\end{aligned}$$

□

För att visa egenskap (iv) i Proposition 9.3 använder vi att termerna från summan då $n = 0$ och $n = -1$ summeras till $2e^{\pi i\tau/4}$, och att resterande termer är av ordning $O(e^{-9\pi t/4})$, vilket ger att egenskapen gäller. □

Vi ska nu definiera en ny funktion Dedekinds etafunktion, $\eta(\tau)$, som behövs i beviset av fyrkvadratssatsen.

Definition 9.2. *För $Im(\tau) > 0$ är Dedekinds etafunktion definierad som*

$$\eta(\tau) = e^{\frac{\pi i\tau}{12}}\prod_{n=1}^{\infty}(1 - e^{2\pi i n\tau})\,.$$

Funktionalekvationen för $\eta(\tau)$ kommer vara relevant när vi bevisar fyrkvadratssatsen, därav formulerar vi följande proposition.

Proposition 9.6. *För $Im(\tau) > 0$ gäller att*

$$\eta(-1/\tau) = \sqrt{\frac{\tau}{i}}\eta(\tau)\,.$$

Denna ekvation kallas även för η's funktionalekvation.

Bevis. Vi vet från Sats 7.3 att thetafunktionen kan uttryckas som en produkt enligt trippelprodukten, $\Pi(z|\tau)$. Med $q = e^{\pi i\tau}$ får vi att

$$\begin{aligned}\Theta(z|\tau) &= \prod_{n=1}^{\infty}(1 - q^{2n})(1 + q^{2n-1}e^{2\pi iz})(1 + q^{2n-1}e^{-2\pi iz}) = \\ &= (1 + qe^{-2\pi iz})\prod_{n=1}^{\infty}(1 - q^{2n})(1 + q^{2n-1}e^{2\pi iz})(1 + q^{2n+1}e^{-2\pi iz})\,,\end{aligned}$$

där första faktorn är noll i punkten $z_0 = 1/2 + \tau/2$. Det här ger att vid derivering med avseende på z kommer alla termer i punkten z_0 vara noll utom termen då vi deriverar första faktorn. Vi får då att

$$\Theta'(z_0|\tau) = 2\pi i H(\tau), \quad \text{där } H(\tau) = \prod_{n=1}^{\infty}(1 - e^{2\pi i n\tau})^3\,.$$

Ta nu $\tau = -1/\tau$ i ekvation (9.3), detta ger oss att

$$\Theta(z|\tau) = \sqrt{\frac{i}{\tau}} e^{-\pi i z^2/\tau} \Theta(-z/\tau| - 1/\tau) .$$

Om vi deriverar detta uttryck med avseende på z och sedan sätter $z = z_0$ får vi att

$$2\pi i H(\tau) = \sqrt{\frac{i}{\tau}} e^{-\frac{\pi i}{4\tau}} e^{-\frac{\pi i}{2}} e^{-\frac{\pi i \tau}{4}} \left(\frac{-2\pi i}{\tau}\right) H(-1/\tau) .$$

Det här ger oss att

$$e^{\frac{\pi i \tau}{4}} H(\tau) = \left(\frac{i}{\tau}\right)^{3/2} e^{-\frac{\pi i}{4\tau}} H(-1/\tau) .$$

Från definitionen av $\eta(\tau)$ ser vi att då τ är rent imaginär så kommer funktionen vara positiv. Det här gör att vi kan ta tredjeroten ur uttrycket ovan och får då att

$$\eta(\tau) = \sqrt{\frac{i}{\tau}} \eta(-1/\tau) .$$

Eftersom både höger- och vänsterled i uttrycket ovan beskriver holomorfa funktioner så har vi med hjälp av analytisk fortsättning att identiteten gäller för alla τ i det övre komplexa halvplanet. $\square$

9.4 Tvåkvadratssatsen

Vi har nu äntligen tillräckligt med kött på benen för att kunna bevisa tvåkvadratssatsen. Vi påminner om att satsen säger på hur många sätt ett positivt heltal n kan skrivas som en summa av två kvadrater. Detta uttrycktes i satsen som

$$r_2(n) = 4(d_1(n) - d_3(n)) , \tag{9.5}$$

där vi lät $r_2(n)$ beteckna antalet sätt ett positivt heltal n kan skrivas som en summa av två kvadrater och $d_1(n)$ och $d_3(n)$ betecknar antalet delare till n på formen $4k + 1$ respektive $4k + 3$.

Bevis av tvåkvadratssatsen. Vi börjar beviset av tvåkvadratssatsen med att göra steg 1 i steglistan av beviset, det vill säga hitta en genererande funktion för sekvensen $r_2(n)$. De trevliga egenskaperna hos just θ-funktionen gör att vi kan uttrycka den genererade funktionen som en potens av θ, nämligen att

$$\theta(\tau)^2 = \sum_{n=0}^{\infty} r_2(n) q^n ,$$

där $q = e^{\pi i \tau}$ och $\tau \in \mathbb{H}$. För att visa att identiteten ovan gäller utgår vi från definitionerna av $r_2(n)$ och θ och vi har att

$$\theta(\tau) = \sum_{n=-\infty}^{\infty} q^{n^2} .$$

Det här ger att

$$\begin{aligned}\theta(\tau)^2 &= \sum_{n_1=-\infty}^{\infty} q^{n_1^2} \sum_{n_2=-\infty}^{\infty} q^{n_2^2} = \\ &= \sum_{(n_1,n_2)\in\mathbb{Z}\times\mathbb{Z}} q^{n_1^2+n_2^2} = \\ &= \sum_{n=0}^{\infty} r_2(n) q^n \,,\end{aligned}$$

där sista likheten gäller ty $r_2(n)$ räknar antalet par (n_1, n_2) sådana att $n = n_1^2 + n_2^2$.

Vi är nu klara med första steget i steglistan och går vidare till steg 2 där vi vill hitta en funktion som genom förhållandet till vår genererande funktion θ^2 uttrycker en identitet som är ekvivalent med den i satsen.

Proposition 9.7. *Identiteten*

$$r_2(n) = 4(d_1(n) - d_3(n)) \,, \tag{9.6}$$

där $n \geq 1$ är ekvivalent med

$$\theta(\tau)^2 = 2 \sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} \,, \tag{9.7}$$

då $q = e^{\pi i \tau}$ och $\tau \in \mathbb{H}$.

Bevis av Proposition 9.7. För att visa detta vill vi visa att vänster- och högerleden i likheterna relaterar till varandra på liknande sätt. Eftersom vi redan visat att θ^2 relaterar till $r_2(n)$ genom dess genererande funktion återstår nu att visa att högerleden relaterar till varandra på ett liknande sätt.

Vi börjar med att utveckla högerledet i (9.7) och vi vet att för positiva n så är

$$\frac{1}{q^n + q^{-n}} = \frac{q^n}{1 + q^{2n}} \,,$$

vilket ger att

$$2 \sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} = 1 + 4 \sum_{n=1}^{\infty} \frac{q^n}{1 + q^{2n}} \,.$$

Vidare har vi att

$$\frac{1}{1 + q^{2n}} = \frac{1 - q^{2n}}{1 - q^{4n}} \,,$$

vilket gör att

$$2 \sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} = 1 + 4 \sum_{n=1}^{\infty} \frac{q^n}{1 + q^{2n}} = 1 + 4 \sum_{n=1}^{\infty} \left(\frac{q^n}{1 - q^{4n}} - \frac{q^{3n}}{1 - q^{4n}} \right) \,.$$

I enlighet med geometrisk summa har vi att

$$\frac{1}{1 - q^{4n}} = \sum_{m=0}^{\infty} q^{4nm} \,. \tag{9.8}$$

Vi vet sedan innan att $d_1(k)$ betecknar antalet delare till k på formen $4m+1$, vilket tillsammans med (9.8) ger att

$$\sum_{n=1}^{\infty} \frac{q^n}{1-q^{4n}} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^{n(4m+1)} = \sum_{k=1}^{\infty} d_1(k) q^k \,.$$

På liknande sätt har vi även att

$$\sum_{n=1}^{\infty} \frac{q^{3n}}{1-q^{4n}} = \sum_{k=1}^{\infty} d_3(k) q^k \,.$$

□

Vi har nu visat att identiteten (9.6) är ekvivalent med (9.7) och är därav färdiga med andra steget i vår steglista. Vi går vidare till steg 3, där det gäller att visa att vår nya identitet, (9.7), håller. Enligt steglistan kan detta delas upp i två delar där första delen är att visa att vänster- och högerled i (9.7) har samma strukturella egenskaper.

För att kunna göra detta börjar vi med att skriva om högerledet i (9.7) med hjälp Eulers formler för cosinus i form av exponentialfunktionen, och får att

$$2\sum_{n=-\infty}^{\infty} \frac{1}{q^n+q^{-n}} = \sum_{n=-\infty}^{\infty} \frac{1}{\cos(n\pi\tau)} \,,$$

där $q = e^{\pi i \tau}$ och $\tau \in \mathbb{H}$. Vi definierar summan i högerledet som $\mathcal{C}(\tau)$. Vi vill nu istället visa att $\theta(\tau)^2 = \mathcal{C}(\tau)$ genom att först visa att de har samma strukturella egenskaper. Vi formulerar detta i en proposition.

Proposition 9.8. *Funktionen $\mathcal{C}(\tau) = \sum 1/\cos(\pi n\tau)$ som är definierad i det övre komplexa halvplanet uppfyller egenskaperna*

(i) $\mathcal{C}(\tau+2) = \mathcal{C}(\tau)$

(ii) $\mathcal{C}(\tau) = (i/\tau)\mathcal{C}(-1/\tau)$

(iii) $\mathcal{C}(\tau) \to 1$ *då* $Im(\tau) \to \infty$

(iv) $\mathcal{C}(1-1/\tau) \approx 4(\tau/i)e^{\pi i\tau/2}$ *då* $Im(\tau) \to \infty$.

Dessa egenskaper gäller även för $\theta(\tau)^2$.

Bevis av Proposition 9.8. Från Proposition 9.3 får vi att alla egenskaper i propositionen gäller för $\theta(\tau)^2$.

Vi vill nu visa att alla egenskaper även gäller för $\mathcal{C}(\tau)$ och börjar med att visa (i), vilken följer direkt från definitionen av $\mathcal{C}(\tau)$.

För att visa (ii) börjar vi med att vi vet att $1/\cosh \pi x$ är sin egen Fouriertransform, se ekvation 2.7 i exemplet i kapitel 2. Vi har alltså att

$$\int_{-\infty}^{\infty} \frac{e^{-2\pi i x\xi}}{\cosh \pi x}\, \mathrm{d}x = \frac{1}{\cosh \pi \xi} \,.$$

Detta ger att Fouriertransformen av $f(x) = e^{-2\pi iax}/\cosh(\pi x/t)$ för $t > 0$ och där a är reellt är $\hat{f}(x) = t/\cosh(\pi(\xi + a)t)$. Enligt Poissons summationsformel får vi då att

$$\sum_{n=-\infty}^{\infty} \frac{e^{-2\pi ian}}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{t}{\cosh(\pi(n+a)t)} . \tag{9.9}$$

Om vi sätter $a = 0$ i uttrycket ovan så får vi att

$$\frac{1}{t} \sum_{n=-\infty}^{\infty} \frac{1}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{1}{\cosh(\pi nt)} .$$

Vi vet att för alla reella x så är $\cos ix = \cosh x$ och vi får med hjälp av uttrycket ovan att

$$(i/\tau)\mathcal{C}(-1/\tau) = \mathcal{C}(\tau) ,$$

för $\tau = it$ och $t > 0$. Vänster- och högerled i ekvationen ovan är båda holomorfa funktioner och därför ger analytisk fortsättning oss att detta gäller för alla $\tau \in \mathbb{H}$.

Vidare har vi att (iii) följer direkt från definitionen av $\mathcal{C}(\tau)$.

Kvar att visa är att (iv) gäller och vi börjar med att undersöka hur $\mathcal{C}(\tau)$ beter sig då $\tau = 1$. För att göra detta studerar vi $\mathcal{C}(1 - 1/\tau)$ och låter τ gå mot oändligheten. Vi kommer använda oss av Poissons summationsformel och börjar med att sätta $a = 1/2$ i ekvation (9.9) och får att

$$\sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cosh(\pi n/t)} = t \sum_{n=-\infty}^{\infty} \frac{1}{\cosh(\pi(n+1/2)t)} . \tag{9.10}$$

Vi har att för $\tau = it$, där $t > 0$ så gäller att

$$\begin{aligned} \mathcal{C}(1 - 1/\tau) &= \sum_{n=-\infty}^{\infty} \frac{1}{\cos(\pi n(1 - 1/\tau))} = \\ &= \sum_{n=-\infty}^{\infty} \frac{1}{\cos(\pi n)\cos(\pi n/\tau)} , \end{aligned}$$

där vi i nämnaren har använt oss av att $\cos(x - y) = \cos(x)\cos(y) + \sin(x)\sin(y)$. Vidare har vi att

$$\begin{aligned} \mathcal{C}(1 - 1/\tau) &= \sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cos(\pi n/\tau)} = \\ &= \sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cosh(\pi n/t)} = \\ &= t \sum_{n=-\infty}^{\infty} \frac{1}{\cosh(\pi(n+1/2)t)} = \\ &= \left(\frac{\tau}{i}\right) \sum_{n=-\infty}^{\infty} \frac{1}{\cos(\pi(n+1/2)\tau)} , \end{aligned}$$

där det näst sista steget fås från ekvation (9.10). Analytisk fortsättning ger oss att detta gäller för alla τ i det övre komplexa talplanet.

Då t går mot oändligheten kommer termerna då $n = 0$ och $n = -1$ i den här summan vara de termer som ger störst bidrag, vilket ger att för $\tau = \sigma + it$ så är

$$\mathcal{C}(1 - 1/\tau) = 4\left(\frac{\tau}{i}\right) e^{\pi i \tau/2} + O(|\tau| e^{-3\pi t/2}),$$

då t går mot oändligheten. □

Vi har nu visat att $\theta(\tau)^2$ och $\mathcal{C}(\tau)$ uppfyller samma strukturella egenskaper. Vi går vidare till steg 3b i steglistan och vill visa att förhållandet mellan funktionerna är konstant lika med 1. För att kunna göra detta behöver vi följande sats, där i vårt fall funktionen $f = \mathcal{C}/\theta^2$.

Sats 9.9. *Anta att f är en holomorf funktion i det övre komplexa halvplanet som uppfyller*

(i) $f(\tau + 2) = f(\tau)$

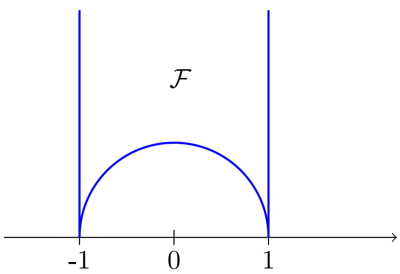
(ii) $f(-1/\tau) = f(\tau)$

(iii) $f(\tau)$ *är begränsad.*

Då gäller att f är konstant.

För att kunna bevisa denna sats börjar vi med att definiera en delmängd av det slutna övre komplexa halvplanet. Vi kallar området för $\mathcal{F}$ och definierar det som

$$\mathcal{F} = \{\tau \in \overline{\mathbb{H}} : |\mathrm{Re}(\tau)| \leq 1 \text{ and } |\tau| \geq 1\}.$$



Figur 9.1: *Området $\mathcal{F}$.*

Genom att använda oss av det här området kommer vi kunna studera hur funktionen f beter sig i hela det övre komplexa halvplanet. För att inse detta kan man studera de två transformationerna i följande lemma, vilka genom upprepningar och kombinationer avbildar alla punkter i det övre komplexa halvplanet på vårt område $\mathcal{F}$.

Lemma 9.10. *Varje punkt i det övre komplexa halvplanet kan avbildas på $\mathcal{F}$ genom kombinationer av följande rationella linjärtransformationer och deras inverser:*

$$T_2 : \tau \to \tau + 2, \quad S : \tau \to -1/\tau.$$

Bevis av lemma 9.10. Vi börjar med att låta G beteckna gruppen som genereras av T_2 och S. Vi vet då att ett element $g \in G$ kan skrivas som

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

där vi har att

$$g(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Eftersom matriserna som representerar transformationerna T_2 och S har heltalskoefficienter och determinanter som är lika med 1, så har alla matriser g i gruppen G samma egenskaper. Det här beror på att om vi multiplicerar två sådana matriser med varandra så kommer produkten vara en matris med samma egenskaper, alltså en matris med heltalskoefficienter och med en determinant som är lika med 1. Notera att

$$\begin{aligned} 2\mathrm{Im}(g(\tau)) &= \frac{a\tau + b}{c\tau + d} - \frac{a\overline{\tau} + b}{c\overline{\tau} + d} = \\ &= \frac{(c\overline{\tau} + d)(a\tau + b) - (c\tau + d)(a\overline{\tau} + b)}{|c\tau + d|^2} = \\ &= \frac{(ad - bc)\tau - (ad - bc)\overline{\tau}}{|c\tau + d|^2} = \\ &= \frac{\tau - \overline{\tau}}{|c\tau + d|^2} = \frac{2\mathrm{Im}(\tau)}{|c\tau + d|^2}. \end{aligned}$$

Sista ledet fås av att $(ad - bc)$ är lika med determinanten som vi vet är lika med 1. Det här ger alltså att

$$\mathrm{Im}(g(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}.$$

Låt nu $\tau \in \mathbb{H}$ och $g \in G$. Vidare kan vi välja $g_0 \in G$ så att $\mathrm{Im}(g_0(\tau))$ blir maximal. Eftersom translationen T_2 inte ändrar imaginärdelen, kan vi applicera den transformationen upprepade gånger och ändå behålla den maximala imaginärdelen. Detta ger att vi kan hitta ett $g_1 \in G$ med $|\mathrm{Re}(g_1(\tau))| \leq 1$ och med maximal imaginärdel.

Vi vill nu visa att $|g_1(\tau)| \geq 1$ för att kunna säga att $g_1 \in \mathcal{F}$ enligt definitionen för mängden. Men om detta inte vore sant, det vill säga om $|g_1(\tau)| < 1$ så skulle vi ha att

$$\mathrm{Im}(Sg_1(\tau)) = \mathrm{Im}(-1/g_1(\tau)) = -\frac{\mathrm{Im}(\overline{g_1(\tau)})}{|g_1(\tau)|^2} > \mathrm{Im}(g_1(\tau)),$$

och det hade motsagt att $\mathrm{Im}(g_1(\tau))$ är maximal. Det här innebär alltså att $|g_1(\tau)| \geq 1$, vilket innebär att $g_1 \in \mathcal{F}$. $\square$

Vi har nu visat att alla tal i det övre komplexa halvplanet kan avbildas på vårt område $\mathcal{F}$. För att nu bevisa Sats 9.9 kommer vi använda oss av den så kallade maximumprincipen, en metod inom komplexanalysen som säger att om vi har en holomorf funktion så kommer dess maximala belopp antas på randen till dess område. Om det istället skulle visa sig att den holomorfa funktionen har ett maximum i det inre av området så är funktionen enligt maximumprincipen konstant. Genom att i beviset anta att vår funktion f, som vi vet är holomorf, inte är konstant ska vi nu undersöka huruvida den antar sitt maximala värde på randen, om inte så motsäger detta maximumprincipen och vi får det vi vill, det vill säga att f måste vara konstant.

Bevis av sats 9.9. Anta att f inte är konstant och låt $g(z) = f(\tau)$, där $z = e^{\pi i \tau}$. Funtionen g är väldefinierad för z på den punkterade enhetsskivan eftersom f är periodisk med perioden 2. Vidare vet vi från tredje egenskapen i satsen att f är begränsad, vilket gör att g kommer vara begränsad nära origo. Detta ger att $z = 0$ är en hävbar singularitet för g och att gränsvärdet $\lim_{z\to 0} g(z) = \lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)$ existerar. Enligt maximumprincipen gäller då att

$$|g_0| = \lim_{\mathrm{Im}(\tau)\to\infty} |f(\tau)| < \sup_{\tau\in\mathcal{F}} |f(\tau)| = \sup_{z\in\mathbb{C}} |g(z)| \,. \tag{9.11}$$

Vi vill nu studera hur f beter sig i punkterna $\tau = \pm 1$ på ett liknande sätt som ovan. Egenskap (i) i satsen säger att $f(\tau+2) = f(\tau)$ vilket ger att $f(-1) = f(1)$. Därför räcker det att studera en av punkterna och vi väljer punkten $\tau = 1$. För att få argumentet i f att vara 1 då τ går mot oändligheten så väljer vi att studera $F(\tau) = f(1-1/\tau)$. Vi påstår att följande gränsvärde existerar och uppfyller

$$\lim_{\mathrm{Im}(\tau)\to\infty} |f(1-1/\tau)| < \sup_{\tau\in\mathcal{F}} |f(\tau)| \,. \tag{9.12}$$

Det viktiga nu är att visa att F är periodisk, eftersom vi då har som ovan, enligt det vi visade i (9.11). Betrakta matrisen

$$U_n = \begin{pmatrix} 1-n & n \\ -n & 1+n \end{pmatrix} .$$

Vi kan skriva transformationen som

$$\tau \to \frac{(1-n)\tau + n}{-n\tau + (1+n)} \,,$$

vilken avbildar 1 på 1. Låt nu $\mu(\tau) = 1/(1-\tau)$ och notera att den avbildar 1 på oändligheten och har en invers som avbildar oändligheten på 1. Vi kan då skriva

$$U_n = \mu^{-1} T_n \mu \,,$$

där T_n är avbildningen $T_n(\tau) = \tau + n$. Detta ger att $U_n U_m = U_{n+m}$ och att man kan uttrycka alla U_n genom ett ändligt antal transformationer av T_2, S eller deras inverser. Till exempel har vi att

$$U_{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} = T_2 S \,.$$

Det här ger även att eftersom f är invariant under transformationerna T_2 och S så kommer f inte heller förändras under U_n, det vill säga

$$f(U_n\tau) = f(\mu^{-1} T_n \mu(\tau)) = f(\tau) \,.$$

Vi har att $F(\tau) = f(1-1/\tau) = f(\mu^{-1}(\tau))$, vilket enkelt kan ses genom att invertera μ. Använder vi oss av identiteten ovan får vi att

$$F(\tau) = f(\mu^{-1}(\tau)) = f(\mu^{-1} T_n \mu(\mu^{-1}(\tau))) = f(\mu^{-1} T_n(\tau)) = F(T_n\tau) \,,$$

vilket ger att F är periodisk med perioden 1. Genom att använda tidigare argument kan vi nu se att $h(z) = F(\tau)$ har en hävbar singularitet i $z = e^{2\pi i \tau} = 0$, vilket ger att olikheten i (9.12) gäller.

Från ekvation (9.11) och (9.12) kan vi dra slutsatsen att f inte antar sitt maximala värde på randen till $\mathcal{F}$. Detta innebär att f i så fall har sitt maximum i det inre av det övre halvplanet, vilket motsäger maximumprincipen och f måste vara konstant. □

Vi är nu på slutspurten till beviset av tvåkvadratssatsen och betraktar funktionen

$$f(\tau) = \mathcal{C}(\tau)/\theta(\tau)^2 \,.$$

Vi vet från Följdsats 7.4 att $\theta(\tau)$ saknar nollställen i det övre komplexa halvplanet, vilket ger att f är holomorf i $\mathbb{H}$. Vidare ger Proposition 9.8 att $\mathcal{C}$ och θ^2 inte ändras under transformationerna T_2 och S, vilket ger att $f = \mathcal{C}/\theta^2$ inte heller gör det. Propositionen ger även att funktionen f kommer vara begränsad i $\mathcal{F}$ och enligt Sats 9.9 måste då f vara konstant.

Vi använder oss återigen av Proposition 9.8 och ser att både $\mathcal{C}$ och θ^2 går mot 1 både när $\operatorname{Im}(\tau)$ går mot oändligheten och när τ går mot ± 1. Det här ger att $f = \mathcal{C}/\theta^2$ kommer gå mot 1 och eftersom vi vet att f är konstant måste den vara konstant lika med ett. Vi har nu visat att $\theta(\tau)^2 = \mathcal{C}(\tau)$ och beviset för tvåkvadratssatsen är klart. □

9.5 Fyrkvadratssatsen

Vi har nu kommit till beviset av fyrkvadratssatsen. Minns att satsen säger att varje positivt heltal kan skrivas som en summa av fyra kvadrater och att

$$r_4(n) = 8\sigma_1^*(n) \,, \tag{9.13}$$

där $r_4(n)$ betecknar antalet sätt ett positivt heltal n kan uttryckas som en summa av fyra kvadrater och där $\sigma_1^*(n)$ betecknar summan av delare till n som inte är delbara med 4.

Vi kommer använda oss av samma steglista som i beviset av tvåkvadratssatsen och i sin helhet liknar dessa två bevis varandra.

Bevis av fyrkvadratssatsen. Vi börjar beviset av fyrkvadratssatsen med att göra steg 1 i steglistan av beviset, det vill säga hitta en genererande funktion för sekvensen $r_4(n)$. På samma sätt som i tvåkvadratssatsen vill vi uttrycka den genererande funktionen som en potens av $\theta(\tau)$ och vi får att

$$\theta(\tau)^4 = \sum_{n=0}^{\infty} r_4(n) q^n \,, \tag{9.14}$$

där $q = e^{\pi i \tau}$ med $\tau \in \mathbb{H}$.

Vi är nu klara med första steget i steglistan och går vidare till steg 2 där vi vill hitta en funktion som genom förhållandet till den genererande funktionen θ^4 uttrycker en identitet som är ekvivalent med den i satsen. Vi gör detta genom att konstruera en enklare variant av Eisensteinserien och vi definierar varianten som

$$E_2^*(\tau) = \sum_m \left(\sum_n \frac{1}{(n + \frac{m\tau}{2})^2} \right) - \sum_m \left(\sum_n \frac{1}{(\frac{n}{2} + m\tau)^2} \right) ,$$

där $\tau \in \mathbb{H}$. Eftersom summorna ovan inte är absolutkonvergenta är det viktigt att man summerar i den givna ordningen. Om vi nu använder oss av den förbjudna Eisensteinserien som är definierad som

$$F(\tau) = \sum_m \left(\sum_n \frac{1}{(n + m\tau)^2} \right) ,$$

får vi att
$$E_2^*(\tau) = F\left(\frac{\tau}{2}\right) - 4F(2\tau)\,. \tag{9.15}$$

Följande proposition ger oss relationen mellan θ^4 och E_2^*.

Proposition 9.11. *För τ i det övre komplexa halvplanet är identiteten $r_4(n) = 8\sigma_1^*(n)$ ekvivalent med*
$$\theta(\tau)^4 = -\frac{1}{\pi^2}E_2^*(\tau)\,. \tag{9.16}$$

Bevis. Eftersom vi redan vet att θ^4 relateras till r_4 enligt ekvation (9.14) så räcker det att visa att $8\sigma_1^*$ och $-\frac{1}{\pi^2}E_2^*$ är relaterade till varandra på liknande sätt för att identiteterna ska vara ekvivalenta. Vi utvecklar högerledet genom att använda Följdsats 6.14, som säger att den förbjudna Eisenseinserien kan skrivas som

$$F(\tau) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) e^{2\pi i n\tau}\,, \tag{9.17}$$

där delarfunktionen $\sigma_1(n)$ är summan av alla delare till n. Vi vill nu hitta ett förhållande mellan delarfunktionen och dess variant $\sigma_1^*(n)$, som vi definierat som summan av alla delare till n som inte är delbara med 4. Vi observerar att

$$\sigma_1^*(n) = \begin{cases} \sigma_1(n) & \text{om } n \text{ inte är delbar med } 4 \\ \sigma_1(n) - 4\sigma_1(n/4) & \text{om } n \text{ är delbar med } 4. \end{cases}$$

Vi använder nu detta och får att

$$\begin{aligned} E_2^*(\tau) &= F\left(\frac{\tau}{2}\right) - 4F(2\tau) = \\ &= \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) e^{\pi i n\tau} - \frac{4\pi^2}{3} + 8\pi^2 \sum_{n=1}^{\infty} 4\sigma_1(n) e^{4\pi i n\tau} = \\ &= -\pi^2 - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1^*(n) e^{\pi i n\tau}\,, \end{aligned}$$

där sista steget fås genom att dela upp summorna på ett sådant sätt att vi kan använda oss av relationen mellan delarfunktionerna σ_1 och σ_1^*. Vi har nu att

$$-\frac{1}{\pi^2}E_2^*(\tau) = -\frac{1}{\pi^2}\left(-\pi^2 - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1^*(n) e^{\pi i n\tau}\right) = 1 + \sum_{n=1}^{\infty} 8\sigma_1^*(n) q^n\,, \tag{9.18}$$

vilket innebär att E_2^* kan relateras till $8\sigma_1^*$ på samma sätt som θ^4 kan relateras till r_4. Från detta ser vi ävan att E_2^* är en genererande funktion till sekvensen $\sigma_1^*(n)$. $\square$

Vi har nu visat att identiteten (9.13) är ekvivalent med (9.16) och är därav färdiga med andra steget i vår steglista. Vi går vidare till steg 3, där det gäller att visa att vår nya identitet, (9.16), håller. Enligt steglistan kan detta delas upp i två delar där första delen är att visa att vänster- och högerled i (9.16) har samma strukturella egenskaper. Vi formulerar dessa egenskaper i en proposition.

Proposition 9.12. *Funktionen E_2^* som är definierad i det övre komplexa halvplanet uppfyller egenskaperna* *(i)* $E_2^*(\tau+2) = E_2^*(\tau)$

(ii) $E_2^*(-1/\tau) = -\tau^2 E_2^*(\tau)$

(iii) $E_2^*(\tau) \to -\pi^2$ *då* $Im(\tau) \to \infty$

(iv) $|E_2^*(1-1/\tau)| = O(|\tau^2 e^{\pi i \tau}|)$ *då* $Im(\tau) \to \infty$.

Dessutom uppfyller $-\pi^2\theta^4$ *samma egenskaper.*

Bevis av proposition 9.12. Från Proposition 9.3 får vi att alla egenskaper i propositionen gäller för $\theta(\tau)^4$.

Vi vill nu visa att alla egenskaper även gäller för E_2^*. Vi ser att (i) följer direkt från definitionen av E_2^*, vilket tydligt ses i vår utveckling av E_2^* i ekvation (9.18). De andra egenskaperna är lite krångligare att visa och för detta behöver vi följande lemma.

Lemma 9.13. *Funktionerna F och $\tilde{F}$ uppfyller*

(a) $F(-1/\tau) = \tau^2 \tilde{F}(\tau)$

(b) $F(\tau) - \tilde{F}(\tau) = 2\pi i/\tau$

(c) $F(-1/\tau) = \tau^2 F(\tau) - 2\pi i \tau$,

där

$$F(\tau) = \sum_m \left(\sum_n \frac{1}{(n+m\tau)^2} \right) \quad \text{och} \quad \tilde{F}(\tau) = \sum_n \left(\sum_m \frac{1}{(n+m\tau)^2} \right) ,$$

Bevis av lemma 9.13. Egenskap (a) följer direkt från definitionen av F och $\tilde{F}$ genom att använda att

$$(m(-1/\tau)+n)^2 = \tau^{-2}(-m+n\tau)^2 .$$

För att visa (b) utgår vi ifrån funktionalekvationen för Dedekinds etafunktion som vi introducerade i Proposition 9.6 enligt

$$\eta(-1/\tau) = \sqrt{\tau/i}\, \eta(\tau) , \tag{9.19}$$

där $\eta(\tau) = q^{1/12}\prod_{n=1}^{\infty}(1-q^{2n})$ och $q = e^{\pi i \tau}$.

Vi vill nu skriva om ekvation (9.19) genom att ta den logaritmiska derivatan av hela uttrycket. Vi börjar med att ta den logaritmiska derivatan av $\eta(\tau)$ och får att

$$\begin{aligned}(\eta'/\eta)(\tau) &= \frac{1}{q^{1/12}}(q^{1/12})' + \sum_{n=1}^{\infty} \frac{1}{1-q^{2n}}(1-q^{2n})' = \\ &= \frac{\pi i}{12} - 2\pi i \sum_{n=1}^{\infty} \frac{nq^{2n}}{1-q^{2n}} .\end{aligned}$$

Vi skriver nu om summan i högerledet ytterligare genom att först använda formeln för geometrisk summa och därefter komma ihåg att $\sigma_1(k)$ betecknar summan av alla delare till k. Detta ger att vi kan skriva summan som

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{nq^{2n}}{1-q^{2n}} &= \sum_{n=1}^{\infty}\sum_{l=0}^{\infty} nq^{2n}q^{2ln} = \\ &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} nq^{2nm} = \\ &= \sum_{k=1}^{\infty}\sigma_1(k)q^{2k}\,.\end{aligned}$$

Använd nu att den förbjudna Eisensteinserien kan skrivas som i (9.17), vilket ger oss förhållandet

$$(\eta'/\eta)(\tau) = \frac{\pi i}{12} - 2\pi i\sum_{k=1}^{\infty}\sigma_1(k)q^{2k} = \frac{i}{4\pi}F(\tau)\,.$$

Om vi istället tar den logaritmiska derivatan av $\eta(-1/\tau)$, som vi har i vänsterledet i (9.19), får vi med hjälp av kedjeregeln att den är $\tau^{-2}(\eta'/\eta)(-1/\tau)$. Vidare om vi använder egenskap (a) får vi att den logaritmiska derivatan av $\eta(-1/\tau)$ är

$$(\log(\eta(-1/\tau)))' = \tau^{-2}(\eta'/\eta)(-1/\tau) = \tau^{-2}\frac{i}{4\pi}F(-1/\tau) = \frac{i}{4\pi}\tilde{F}(\tau)\,.$$

Tar vi den logaritmiska derivatan av funktionalekvationen för η, se (9.19), får vi att

$$\frac{i}{4\pi}\tilde{F}(\tau) = \frac{1}{2\tau} + \frac{i}{4\pi}F(\tau)\,.$$

Det här ger att

$$\tilde{F}(\tau) = -\frac{2\pi i}{\tau} + F(\tau)\,,$$

och vi har att (b) gäller.

Därefter följer (c) direkt från de tidigare egenskaperna och lemmat är bevisat. □

Vi återgår nu till beviset av Proposition 9.12 där vi vill visa (ii) med hjälp av lemmat ovan. Vi börjar med att

$$E_2^*(\tau) = F(\tau/2) - 4F(2\tau)\,.$$

Det ger oss att

$$\begin{aligned}E_2^*(-1/\tau) &= F(-1/(2\tau)) - 4F(-2/\tau) = \\ &= \left(4\tau^2F(2\tau) - 4\pi i\tau\right) - 4\left((\tau/2)^2F(\tau/2) - \pi i\tau\right)\,,\end{aligned}$$

vilket följer från (c) i Lemma 9.13. Vi utvecklar vidare och genom att återigen använda oss av egenskap (c) i Lemma 9.13 får vi att

$$\begin{aligned}E_2^*(-1/\tau) &= 4\tau^2F(2\tau) - 4(\tau^2/4)F(\tau/2) = \\ &= -\tau^2(F(\tau/2) - 4F(2\tau)) = \\ &= -\tau^2E_2^*(\tau)\,,\end{aligned}$$

vilket är precis det vi vill ha.

För att visa (iii) minns vi från (9.17) att $F(\tau) = \frac{\pi^2}{3} - 8\pi^2 \sum_{k=1}^{\infty} \sigma_1(k) e^{2\pi i k\tau}$, där summan går mot 0 då $\mathrm{Im}(\tau)$ går mot oändligheten. Om vi då använder oss av att

$$E_2^*(\tau) = F(\tau/2) - 4F(2\tau) = -\pi^2 - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1^*(n) e^{\pi i n\tau},$$

får vi att E_2^* går mot $-\pi^2$ då $\mathrm{Im}(\tau)$ går mot oändligheten.

I beviset av propositionen återstår nu endast att visa (iv) och vi kommer börja med att visa att

$$E_2^*(1-1/\tau) = \tau^2 \left(F\left(\frac{\tau-1}{2}\right) - F(\tau/2) \right). \tag{9.20}$$

Genom att använda (9.15) får vi att

$$E_2^*(1-1/\tau) = F(\frac{1}{2} - \frac{1}{2\tau}) - 4F(2-2/\tau).$$

Från egenskap (c) i Lemma 9.13 får vi att

$$\begin{aligned} F\left(\frac{1}{2} - \frac{1}{2\tau}\right) &= F\left(\frac{\tau-1}{2\tau}\right) = \\ &= \left(\frac{2\tau}{\tau-1}\right)^2 F\left(\frac{2\tau}{1-\tau}\right) - 2\pi i \frac{2\tau}{1-\tau}, \end{aligned}$$

och på liknande sätt får vi att

$$\begin{aligned} F\left(\frac{2\tau}{1-\tau}\right) &= F\left(-2 + \frac{2}{1-\tau}\right) = \\ &= F\left(\frac{2}{1-\tau}\right) = \\ &= \left(\frac{1-\tau}{2}\right)^2 F\left(\frac{\tau-1}{2}\right) - 2\pi i \left(\frac{\tau-1}{2}\right). \end{aligned}$$

Lägger vi in detta i uttrycket för $F\left(\frac{1}{2} - \frac{1}{2\tau}\right)$ får vi att

$$F\left(\frac{1}{2} - \frac{1}{2\tau}\right) = \tau^2 F\left(\frac{\tau-1}{2}\right) - \frac{2\pi i 2\tau}{1-\tau} - 2\pi i \frac{(2\tau)^2}{(\tau-1)^2} \left(\frac{\tau-1}{2}\right).$$

Vi har även att

$$F(2-2/\tau) = F(-2/\tau) = \frac{\tau^2}{4} F(\tau/2) - \frac{2\pi i\tau}{2},$$

vilket ger att

$$\begin{aligned} E_2^*(1-1/\tau) &= F(1/2 - 1/2\tau) - 4F(2-2/\tau) = \\ &= \tau^2 \left(F\left(\frac{\tau-1}{2}\right) - F(\tau/2) \right) - 2\pi i \left(\frac{2\tau}{1-\tau} + \frac{2\tau^2}{\tau-1} \right) + 4\pi i\tau = \\ &= \tau^2 \left(F\left(\frac{\tau-1}{2}\right) - F(\tau/2) \right), \end{aligned}$$

vilket visar (9.20). Genom att använda oss av detta och att den förbjudna Eisensteinserien kan skrivas enligt (9.17) får vi att

$$E_2^*(1-1/\tau) = 8\pi^2\tau^2 e^{\pi i\tau}\sum_{n=1}^{\infty}\sigma_1(n)e^{\pi i(n-1)\tau}(1-e^{-\pi i n}),$$

vilket kommer vara av storleksordning $O(|\tau^2 e^{\pi i\tau}|)$ då $\mathrm{Im}(\tau)$ går mot oändligheten. $\square$

Vi har nu visat att $-\pi^2\theta^4$ och E_2^* uppfyller samma strukturella egenskaper, och är därmed klara med steg 3a i vår steglista. Det är nu dags att knyta ihop säcken av beviset till fyrkvadratssatsen genom att ge oss på det sista steget i steglistan. Vi börjar med att betrakta kvoten

$$f(\tau) = \frac{E_2^*(\tau)}{\theta(\tau)^4},$$

och använder oss av Sats 9.9 på samma sätt som vi gjorde i tvåkvadratssatsen. Vi har från de strukturella egenskaperna hos θ^4 och E_2^* att f inte ändras under transformationerna T_2 och S och att f även måste vara begränsad. Detta ger att f måste vara konstant.

Vi använder oss av Proposition 9.12 och ser att E_2^* går mot $-\pi^2$ och att θ^4 går mot 1 när $\mathrm{Im}(\tau)$ går mot oändligheten. Det här ger att $f = E_2^*/\theta^4$ kommer gå mot $-\pi^2$ och eftersom vi vet att f är konstant måste den vara konstant lika med $-\pi^2$. Vi har nu visat att $-\pi^2\theta^4(\tau) = E_2^*(\tau)$ och beviset för fyrkvadratssatsen är klart. $\square$

Kapitel 10

Dirichlets sats

10.1 Introduktion

I denna del av rapporten kommer vi att studera en specifik sats som är känd inom talteori, Dirichlets sats om primtal i aritmetiska talföljder. Satsen säger att om q och ℓ är två positiva heltal som saknar gemensamma delare så kommer följden

$$\ell, \ell + q, \ell + 2q, \ell + 3q, \ldots, \ell + kq, \ldots ,$$

att innehålla oändligt många primtal. Denna sats kan ses som en generalisering av Euklides sats som säger att antalet primtal är oändligt. Målet med detta avsnitt är således att konstruera ett bevis för Dirichlets sats, dock börjar vi med att studera en hel del teori som kommer vara av stor nytta innan vi tacklar själva beviset.

Peter Gustav Lejeune Dirichlet (1805-1859) var en stor matematiker som bidrog oerhört mycket till många olika grenar inom matematiken, men främst verksam var han inom talteorin och Fourieranalysen. Han är även känd för att vara en av de första matematikerna i modern tid till att ge en formell definition av begreppet funktion. Med hjälp av matematisk analys publicerade Dirichlet satsen om artimetiska talföljder 1837 och gav samtidigt upphov till en ny gren inom matematiken: analytisk talteori. För att bevisa satsen införde han de så kallade Dirichlet-karaktärerna och L-funktionerna, vilka vi kommer att studera närmare.

10.2 Dirichlets sats

Dirichlet bevisade satsen om aritmetiska talföljder genom att bevisa följande starkare sats.

Sats 10.1. *Om ℓ och q delar saknar gemensamma delare så divergerar*

$$\sum_{p \equiv \ell \bmod q} \frac{1}{p},$$

där $p \equiv \ell \bmod q$ är alla primtal p kongruenta mot ℓ modulo q.

Vi inleder med att introducera en proposition som kommer hjälpa oss lite senare.

Proposition 10.2. *Serien*

$$\sum_p \frac{1}{p},$$

divergerar, där summan är över alla primtal.

Bevis. Vi försöker uppskatta serien nedåt med en serie som är mindre, och sådan att serien divergerar. Då följer propositionen. Vi kan uppskatta det n:te primtalet p_n med primtalssatsen, det vill säga vi vet att

$$\pi(x) \geq \frac{x}{2\log x} \Rightarrow n \leq \frac{1}{2}\frac{p_n}{\log p_n} \Rightarrow p_n \leq 4n\log n\,.$$

Vi applicerar denna olikhet och får därför

$$\sum_{n=1}^{\infty} \frac{1}{p_n} \geq \sum_{n=1}^{\infty} \frac{1}{4n\log n}\,. \tag{10.1}$$

Vi har att

$$\frac{1}{4}\int_1^{\infty} \frac{1}{x\log x}\,\mathrm{d}x = \frac{1}{2}\left[\frac{1}{\log\log x}\right]_1^{\infty},$$

divergerar, och enligt integralkriteriet divergerar därför summan i högerledet i ekvation (10.1). Därmed följer också att $\sum_p \frac{1}{p}$ divergerar. □

Exempel

Innan vi bevisar satsen generellt så börjar vi med att illustrera ett exempel: finns det oändligt många primtal av formen $4k+1$? Detta är specialfallet då $q = 4$ och $\ell = 1$. Vi betraktar karaktären på gruppen $\mathbb{Z}^*(4) = \{1, 3\}$ som definieras av $\chi(1) = 1$ och $\chi(3) = -1$. Denna karaktär kan utvidgas till hela $\mathbb{Z}$:

$$\chi(n) = \begin{cases} 0 & \text{om } n \text{ är jämn} \\ 1 & \text{om } n = 4k+1 \\ -1 & \text{om } n = 4k+3 \end{cases}.$$

Observera att denna karaktär är multiplikativ, det vill säga $\chi(nm) = \chi(n)\chi(m)$ på hela $\mathbb{Z}$. Vi definierar vidare funktionen $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$, alltså

$$L(s,\chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \ldots\,.$$

Summan som utgörs av $L(1,\chi)$ blir då

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1},$$

och kommer således att konvergera enligt Leibniz konvergenskriterium. Dessutom så gäller det att $L(1,\chi) \neq 0$ då vi har en avtagande och alternerande serie. I och med att $\chi(n)$ är multiplikativ kan vi uttrycka

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}}\,.$$

Detta samband kommer vi att bevisa senare, se Sats 10.5. Vidare, om vi logaritmerar båda sidor i uttrycket ovan får vi att

$$\log L(s, \chi) = \sum_p \frac{\chi(p)}{p^s} + O(1)\,.$$

Vi låter nu s gå mot 1^+, vilket ger oss att $\sum_p \chi(p)/p^s$ är begränsad i och med att $L(1,\chi) \neq 0$. Men vi kan skriva

$$\sum_p \frac{\chi(p)}{p^s} = \sum_{p\equiv 1} \frac{1}{p^s} - \sum_{p\equiv 3} \frac{1}{p^s}$$

som är begränsad då $s \to 1^+$. Proposition 10.2 ger oss att $\sum p^{-s}$ är obegränsad då s går mot 1^+, vilket ger att någon av summorna $\sum_{p\equiv 1} p^{-s}$ eller $\sum_{p\equiv 3} p^{-s}$ är obegränsad. Men då $\sum \chi(p)p^{-s}$ är begränsad måste alltså båda summorna vara begränsade då s går mot 1^+. Det här ger att summan $\sum_{p\equiv 1} 1/p$ divergerar, vilket medför att det finns oändligt många primtal på formen $4k+1$.

Det generella beviset av Dirichlets sats kommer gå till på samma sätt som exemplet ovan. Vi kommer att utvidga karaktärerna definierade på $\mathbb{Z}^*(q)$ till hela $\mathbb{Z}$. Med Fourieranalys kommer Dirichlets sats att reduceras ner till ett påstående om $L-$funktioner.

10.3 Dirichlet-karaktärer

Målet med detta avsnitt är att på den abelska gruppen $\mathbb{Z}^*(q)$ utveckla ett nytt begrepp: Dirichlet-karaktärer. Med hjälp av dessa karaktärer kommer beviset av Dirichlets sats att reduceras till påståendet om huruvida L-funktioner har nollställen vid $s = 1$.

Vi betraktar den abelska gruppen $\mathbb{Z}^*(q)$, vilken vi framöver kommer beteckna med G. Ordningen av G ges av Eulers phi-funktion, vilken definieras som

Definition 10.1. *Eulers phi-funktion betecknas $\varphi(q)$ och är lika med antalet heltal mellan 0 och q som är relativt prima q. Vidare gäller det att $|G| = \varphi(q)$.*

Vi definierar funktionen δ_ℓ på G:

$$\delta_\ell(n) = \begin{cases} 1 \text{ om } n = \ell \bmod \text{q}\,, \\ 0 \text{ annars}\,. \end{cases}$$

Betrakta nu funktionens Fourierserieutveckling

$$\delta_\ell(n) = \sum_{e\in\hat{G}} \hat{\delta}_\ell(e)e(n)\,,$$

där

$$\hat{\delta}_\ell(e) = \frac{1}{|G|}\sum_{m\in G} \delta_\ell(m)\overline{e(m)} = \frac{1}{|G|}\overline{e(\ell)}\,.$$

Detta ger oss att

$$\delta_\ell(n) = \frac{1}{|G|}\sum_{e\in\hat{G}} \overline{e(\ell)}e(n)\,. \tag{10.2}$$

Vi kan utvidga δ_ℓ till hela $\mathbb{Z}$ genom att låta $\delta_\ell(n) = 0$ då n och m ej är relativt prima, alltså då de har gemensamma delare. På samma sätt utvidgar vi karaktärerna $e \in \hat{G}$ till hela $\mathbb{Z}$ genom

$$\chi(m) = \begin{cases} e(m \bmod q) & \text{om } m \text{ och } q \text{ är relativt prima} \\ 0 & \text{annars} \end{cases}\,.$$

Dessa är Dirichlet-karaktärerna modulo q. Vi kommer att beteckna den triviala Dirichlet-karaktären som χ_0, det vill säga den karaktär där det gäller att $\chi_0(m) = 1$ om q och m är relativt prima och annars 0.

Lemma 10.3. *Dirichlet-karaktärerna är multiplikativa på hela $\mathbb{Z}$, det vill säga $\chi(nm) = \chi(n)\chi(m)$ för alla $n, m \in \mathbb{Z}$. Dessutom gäller att*

$$\delta_\ell(m) = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(\ell)} \chi(m)\,,$$

där summeringen går över alla Dirichlet-karaktärer.

Bevis. Lemmat följer från (10.2) i och med att $\delta_\ell(m)$ och $\chi(m)$ är q-periodiska. □

En konsekvens av detta lemma är att

$$\sum_{p \equiv \ell} \frac{1}{p^s} = \sum_{p} \frac{\delta_\ell(p)}{p^s} = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(\ell)} \sum_{p} \frac{\chi(p)}{p^s}\,.$$

Vi kan i och med denna likhet reducera beviset av Sats 10.1 till en sats om hur $\sum_p \chi(p)p^{-s}$ beter sig. Vi kan till och med dela upp summan i två delar beroende på om χ är trivial eller inte, det vill säga

$$\begin{aligned}\sum_{p \equiv \ell} \frac{1}{p^s} &= \frac{1}{\varphi(q)} \sum_{p} \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(\ell)} \sum_{p} \frac{\chi(p)}{p^s} = \\ &= \frac{1}{\varphi(q)} \sum_{p \nmid q} \frac{1}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(\ell)} \sum_{p} \frac{\chi(p)}{p^s}\,.\end{aligned} \tag{10.3}$$

Vi har från Proposition 10.2 att den första summan i högerledet divergerar då s går mot 1^+. Dessa observationer visar på att Dirichlets sats följer av Sats 10.4.

Sats 10.4. *Om χ är en icke-trivial Dirichlet-karaktär förblir summan*

$$\sum_{p} \frac{\chi(p)}{p^s}$$

begränsad då $s \to 1^+$.

Har vi alltså bevisat Sats 10.4 har vi lyckats bevisa hela Dirichlets sats. Men innan vi kan bevisa denna sats behöver vi emellertid introducera Dirichlets L-funktioner, och med hjälp av dessa reducera beviset av Sats 10.4 till ett påstående om hur dessa funktioner beter sig.

10.4 Dirichlets L-funktioner

L-funktioner infördes redan 1837 av Dirichlet i samband med beviset för Dirichlets sats. L-funktionerna delar vissa likheter med Riemanns ζ-funktion: funktionerna har inga nollställen då $\mathrm{Re}(s) \geq 1$.

Vi påminner om ζ-funktionen som definieras enligt

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{då } \mathrm{Re}(s) > 1\,.$$

Definition 10.2. *Låt χ vara en Dirichlet-karaktär. Vi definierar då Dirichlets L-funktioner som*

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \text{ för } \operatorname{Re}(s) > 1\,.$$

Man kan alltså betrakta L-funktionerna som generaliseringar av $\zeta(s)$. Dessa kan utvidgas till meromorfa funktioner över hela $\mathbb{C}$ med en analytisk fortsättning, analogt med $\zeta(s)$. Att $\zeta(s)$ har en meromorf fortsättning visades tidigare i Sats 4.13.

Sats 10.5 (Dirichlets produktformel)**.** *För alla komplexa tal s med* $\operatorname{Re}(s) > 1$ *gäller att*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{(1-\chi(p)p^{-s})}\,,$$

där produkten över alla primtal.

Vi väntar med beviset till denna sats och antar att den gäller. Vi är inte ännu redo att bevisa Sats 10.4, men vi kan börja motivera hur beviset skall gå till. Om vi kan ge innebörd till att logaritmera produkten i Sats 10.5 skulle vi på så sätt få

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log(1-\chi(p)p^{-s}) = \\ &= -\sum_p \left[-\frac{\chi(p)}{p^s} + O\left(\frac{1}{p^{2s}}\right)\right] = \\ &= \sum_p \frac{\chi(p)}{p^s} + O(1)\,.\end{aligned}$$

Här använde vi oss av att $\log(1+x) = x + O(x^2)$ för små x. Om $L(1,\chi)$ är ändlig och nollskild så kommer $\log L(1,\chi)$ att vara begränsad då s går mot 1^+, vilket ger oss att summan

$$\sum_p \frac{\chi(p)}{p^s}\,,$$

är begränsad då s går mot 1^+. Det återstår nu att bevisa att L-funktionerna beter sig på ett sådant sätt som vi hävdade i beviset ovan för att Dirichlets sats ska följa av Sats 10.4.

10.5 Bevis av Dirichlets sats

För att få ett rigoröst bevis av satsen finns det tre saker vi måste göra. För det första måste vi visa att Sats 10.5 om Dirichlets produktformel håller.

För det andra behöver vi reda ut vad det innebär att logaritmera både vänster- och högerled i produktformeln. Svårigheten här ligger i att χ kan vara komplexvärd, i och med att den komplexa logaritmen är en flervärd funktion. Således är inte logaritmen nödvändigtvis en produkt en summa av logaritmerna.

För det tredje och sista behöver vi visa att då χ är en icke-trivial Dirichlet-karaktär så gäller att $\log L(s,\chi)$ är begränsad då s går mot 1^+. Om $L(s,\chi)$ är holomorf räcker det således att visa att $L(s,\chi) \neq 0$, men det är just här svårigheten av beviset ligger.

Vi kommer därmed att fokusera på tre punkter när vi bevisar satsen:

1. Komplexa logaritmer och oändliga produkter.
2. Studera egenskaperna hos $L(s,\chi)$.
3. Visa att $L(1,\chi) \neq 0$ om χ är icke-trivial.

Vi börjar med att bevisa Dirichlets produktformel.

Bevis av Sats 10.5. Vi bildar den partiella summan och produkten enligt

$$S_N = \sum_{n \le N} \frac{\chi(n)}{n^s} \quad \text{och} \quad \prod_N = \prod_{p \le N} \left(\frac{1}{1-\chi(p)p^{-s}} \right).$$

Den oändliga produkten

$$\prod = \lim_{N\to\infty} \prod_N = \prod_p \left(\frac{1}{1-\chi(p)p^{-s}} \right),$$

konvergerar för $\mathrm{Re}(s) > 1$, enligt Sats 3.1 då

$$\sum_p |\chi(p)p^{-s}| < \infty.$$

Vi vet att $\prod(1-a_n)^{-1}$ konvergerar om $\sum |a_n| < \infty$, vilken ger att $\prod_N$ konvergerar. Låt nu

$$\prod_{N,M} = \prod_{p \le N} \left(1 + \frac{\chi(p)}{p^s} + \dots + \frac{\chi(p^M)}{p^{Ms}} \right).$$

Fixera $\varepsilon > 0$ och välj N tillräckligt stort så att

$$\left| S_N - \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \right| < \varepsilon \quad \text{och} \quad \left| \prod_N - \prod \right| < \varepsilon.$$

Vi påstår att vi kan välja M stort nog så att

$$\left| S_N - \prod_{N,M} \right| < \varepsilon \quad \text{och} \quad \left| \prod_{N,M} - \prod_N \right| < \varepsilon. \tag{10.4}$$

Vi påminner här om att varje heltal större än 1 är antingen ett primtal eller en produkt av primtal. Använder vi detta faktum, samt att Dirichlet-karaktärerna är multiplikativa, ger att vi kan välja M så att första olikheten i (10.4) gäller. För att se att den andra olikheten gäller utnyttjar vi att $\sum_{n=1}^{\infty} \chi(p^n)/p^{ns}$ konvergerar. Då

$$\prod_{N,\,M}^{\infty} \underset{M\to\infty}{\longrightarrow} \prod_N,$$

kan vi välja M så att den andra gäller. Triangelolikheten ger nu att

$$\left| \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} - \prod \right| \le \left| \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} - S_N \right| + \left| S_N - \prod_{N,M} \right| + \left| \prod_{N,M} - \prod_N \right| + \left| \prod_N - \prod \right| < 4\varepsilon,$$

och därmed är beviset klart. $\square$

10.6 L-funktioner

Nu när vi definierat de två logaritmerna går vi vidare och studerar L-funktionerna. Funktionernas egenskaper som funktioner av s beror på om χ är trivial eller inte. Som vi kommer att se är fallet då s är nära 1 speciellt intressant. Vi börjar med fallet beträffande den triviala Dirichlet-karaktären, då $\chi = \chi_0$.

Proposition 10.6. *Antag att χ_0 är den triviala Dirichlet-karaktären och att $q = p_1^{a_1} \dots p_N^{a_N}$ är primtalsfaktoriseringen av q. Då gäller att*

$$L(s, \chi_0) = (1 - p_1^{-s})(1 - p_2^{-s}) \dots (1 - p_N^{-s})\zeta(s)\,,$$

där $p_1, \dots, p_k$ är alla (ändligt många) primtal relativt prima q. Alltså har $L(s, \chi_0)$ en enkelpol i $s = 1$.

Bevis. Propositionen följer direkt genom att jämföra Dirichlets och Eulers produktformler. Vi börjar med Dirichlets produktformel och får att

$$L(s, \chi_0) = \prod_p \frac{1}{1 - \chi_0(p)p^{-s}} = \prod_{p|q} \frac{1}{1 - p^{-s}} =$$

$$= (1 - p_1^{-s})(1 - p_2^{-s})...(1 - p_N^{-s}) \prod_p \frac{1}{1 - p^{-s}} = (1 - p_1^{-s})(1 - p_2^{-s})...(1 - p_N^{-s})\zeta(s)\,.$$

Det sista påståendet gäller eftersom $\zeta(s)$ har en enkelpol i $s = 1$. □

En viktig observation är att vi alltså kan betrakta $\zeta(s)$ som en L-funktion med Dirichlet-karaktären χ_0 modulo 1. De resterande L-funktionerna, det vill säga då $\chi \neq \chi_0$, är aningen snällare. En anmärkningsvärd egenskap hos dessa funktioner är att de nu är holomorfa då $\mathrm{Re}(s) > 0$. Vi vet dessutom ännu mer om funktionerna, vilket sammanfattas i en proposition.

Proposition 10.7. *Om χ är en icke-trivial Dirichlet-karaktär så konvergerar följande serie för* $\mathrm{Re}(s) > 0$*,*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}\,,$$

och vi betecknar dess summa med $L(s, \chi)$. Vidare gäller också att

(i) Funktionen $L(s, \chi)$ är holomorf på $\mathrm{Re}(s) > 0$

(ii) Det existerar konstanter $a, b > 0$ sådana att

$$\begin{aligned} L(s,\chi) &= 1 + O(e^{-a\,\mathrm{Re}(s)}) \qquad \text{då } \mathrm{Re}(s) \to \infty\,, \\ L'(s,\chi) &= O(e^{-b\,\mathrm{Re}(s)}) \qquad \text{då } \mathrm{Re}(s) \to \infty\,. \end{aligned}$$

Innan vi bevisar denna proposition behöver vi ett lemma som demonstrerar en mycket viktig egenskap hos de icke-triviala Dirichlet-karaktärerna, som står för beteendet av $L(s, \chi)$ som introducerades i propositionen ovan.

Lemma 10.8. *Om χ är en icke-trivial Dirichlet-karaktär så gäller att*

$$\left| \sum_{n=1}^{k} \chi(n) \right| \leq q\,, \qquad \text{för alla } k\,.$$

Bevis. Vi påminner om att
$$\sum_{n=1}^{q} \chi(n) = 0\,.$$
från 5.3. Låt nu $k = aq + b$ så att $0 \leq b < q$. Vi noterar att
$$\sum_{n=1}^{k} \chi(n) = \sum_{n=1}^{aq} \chi(n) + \sum_{aq<n\leq aq+b} \chi(n) = \sum_{aq<n\leq aq+b} \chi(n)\,.$$
I summan till höger har vi inte fler än q termer. Vidare eftersom $|\chi(n)| \leq 1$, följer lemmat. $\square$

Bevis av Proposition 10.7. För att bevisa att L-funktionen är holomorf för $\mathrm{Re}(s) > 1$ och $\chi \neq \chi_0$ använder vi oss av partiell summmering. Låt $\{a_n\}$ och $\{b_n\}$ vara sekvenser av komplexa tal sådana att partialsummorna $A_N = \sum_{n=1}^{N} a_n$ är begränsade och att b_N går mot 0. Med $A_0 = 0$ har vi således att
$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=1}^{\infty} (A_n - A_{n-1}) b_n = \sum_{n=0}^{\infty} A_n b_n - \sum_{n=0}^{\infty} A_n b_{n+1} = \sum_{n=0}^{\infty} A_n (b_n - b_{n+1})\,.$$
Vi låter nu $a_n = \chi(n)$ och $b_n = n^{-s}$. Detta ger oss att
$$L(s,\chi) = \sum_{n=0}^{\infty} \left(\sum_{\ell=1}^{N} \chi(\ell) \right) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) = \sum_{n=0}^{\infty} O\left(\frac{1}{n^{s+1}} \right)\,,$$
vilket ger oss att $L(s,\chi)$ är holomorf för $\mathrm{Re}(s) > 0$.

Det återstår nu endast att visa (*ii*). Vi noterar att om vi väljer $\mathrm{Re}(s)$ tillräckligt stort får vi att
$$|L(s,\chi) - 1| \leq \sum_{n=2}^{\infty} \left| \frac{\chi(n)}{n^s} \right| \leq \sum_{n=2}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} = 2^{-\mathrm{Re}(s)} + \sum_{n=3}^{\infty} \frac{1}{\left(\frac{n}{2}\right)^{\mathrm{Re}(s)}} = 2^{-\mathrm{Re}(s)} O(1)\,.$$
Välj nu $a = \log 2$ i Proposition 10.7 och se att $L(s,\chi) = 1 + O(e^{-c\,\mathrm{Re}(s)})$ då $\mathrm{Re}(s)$ går mot oändligheten. Helt analogt följer att $L'(s,\chi) = O(e^{-b\,\mathrm{Re}(s)})$ då $\mathrm{Re}(s)$ går mot oändligheten. $\square$

Vi har nu gått igenom tillräckligt mycket teori för att definiera två logaritmer.

Definition 10.3. *För $z < 1$ gäller det att*
$$\log_1 \left(\frac{1}{1-z} \right) = \sum_{k} \frac{z^k}{k}\,.$$

Definition 10.4. *Om $\chi \neq \chi_0$ och $\mathrm{Re}(s) > 1$ definierar vi*
$$\log_2 L(s,\chi) = -\int_{s}^{\infty} \frac{L'(t,\chi)}{L(t,\chi)}\,\mathrm{d}t\,.$$
Vi vet att $L(t,\chi) \neq 0$ för alla $\mathrm{Re}(t) > 1$ eftersom den ges av en produkt (Proposition 3.1). Vidare så är integralen konvergent eftersom
$$\frac{L'(t,\chi)}{L(t,\chi)} = O(e^{-ct})\,,$$
vilket följer från Proposition 10.7. Vi kan nu visa ett samband mellan de två logaritmerna i en proposition:

Proposition 10.9. *För* $\mathrm{Re}(s) > 1$ *gäller det att*

$$e^{\log_2 L(s,\chi)} = L(s,\chi)\,.$$

Dessutom gäller att

$$\log_2 L(s,\chi) = \sum_p \log_1\left(\frac{1}{1-\chi(p)/p^s}\right).$$

Bevis. Vi börjar med att derivera $e^{-\log_2 L(s,\chi)}L(s,\chi)$ med avseende på s. Detta ger oss att

$$\begin{aligned}
&-\frac{L'(s,\chi)}{L(s,\chi)}e^{-\log_2 L(s,\chi)}L(s,\chi) + e^{-\log_2 L(s,\chi)}L'(s,\chi) = \\
&= e^{-\log_2 L(s,\chi)}(L'(s,\chi) - L'(s,\chi)) \equiv 0\,.
\end{aligned}$$

I och med att derivatan är identiskt lika med noll har vi att $e^{-\log_2 L(s,\chi)}L(s,\chi) \equiv c$, där c är en konstant. Vidare ser vi att $c = 1$ om vi låter $\mathrm{Re}(s)$ gå mot oändligheten. Vi har således bevisat första påståendet.

För att bevisa det andra påståendet fixerar vi s och exponentierar båda led. Vänsterledet blir således $e^{\log_2 L(s,\chi)} = L(s,\chi)$ och högerledet blir

$$e^{\sum_p \log_1\left(\frac{1}{1-\chi(p)/p^s}\right)} = \prod_p e^{\log_1\left(\frac{1}{1-\chi(p)/p^s}\right)} = \prod_p \left(\frac{1}{1-\chi(p)/p^s}\right) = L(s,\chi)\,,$$

vilket fås genom att använda Sats 10.5 om Dirichlets produktformel. Därav existerar det för varje s ett heltal $M(s)$ sådant att

$$\log_2 L(s,\chi) - \sum_p \log_1\left(\frac{1}{1-\chi(p)/p^s}\right) = 2\pi i M(s)\,.$$

Då vänsterledet är holomorft för $\mathrm{Re}(s) > 1$ medför detta att funktionen $M(s)$ också är holomorf. Däremot är $M(s)$ en heltalsvärd funktion och måste alltså vara konstant. Genom att låta $\mathrm{Re}(s)$ gå mot oändligheten ser vi att denna konstant måste vara 0, och därmed är beviset klart. □

Sammanfattningsvis har vi att då $\log_1 \frac{1}{1-z} = z + O(|z^2|)$ är

$$\begin{aligned}
&\sum_p \log_1\left(\frac{1}{1-\chi(p)/p^s}\right) = \sum_p \frac{\chi(p)}{p^s} + O\left(\sum_p \frac{1}{p^{2\,\mathrm{Re}(s)}}\right) = \\
&= \sum_p \frac{\chi(p)}{p^s} + O(1)\,.
\end{aligned}$$

Om nu $L(1,\chi) \neq 0$ för en icke-trivial Dirichlet-karaktär gäller att $\log_2 L(s,\chi)$ från sin integralrepresentation kommer fortsätta vara begränsad då s går mot 1. Därmed medför identiteten mellan logaritmerna att $\sum_p \chi(p)p^{-s}$ fortsätter vara begränsad då s går mot 1, vilket är vad vi önskade. Det återstår således att visa att $L(1,\chi) \neq 0$ då χ är icke-trivial för att avsluta beviset av Dirichlets sats. Vi formulerar detta i en sats.

Sats 10.10. $L(1,\chi) \neq 0$ *för alla icke-triviala Dirichlet-karaktärer* χ.

Denna sats går att bevisa med hjälp av komplexanalytiska metoder, vilket vi kommer att göra genom att betrakta funktionen definierad som

$$\zeta_q(s) := \prod_{\chi} L(s, \chi) .$$

Vi definierar nu ett begrepp vi kommer att ha användning för.

Definition 10.5. *En Dirichletserie är en funktion på formen*

$$f(s) = \sum \frac{a_n}{n^s} ,$$

där summan konvergerar för $\mathrm{Re}(s) > \rho$.

Vi noterar att Riemanns zeta-funktion är en Dirichletserie med $a_n = 1$ för alla n.

Lemma 10.11. *Antag att en Dirichletserie $f(s)$ med $a_n \geq 0$ konvergerar för $\mathrm{Re}(s) > \rho$. Antag vidare att den har en analytisk fortsättning till ett halvplan $\mathrm{Re}(s) > \alpha$. Då konvergerar Dirichletserien på halvplanet $\mathrm{Re}(s) > \alpha$.*

Bevis. Vi gör beviset för $\rho = 0$ och visar att Dirichletserien stämmer överens med sin Taylorutveckling kring $s = 1$, vilken är giltig fram till $s = -\varepsilon > \alpha$, för ett godtyckligt α. Då $\sum a_n/n^s$ konvergerar likformigt på varje halvplan $\mathrm{Re}(s) \geq \rho > 0$ är f holomorf för $\mathrm{Re}(s) > 0$. Vi kan alltså Taylorutveckla f runt 1 och börjar med att derivera termvis k gånger för att få

$$f^{(k)}(s) = \sum_{n=1}^{\infty} a_n(-\log n)^k n^{-s} , \qquad \mathrm{Re}(s) > 0 .$$

Taylorutvecklingen av $f(s)$ runt $s = 1$ blir därför

$$f(s) = \sum_{k=0}^{\infty} \frac{f^{(k)}(1)}{k!}(s-1)^k = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n}{k!n}(-\log n)^k (s-1)^k .$$

Vi får därför att för $s = -\varepsilon > \alpha$ godtyckligt, kommer

$$f(-\varepsilon) = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n}{k!n}(-\log n)^k(-\varepsilon-1)^k = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{a_n}{k!n}(\log n)^k(\varepsilon+1)^k .$$

Vi utnyttjar här att alla termerna i summan är positiva, och byter därför summationsordning vilket leder till att den ena summan summerar till $e^{(\varepsilon+1)\log n}$. Alltså har vi att

$$f(-\varepsilon) = \sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{k=0}^{\infty} \frac{1}{k!}(\log n)^k(\varepsilon+1)^k = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{(\varepsilon+1)\log n} = \sum_{n=1}^{\infty} \frac{a_n}{n} n^{\varepsilon+1} = \sum_{n=1}^{\infty} a_n n^{\varepsilon} .$$

□

Vi introducerar nu ytterligare två lemman som kommer att behövas för att visa att $L-$funktionerna faktiskt är nollskilda i $s = 1$.

Lemma 10.12. $\zeta_q(s)$ *kan skrivas som en Dirichletserie med icke-negativa koefficienter.*

Bevis. Vi börjar med att visa polynomidentiteten

$$\prod_{\chi\in\hat{G}}(1-\chi(p)x)=(1-x^{f(p)})^{g(p)}, \quad p\nmid q\,, \tag{10.5}$$

där $f(p)$ är ordningen på p i gruppen $\mathbb{Z}^*(q)$ och $f(p)g(p)=\varphi(q)$. För att visa likheten räcker det att visa att vänster- och högerled har samma rötter och ledande koefficient. Vi har att

$$\left(\frac{1}{\chi(p)}\right)^{f(p)}=\overline{\chi(p)}^{f(p)}=\overline{\chi(p^{f(p)})}=\overline{\chi(1)}=1\,.$$

Alltså är $\chi(p)$ en $f(p)$-rot till enheten. Låt X vara mängden av alla $f(p)$-rötter till enheten. Vi har också att

$$\prod_{\xi\in X}(1-\xi x)=1-x^{f(p)}\,.$$

Alla rötter till vänsterledet finns i X eftersom $\chi(p)\in X$ för alla $\chi\in\hat{G}$. Vidare har alla rötter samma multiplicitet då det existerar $g(p)$ karaktärer $\chi(p)\in\hat{G}$ sådana att $\chi(p)=\xi$, vilket följer av symmetriskäl.

Genom att nu byta ut varje L-funktion med dess produktutveckling och genom att använda (10.5) med $x=p^{-s}$ kan vi utveckla produkten som definierar ζ_q till

$$\zeta_q(s)=\prod_{\chi}L(s,\chi)=\prod_{\chi,\,p}\frac{1}{1-\chi(p)p^{-s}}=\prod_p\frac{1}{(1-p^{-sf(p)})^{g(p)}}=$$

$$=\prod_p(1+p^{-sf(p)}+p^{-2sf(p)}+...)^{g(p)}\,,$$

vilken är en Dirichletserie med icke-negativa koefficienter och som konvergerar för $\mathrm{Re}(s)>1$. $\square$

Lemma 10.13. *Dirichletserien för $\zeta_q(s)$ divergerar i $s=1/\varphi(q)$ där φ är Eulers funktion.*

Bevis. För att visa att Dirichletserien för $\zeta_q(s)$ divergerar visar vi att den kan uppskattas nedåt med en divergent serie.

Vi gör detta genom att betrakta

$$\sum_{n=1}^{\infty}\frac{1}{n^{s\varphi(q)}}=\prod_p(1+p^{-s\varphi(q)}+p^{-2s\varphi(q)}+...)\,,$$

som är ekvivalent med Riemanns zetafunktion i punkten $s\varphi(q)$. Vi vill alltså visa att

$$\prod_p(1+p^{-sf(p)}+p^{-2sf(p)}+...)^{g(p)}\geq\prod_p(1+p^{-s\varphi(q)}+p^{-2s\varphi(q)}+...)\,,$$

Men eftersom $\varphi(q)=f(p)g(p)$ räcker det att visa att

$$\prod_p(1+p^{-sf(p)}+p^{-2sf(p)}+...)^{g(p)}\geq\prod_p(1+p^{-sf(p)g(p)}+p^{-2sf(p)g(p)}+...)\,.$$

Vilket innebär alltså att vi vill visa att produkten till höger blir mindre än den vänstra om man flyttar in potensen $g(p)$ och istället upphöjer varje enskild term. Detta kan formuleras för ett allmänt fall för godtyckliga tal $a_n \geq 0$ och ett tal $n \in \mathbb{N}$ enligt

$$(a_0 + a_1 + a_2 + \ldots)^n \geq (a_0^n + a_1^n + a_2^n + \ldots)\,.$$

Denna olikhet följer dock direkt utav binomialsatsen. Därmed gäller det att

$$\prod_p (1 + p^{-sf(p)} + p^{-2sf(p)} + \ldots)^{g(p)} \geq \prod_p (1 + p^{-s\varphi(q)} + p^{-2s\varphi(q)} + \ldots) = \sum n^{-s\varphi(q)}\,.$$

Notera att för $s = 1/\varphi(q)$ får vi den divergenta summan $\sum n^{-1}$ i högerledet. Enligt jämförelsekriteriet för summor divergerar därför då

$$\prod_p (1 + p^{-sf(p)} + p^{-2sf(p)} + \ldots)^{g(p)}\,,$$

vilket skulle visas. □

Bevis av Sats 10.10. Om det hade funnits en karaktär χ sådan att $L(1,\chi) = 0$, skulle detta innebära att $\zeta_q(s)$ är holomorf på halvplanet $\mathrm{Re}(s) > 0$, enligt Sats 10.13 och då $L(s,\chi_0)$ har en enkelpol i $s = 1$. Detta hade i sin tur medfört att Dirichletserien för $\zeta_q(s)$ konvergerade i detta halvplan, enligt Lemma 10.11 och 10.12. Men, vi *vet* att Dirichletserien för $\zeta_q(s)$ inte konvergerar enligt Lemma 10.13, alltså kan det ej finnas ett χ sådant att $L(1,\chi) = 0$. □

Bevis av Sats 10.4. Vi har alltså lyckats visa att $L(1,\chi) \neq 0$, samtidigt som vi har gett betydelse åt den komplexvärda logaritmen och bevisat Dirichlets produktformel. Proposition 10.9 ger då att

$$\log_2 L(s,\chi) = -\sum_p \log_1(1 - \chi(p)p^{-s}) = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Alltså gäller det att $\sum \chi(p)p^{-s}$ förblir begränsad och således divergerar

$$\lim_{s\to 1^+} \sum_{p\equiv \ell} \frac{1}{p^s}\,.$$

□