SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Primtalsfördelningar i linjära och ickelinjära mängder

av

Robert Jensen

2014 - No 19

Primtalsfördelningar i linjära och ickelinjära mängder

Robert Jensen

Självständigt arbete i matematik 30 högskolepoäng, grundnivå

Handledare: Rikard Bögvad

2014

PRIMTALSFÖRDELNINGAR I LINJÄRA OCH ICKELINJÄRA MÄNGDER

ROBERT JENSEN

Date: 10 September, 2014.

SAMMANFATTNING. Denna uppsats studerar hur primtal fördelar sig bland de naturliga talen, bland värden till linjära funktioner för att avslutningsvis studera primtal bland värden av kvadratiska funktioner. Vi bevisar Dirichlets Sats för aritmetisk progression med Dirichlet karaktärer och L-serier. I den avslutande delen drar vi paralleller mellan Bunyakowskihypotesen, Bateman-Horn hypotesen och Hardy-Littlewood hypotesen och illustrerar med en del enklare exempel.

Innehåll

1. Inledning

Denna uppsats kommer i stora drag att studera hur serier av primtal fördelar sig över olika mängder och funktioner. Vi börjar med att definiera vad ett primtal är.

Definition 1. Ett heltal $n > 1$ sägs vara ett primtal om de enda positiva delarna till n är 1 och n. Annars kallas n ett sammansatt tal. Vi kommer använda notationen p eller q för primtal.

Ofta brukar primtalen kallas talens byggstenar då varje heltal som har en faktor kan brytas ner som en produkt av primtal som t.ex. $60 = 2^2 \cdot 3 \cdot 5$ som kan delas med 2 (två gånger), 3 och 5. Aritmetikens fundamentalsats säger att varje sådan produkt är unik förutom ordningen på primtalen. Ett av de största problemen med primtal är att de är inhomogent distribuerade över de naturliga talen vilket gör att de är svåra att hitta. Detta innebär i praktiken att:

i) Det finns ingen generell formel för att erhålla primtal.
ii) Det är svårt att fullständigt faktorisera ett stort sammansatt tal.
iii) Det är oftast enkelt att heuristiskt förstå påståenden om primtal men det är extremt svårt att bevisa dem.

Även fast i) gäller (och kommer antagligen hålla väldigt länge) så finns det sätt att erhålla stora mängder primtal. Eratosthenas var en grekisk matematiker som levde på 200-talet f.kr. som kom på en enkel princip för detta. Tanken är att mängden av alla naturliga tal består dels av rena primtal samt andra tal som är sammansätta med flera faktorer. Således är en enkel metod att eliminera alla tal som har mer än en faktor för att endast få primtalen kvar. Detta kan då göras systematiskt genom att utgå från alla $n \in \mathbb{N}$ och först eliminera alla termer med faktorn 2 (förutom 2), sedan alla med faktorn $3, 4, 5, \ldots$ osv. tills endast de talen som är delbara med 1 och sig själva finns kvar. Detta kan låta som en omständig process, men är i själva verket smidig så länge N inte är stor eftersom nästan alla tal elimineras för de små faktorerna. Om vi t.ex. eliminerar faktorn 2 har vi automatiskt redan tagit bort faktorer $4, 6, 8, \ldots$ och om vi eliminerar faktorn 3 stryks faktorerna $6, 9, 12, \ldots$ osv. Om vi nu vill använda denna metod för att få fram alla primtal upp till $N = 120$ skulle det räcka med att dra bort faktorerna: $2, 3, 5, 7$. Eftersom den relativt prima faktor som kommer därefter är 11 kommer nästa tal som elimineras vara ett $n \geq 11^2 = 121$. Om vi genomför detta blir resultatet alla primtal $p \in \mathbb{N}$ där $p \leq 120$. De är

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113	....

Vi ser att primtalen avtar i antal för större N eftersom vi stryker tal för fler och fler faktorer ju större N blir. Om $N < p^2$ blir endast de n som är

relativt prima $2 \cdot 3 \cdot \ldots \cdot p$ primtal. Detta innebär att sannolikheten för att ett tal ska vara primtal minskar för större N. När man studerar stora mängder primtal tittar man ofta på dess asymptotiska uppföranden, dvs. vad som händer när N blir stort och gör en grov uppskattning på hur primtalen uppför sig. Vi kan nu studera primtal för stora N och undersöka om vi kan hitta en väldefinierad funktion som beskriver antalet primtal. Vi använder oss av funktionen $\pi(N)$ som för ett heltal N returnerar antalet primtal upp till N.[1]

N	$\pi(N)$
10^3	168
10^6	78,498
10^9	50,847,534
10^{12}	37,607,912,018
10^{15}	29,844,570,422,669
10^{18}	24,739,954,287,740,860

Denna tabell ger oss inte speciellt mycket information som vi inte redan vet. Vi ser att antalet primtal tunnas ut för större N dvs. att de påträffas mer sällan för stora tal, men vi kan fortfarande inte urskilja med hur mycket. Därför delar vi den första kolumnen med den andra för att se om det finns något mönster. Det vi får fram då är antalet heltal per primtal upp till ett visst värde N.

N	$\frac{N}{\pi(N)}$
10^3	5.9524
10^6	12.7392
10^9	19.6665
10^{12}	26.5901
10^{15}	33.6247
10^{18}	40.4204

Om vi nu tittar på tabellen ser vi att denna kvot ökar mellan $6.8 - 7.0$ när vi går från ett visst N till $10^3 N$. Denna typ av funktion känner vi igen från elementär analys. Om $y = e^{f(x)}$ är $f(x) = \ln y$. Vi jämför nu dessa två funktioner i en tabell med respektive procentuella fel (σ).

N	$\frac{N}{\pi(N)}$	$\ln N$	$\sigma(\%)$
10^3	5.9524	6.9077	16.0490
10^6	12.7392	13.8155	8.4487
10^9	19.6665	20.7232	5.3731
10^{12}	26.5901	27.6310	3.9146
10^{15}	33.6247	34.5378	2.7156
10^{18}	40.4204	41.4465	2.5386

[1] Vi använder tabeller och resonemang från Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics s.38-39

För stora N ser vi att $\frac{N}{\pi(N)}$ och $\ln N$ närmar sig varandra eftersom $\sigma \to 0$. Detta innebär att

$$\frac{N}{\pi(N)} \sim \ln N \Rightarrow \pi(N) \sim \frac{N}{\ln N},$$

för stora värden på N. Resultatet vi empiriskt har kommit fram till kallas Primtalssatsen. Vi kan dra direkta slutsatser från detta preliminära resultat.

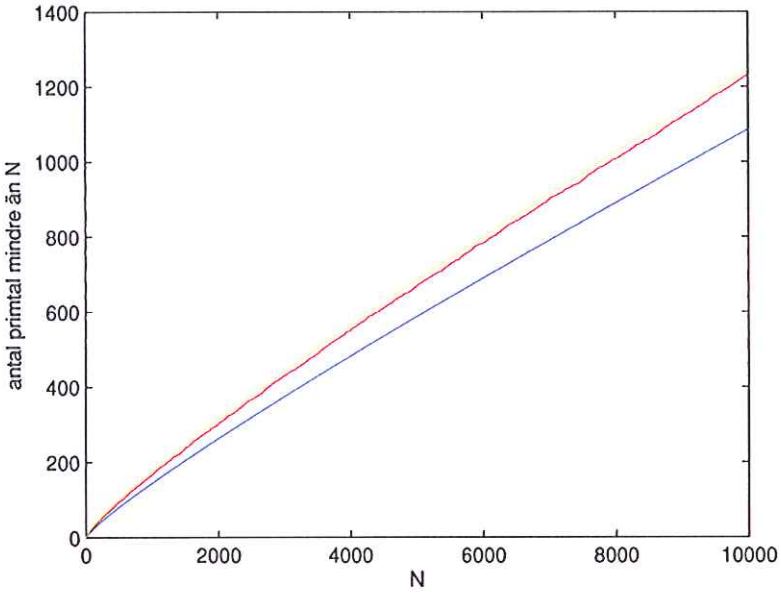
Vi observerar att $\pi(N)/N$ berättar om förhållandet mellan antalet primtal och heltal, dvs. sannolikheten att ett tal upp till N ska vara primtal vilket kallas *primtalsdensitet*. Primtalssatsen ger oss då en approximativ funktion till denna sannolikhet som blir mer exakt för större N:

$$\pi(N)/N \sim \frac{1}{\ln N}.$$

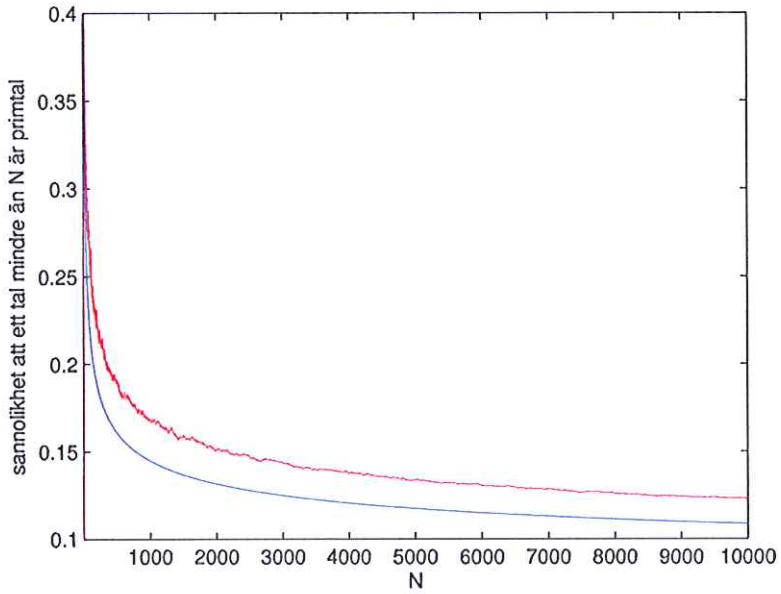
Detta är ett viktigt resultat. Om vi nu tänker oss att vi multiplicerar varje tal t där $2 \leq t \leq N$ med respektive sannolikhet att t ska vara ett primtal och sedan summerar alla dessa borde detta logiskt ge antalet primtal upp till N. Detta var vad Carl Friedrich Gauss gissade när han ansåg att en bättre approximation på $\pi(N)$ kunde göras med detta resonemang. I praktiken gjordes detta med en logaritmisk integral för alla värden mellan 2 och N, vilket även innebär att singulariteten vid $t = 1$ undviks.

$$\mathrm{Li}(N) = \int_2^N \frac{dt}{\ln(t)}.$$

Detta innebär att vi har två olika uppskattningar $\mathrm{Li}(N) \sim N/\ln N \sim \pi(N)$ på hur primtalen är distribuerade över $\mathbb{N}$ för stora N. För att illustrera sambandet mellan antalet primtal och dessa två uppskattningar ser vi från Fig.1 att $\ln N < N/\pi(N) < \mathrm{Li}(N)$ för $N = 10000$ dvs. att proportionen mellan antalet tal och primtal är inspärrade mellan dessa två funktioner. Alla grafer är ritade i Matlab.



FIGUR 1. Jämförelse mellan $\pi(N)$(röd kurva), $\mathrm{Li}(N)$ (gul kurva) och $N/\ln N$(blå kurva) upp till $N = 10000$.



FIGUR 2. Visar sannolikheten för att ett tal ska vara primtal (röd kurva) jämfört med $1/\ln N$ (blå kurva).

Enligt Fig.1 ser vi, såsom vi tidigare har noterat, att sannolikheten för att ett tal ska vara primtal minskar med större tal, dvs. att primtalen tunnas ut för större tal. Frågan är om primtalen för tillräckligt stora värden kommer att ta slut och ett största primtal kan hittas var fram till 300 f.kr. ett *öppet problem* då den grekiske matematikern Euklides lyckades bevisa detta. Detta är ett av de mest välkända bevisen inom matematiken som bygger på att det i en lista med primtal finns det alltid ett större primtal att hitta.

Sats 1. *Det finns oändligt antal primtal.*

Bevis. Anta att $p_1 = 2 < p_2 = 3 < \ldots < p_n$ är en ändlig lista över alla primtal. Låt $P = p_1 p_2 \cdot \ldots \cdot p_n + 1$. Det är antingen ett primtal eller sammansatt av primtal. Om P är ett primtal har vi hittat ett primtal som inte hör till vår lista. Om P inte är ett primtal finns det ett primtal p som delar P. Observera att p inte kan vara någon av $p_1, p_2, \ldots, p_n$ eftersom då skulle p dela 1 vilket är omöjligt. Alltså måste p vara ett primtal som inte finns i listan. □

Vi har visat att det finns oändligt många primtal för de naturliga talen $\mathbb{N}$. Vi kommer nu studera vad som händer om vi t.ex. delar in $\mathbb{N}$ i fyra delar dvs. $\mathbb{N} = \{4\mathbb{N}, (4\mathbb{N}+1), (4\mathbb{N}+2), (4\mathbb{N}+3)\}$. Detta kan representeras med fyra aritmetiska följder där $n \in \mathbb{N}$

$$4n : 0, 4, 8, 12, 16, 20, 24, \ldots$$

$$4n+1 : 1, 5, 9, 13, 17, 21, 25, \ldots$$

$$4n+2 : 2, 6, 10, 14, 18, 22, 26, \ldots$$

$$4n+3 : 3, 7, 11, 15, 19, 23, 27, \ldots .$$

Vi observerar uppenbart att inga primtal finns med i sekvensen $4n$ då för $n \geq 1$ varje term är delbar med 2^2. I $4n+2$ finns endast ett primtal, nämligen 2 då $n = 0$, annars är varje term delbar med 2. Detta innebär att de oändligt antal primtal som finns i $\mathbb{N}$ borde således ligga i de aritmetiska följderna $4n+1$ och $4n+3 = 4n-1$ för $n \in \mathbb{N}$. Vi bevisar nu att även dessa följder har oändligt antal primtal.[2]

Sats 2. *Det finns ett oändligt antal primtal i följden* $4n-1$ *där* $n \in \mathbb{N}$.

Bevis. Detta kan bevisas genom motsägelse. Antag att det finns ett ändligt antal primtal i följden $4n-1$ där $n \in \mathbb{N}$ och att p är det största primtalet. Om vi tittar på produkten

$$N = 2^2 \cdot 3 \cdot 5 \cdot \ldots p - 1,$$

[2]Apostol, Tom M., Introduction to analytic number theory, Undergraduate Texts in Mathematics, Springer-Verlag, (1976) s. 147

så är N på formen $4n-1$ men kan inte vara ett primtal eftersom $N > p$. Inget primtal som är mindre än p delar N så alla primfaktorer måste överstiga p. Dock kan inte alla primtalsfaktorer vara på formen $4n+1$ eftersom produkten av två sådana tal också är på formen $4n+1$. Detta medför att några av primtalsfaktorerna måste vara på formen $4n-1$. Detta är en motsägelse. □

Vi visar att följden $4n+1$ har oändligt antal primtal med ett annat argument där vi använder oss av Euler-Fermats theorem.

Sats 3. *Det finns ett oändligt antal primtal i följden* $4n+1$ *där* $n \in \mathbb{N}$.

Bevis. Vi visar att för ett godtyckligt tal $N > 1$ finns det alltid ett större primtal p att hitta med $p \equiv 1 \pmod 4$. Om vi låter

$$m = (N!)^2 + 1$$

ser vi att $m > 1$ är ett udda tal eftersom $N!$ alltid är jämn. Låt p vara den minsta primfaktorn av m. Vi ser att inget av talen $2, 3, \ldots, N$ delar m vilket innebär att $p > N$. Vi har då

$$(N!)^2 \equiv -1 \pmod p.$$

Genom att höja upp båda sidorna med $(p-1)/2$ får vi

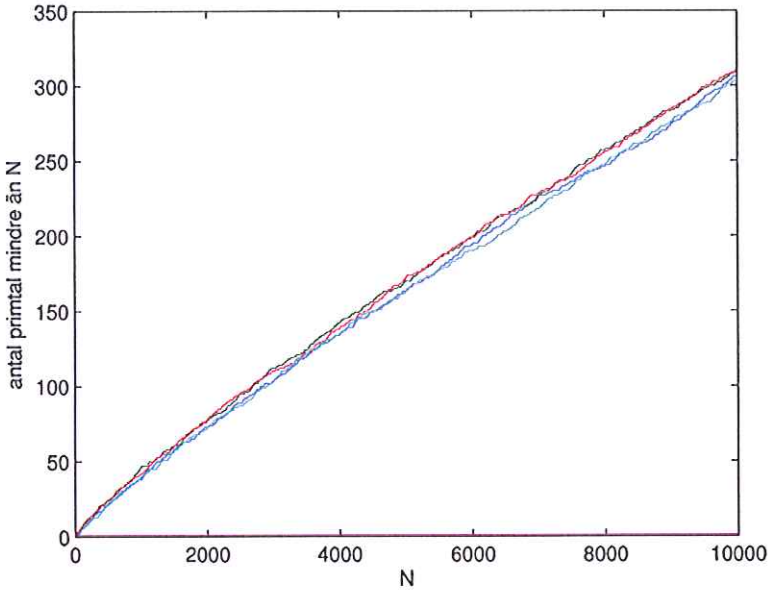
$$(N!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p.$$

Enligt Euler-Fermats sats gäller att $(N!)^{p-1} \equiv 1 \pmod p$

$$(-1)^{(p-1)/2} \equiv 1 \pmod p.$$

Detta inträffar då $(p-1)/2$ är ett jämt tal n dvs. då $(p-1)/2 = 2n$. Om vi löser ut p ser vi att $p = 4n+1$ vilket är detsamma som $p \equiv 1 \pmod 4$. Alltså finns det ett alltid primtal p större än N för vilket $p \equiv 1 \pmod 4$. □

Nu har vi således visat att det finns ett oändligt antal primtal i de aritmetiska följderna $4n+1$ och $4n+3$ medan för de andra två följderna $4n$ och $4n+2$ fanns det noll respektive ett primtal. Om vi analogt delar in heltalen i fem delar $\mathbb{N} = \{5\mathbb{N}, (5\mathbb{N}+1), (5\mathbb{N}+2), (5\mathbb{N}+3), (5\mathbb{N}+4)\}$, så har följden $5n, n \in \mathbb{N}$ endast primtalet 5 medan de andra aritmetiska följderna verkar ha stora mängder primtal. Frågan är hur primtalen fördelar sig över dessa följder, vilket vi undersöker med grafer för $\#\{p : \text{primtal}, p \equiv a \pmod 5, p \leq N\}$ upp till $N = 10000$ och $a = 0, 1, 2, 3, 4$.

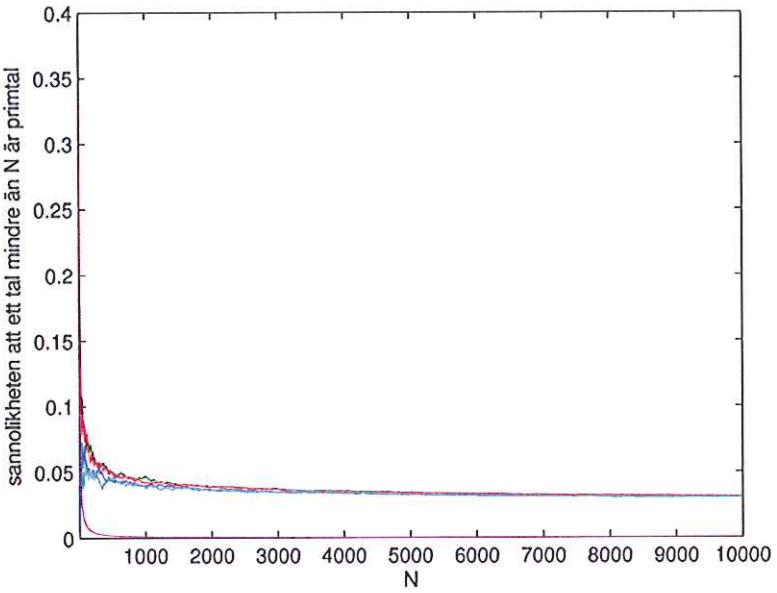


FIGUR 3. Grafen visar $\#\{p \equiv a \pmod 5, p \leq N\}$ för $a = 0, 1, 2, 3, 4$ upp till $N = 10000$.

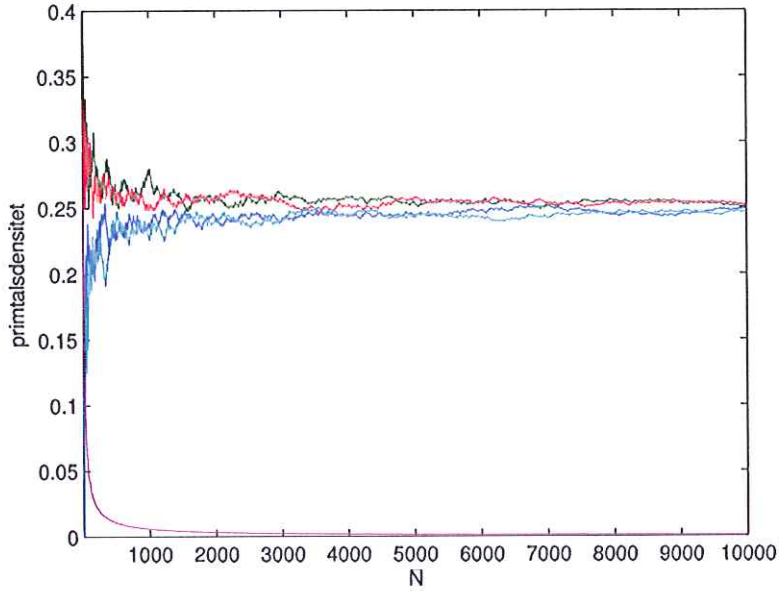
Vi observerar att primtalen verkar distribuera sig jämt för stora N mellan de aritmetiska följderna med relativt prima koefficenter för $(a, 5) = 1$ dvs. $a = 1, 2, 3, 4$. Här kan konstateras att totala antalet primtal som finns med i detta fallet blir $306+309+310+303+1 = 1229$ vilket stämmer överens med den andra grafen för de naturliga talen upp till $N = 10000$. Utifrån Figur 5 kan vi gissa att primtalsdensiteten för respektive aritmetisk följd ges av

$$\lim_{N\to\infty} \frac{\#primtal \equiv a \pmod 5}{\#primtal} \to \frac{1}{4}$$

för $a = 1, 2, 3, 4$.



FIGUR 4. Grafen visar $\#\{p \equiv a \pmod 5), p \leq N\}/N$ för $a = 0, 1, 2, 3, 4$ upp till N=10000.



FIGUR 5. Grafen visar $\#\{p \equiv a \pmod 5), p \leq N\}/\#\{p, p \leq N\}$ för $a = 0, 1, 2, 3, 4$ upp till $N = 10000$.

Större delen av denna uppsats kommer fokusera på att generalisera och visa detta resonemang strikt. Den tyske matematikern Dirichlet lyckades 1837 med detta m.h.a. analytiska metoder och visade speciellt att varje aritmetisk följd med relativt prima koefficenter har ett oändligt antal primtal. Detta är alltså en utvidgning av Euklides bevis som endast visar att de naturliga talen har oändligt antal primtal. Nästa sektion kommer gå igenom grundteori som behövs för att bevisa Dirichlets sats för aritmetisk progression.

2. Grundteori

2.1. Riemanns zetafunktions koppling till primtalen. [3]Riemann zetafunktion definieras som

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots \tag{1}$$

Denna funktion konvergerar för $s > 1$ och konvergerar till och med likformigt för $s \geq 1+\delta > 1$, för ett litet tillskott $\delta > 0$. Således är (1) en analytisk funktion på halvplanet för alla $s > 1$. Riemanns zetafunktion kan på ett naturligt sätt länkas till en oändlig produkt över primtal genom Eulers upptäckt.

Proposition 1. *Om $s > 1$ så gäller att*

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1} \tag{2}$$

där produkten tas över alla primtal.

När Euler kom fram till (2) använde han sig av Eratosthenes princip, som vi har talat om tidigare. Inledningsvis illustreras detta på ett mer övergripligt sätt med denna metod.

$$\zeta(s) = \textstyle\sum_{n=1}^{\infty} n^{-s} \implies$$

$$2^{-s}\zeta(s) = 2^{-s} \textstyle\sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} (2n)^{-s}$$

Vi börjar med att eliminera alla termer med en faktor 2 från Riemann-zeta funktionen genom att subtrahera den andra ekvationen från den första.

$$\zeta(s) - 2^{-s}\zeta(s) = (1 - 2^{-s})\zeta(s) = \sum_{n=1}^{\infty} (n^{-s} - (2n)^{-s}) = \sum_{2 \nmid n} n^{-s}.$$

Fortsätt analogt processen genom att dra bort alla faktorer med en faktor 3.

$$(1 - 2^{-s})(1 - 3^{-s})\zeta(s) = (1 - 2^{-s})\zeta(s) - 3^{-s}(1 - 2^{-s})\zeta(s) =$$

[3]Detta avsnitt följer Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, 2nd ed. (1990) s.249-261

$$\sum_{2\nmid n} n^{-s} - 3^{-s}\sum_{2\nmid n} n^{-s} = \sum_{2\nmid n}(n^{-s} - (3n)^{-s}) = \sum_{2,3\nmid n} n^{-s}.$$

Genom att analogt upprepa processen får vi till slut

$$(1-2^{-s})(1-3^{-s})(1-5^{-s})\dots(1-p^{-s})\dots\zeta(s) = \sum_{2,3,5,7,\dots\nmid n} n^{-s} = 1.$$

Genom att omordna termerna kommer vi fram till (2).

För att göra ett mer strikt bevis behöver vi använda oss av oändliga geometriska serier för summor.

Lemma 1. ***Geometrisk serie för summor*** *Om* $|x| < 1$ *gäller att*

(3)

a)

$$(1-x)^{-1} = \sum_{n=0}^{\infty} x^n.$$

b)

$$\ln(1-x)^{-1} = \sum_{n=1}^{\infty} x^n n^{-1}.$$

Bevis. *a*) Sätt $s_N = \sum_{k=0}^{N} x^k$. Vi kan multiplicera med $1-x$ för att sedan flytta om termerna

$$(1-x)s_N = (1-x)\sum_{k=0}^{N} x^k = \sum_{k=0}^{N}(1-x)x^k = \sum_{k=0}^{N}(x^k - x^{k+1}) = 1 - x^{N+1}.$$

Vi ser att alla termer tar ut varandra förutom den första och den sista. Lös ut s_N och låt $N \to \infty$

$$\lim_{N\to\infty} s_N = \lim_{N\to\infty}\left((1-x^{N+1})(1-x)^{-1}\right) = (1-x)^{-1}$$

då $|x| < 1$. Således konvergerar s_N för alla $|x| < 1$ med gränsvärdet $s_N = (1-x)^{-1}$. Observera att *a*) kan analogt visas gälla för alla komplexa tal $|z| < 1, z \in \mathbb{C}$.

b) visas genom att integrera båda leden i *a*) med avseende på en parameter $0 < t < x$.

$$\int_0^x (1-t)^{-1}dt = \int_0^x \sum_{k=0}^{\infty} x^k dt.$$

Integralen i vänster led beräknas som

$$\int_0^x (1-t)^{-1}dt = [-\ln(1-t)]_0^x = \ln(1-x)^{-1}.$$

Höger led ger sedan

$$\int_0^x \sum_{k=0}^{\infty} x^k dt = \sum_{k=0}^{\infty} \int_0^x x^k dt = \sum_{k=0}^{\infty} \left[t^{k+1}(t+1)^{-1}\right]_0^x =$$

$$\sum_{k=0}^{\infty} x^{k+1}(x+1)^{-1} = \sum_{k=1}^{\infty} x^k x^{-1}$$

där den första likheten är sann pga. den likformiga konvergensen vilket visar b)[4]. □

Med dessa resultat är vi redo att bevisa (2).

Bevis. (2) Om $s > 1$ så $p^{-s} < 1$.

Således ger (3a) med $x = p^{-s}$ att

$$\sum_{m=1}^{\infty} (p^{-s})^m = (1 - p^{-s})^{-1}.$$

Produkten över alla primtal $p \leq N$ ger

$$\prod_{p \leq N} (\sum_{m=1}^{\infty} p^{-sm}) = \prod_{p \leq N} (1 - p^{-s})^{-1}.$$

Varje tal har en unik primtalsfaktorisering enligt aritmetikens fundamentalsats vilket medför

$$\prod_{p \leq N} (1 - p^{-s})^{-1} = \sum_{n \leq N} n^{-s} + R_N(s).$$

Det som återstår är visa att när $N \to \infty$ så gäller att $R_N(s) \to 0$. Detta gör vi genom att hitta en övre begränsning till $R_N(s)$. Uppenbart gäller att $R_N(s) \leq \sum_{N+1}^{\infty} n^{-s}$. Eftersom $\zeta(s)$ konvergerar så följer att $R_N(s) \to 0$. $R_N(s)$ är en begränsad funktion och då $N \to \infty$ så gäller att $R_N(s) \to 0$. □

Dirichlet studerade hur Riemanns zetafunktion uppför sig när den närmar sig $s = 1^+$. Nedan visar vi att Riemanns zetafunktion har en enkel pol i $s = 1$ med residyn 1.

Proposition 2. *Anta att $s > 1$. Då gäller*

$$\lim_{s \to 1} (s - 1)\zeta(s) = 1. \tag{4}$$

Bevis. För fixerat s är $f(t) = t^{-s}$ en monotont avtagande funktion för alla positiva $n \Rightarrow$ på intervallet $[n, n+1]$ är $\max(f([n, n+1])) = f(n)$ och $\min(f([n, n+1])) = f(n+1)$ vilket innebär att arean under grafen till $f(t)$ är instängd mellan de två rektanglarna $f(n+1)((n+1)-n) = f(n+1)$ och $f(n)((n+1)-n) = f(n)$. Detta medför att

[4]E.B. Saff, A.D. Snider, Fundamentals of Complex Analysis, 3rd ed., Pearsson Education(2003), s.239

$$f(n+1) < \int_n^{n+1} f(t)dt < f(n) \Rightarrow (n+1)^{-s} < \int_n^{n+1} t^{-s}dt < n^{-s}.$$

Summation över alla $n \in \mathbb{Z}_+$ ger

$$\sum_{n=1}^{\infty}(n+1)^{-s} = \sum_{n=1}^{\infty} n^{-s} - 1 < \int_1^{\infty} t^{-s}dt < \sum_{n=1}^{\infty} n^{-s}.$$

Integralen beräknas genom

$$\int_1^{\infty} t^{-s}dt = \lim_{N\to\infty}\left[(1-s)^{-1}t^{1-s}\right]_1^N = \lim_{N\to\infty}(1-s)^{-1}(N^{1-s}-1) = (s-1)^{-1}.$$

Kombinerat med värdet på integralen har vi då

$$\zeta(s) - 1 < (s-1)^{-1} < \zeta(s) \Rightarrow 1 < (s-1)\zeta(s) < s.$$

Avslutningsvis stänger vi in värdet genom att låta s närma sig 1, vilket fullbordar beviset och ger att

$$\lim_{s\to 1}(s-1)\zeta(s) = 1.$$

□

Nästa proposition är ett viktigt gränsvärde.

Proposition 3. *Då $s \to 1$ gäller att*

$$\frac{\ln\zeta(s)}{\ln(s-1)^{-1}} \to 1. \tag{5}$$

Bevis. Definiera hjälpfunktionen $\rho(s) = (s-1)\zeta(s)$ där $\rho(s) \to 1$ då $s \to 1$ enligt tidigare proposition. Logaritmering ger att

$$\ln(s-1) + \ln\zeta(s) = \ln\rho(s) \Rightarrow \frac{\ln\zeta(s)}{\ln(s-1)^{-1}} = 1 + \frac{\ln\rho(s)}{\ln(s-1)^{-1}}$$

där $\ln\rho(s) \to 0$ samt $ln(s-1)^{-1} = -ln(s-1) \to \infty$ då $s \to 1$. Alltså är

$$\lim_{s\to 1}\frac{\ln\rho(s)}{\ln(s-1)^{-1}} = 0.$$

Beviset fullbordas vid gränsövergång

$$\lim_{s\to 1}\frac{\ln\zeta(s)}{\ln(s-1)^{-1}} = 1.$$

□

Om vi logaritmerar Eulers produkt över primtal (2), skriver om den som en summa plus en begränsad funktion med försumbara termer får vi följande resultat.

Proposition 4. *Det gäller att*

$$\ln \zeta(s) = \sum_p p^{-s} + R(s) \tag{6}$$

där R(s) är en begränsad funktion då $s \to 1$.

Bevis. Logaritmering av (1) kombinerat med (3) ger att

$$\ln \zeta(s) = \ln\left(\sum_{n=1}^{\infty} n^{-s}\right) = \ln\left(\prod_p (1-p^{-s})^{-1}\right) = \sum_p \ln\left((1-p^{-s})^{-1}\right).$$

Om vi använder (3b) med $x = p^{-s} < 1$ kan vi skriva detta som

$$\ln \zeta(s) = \sum_p \sum_{m=1}^{\infty} p^{-ms} m^{-1} = \sum_p p^{-s} + \sum_p \sum_{m=2}^{\infty} p^{-ms} m^{-1} = \sum_p p^{-s} + R(s).$$

Det räcker med att visa att R(s) har en övre begränsning. Detta gör vi genom att använda (2) och hitta lämpliga övre gränser.

$$R(s) = \sum_p \sum_{m=2}^{\infty} p^{-ms} m^{-1} \leq \sum_p p^{-2s}(1-p^{-s})^{-1} = \sum_p p^{-2s} \sum_p (1-p^{-s})^{-1}$$

där vi har använt att $1/m < 1$ och att $\sum_{m=2} p^{-ms} = p^{-2s}(1-p^{-s})^{-1}$ samt delat upp summan. Vidare är $\sum_p (1-p^{-s})^{-1} < (1-2^{-s})^{-1}$ vilket innebär att

$$\sum_p p^{-2s} \sum_p (1-p^{-s})^{-1} < (1-2^{-s})^{-1} \sum_p p^{-2s} \leq (1-2^{-s})^{-1} \zeta(2s).$$

Således är $R(s) < (1-2^{-s})^{-1}\zeta(2s)$ begränsad och beviset är fullbordat. □

Med dessa resultat kan vi nu definiera Dirichletdensitet.

2.2. Dirichletdensitet.

Definition 2. En mängd $\mathscr{P} = \{p \in \mathscr{P}; p > 0\}$ sägs ha Dirichletdensitet om $\exists d(\mathscr{P})$ s.a.

$$d(\mathscr{P}) = \lim_{s \to 1} \frac{\sum_{p \in P} p^{-s}}{\ln(s-1)^{-1}}. \tag{7}$$

$d(\mathscr{P})$ sägs då vara Dirichletdensiteten av $\mathscr{P}$.

Dirichletdensitetens värde följer ett enkelt samband beroende på vilka egenskaper $\mathscr{P}$ har. Detta illustreras av nästa proposition.

Proposition 5. *Låt* $\mathscr{P}$ *vara en mängd av primtal. Då gäller att*

a) *Om* $\mathscr{P}$ *är en ändlig mängd är Dirichlet densiteten* $d(\mathscr{P}) = 0$.
b) *Om* $\mathscr{P}$ *är en alla primtal bortsett från ett ändligt antal gäller att* $d(\mathscr{P}) = 1$.

c) *Om* $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2$, *där* $\mathscr{P}_1$ *och* $\mathscr{P}_2$ *är disjunkta mängder med Dirichlet-densitet, så gäller att* $d(\mathscr{P}) = d(\mathscr{P}_1) + d(\mathscr{P}_2)$.

3. Dirichlets sats

Nu är vi i stånd att kunna formulera denna uppsats huvudsats.

Sats 4. *Antag att* $a, m \in \mathbb{Z}$ *med* $(a, m) = 1$. *Låt* $\mathscr{P}(a, m)$ *vara mängden av alla positiva primtal* p *s.a* $p \equiv a \pmod{m}$. *Då gäller att*

$$d(\mathscr{P}(a, m)) = \frac{1}{\phi(m)}. \tag{8}$$

3.1. **Vad säger Dirichlets sats?** Om vi har ett primtal i en av kongruensklasserna modulo m, dvs. av formen $p = a + mn$, $n \in \mathbb{Z}$ så måste $(a, m) = 1$. Antalet $0 \leq a \leq m$ så att $(a, m) = 1$ är $\phi(m)$ där ϕ är Eulers ϕ-funktion. Alltså måste p ligga i en av $\phi(m)$ kongruensklasser. Dirichlets sats säger nu att primtalen ligger jämnt, alltså ungefär lika många (mätt med Dirichletdensitet) i var och en av dessa kongruensklasser. T.ex. om $m = 4$ är $1, 3$ de enda möjliga $0 < a \leq 4$ sådana att $(a, m) = 1$ och $\phi(4) = 2$. Satsen säger att ungefär hälften av alla primtal är av formen $4n + 1$, $n \in \mathbb{Z}$ och hälften är av formen $4n - 1$ vilket överensstämmer med tidigare exprimentella resultat. Avslutningsvis säger Dirichlets sats att mängden primtal i varje aritmetisk progression, $\mathscr{P}(a, m)$, måste vara oändlig eftersom annars skulle Dirichletdensiteten vara noll enligt proposition 5b) dvs. alla aritmetiska följder med relativt prima koefficenter har oändligt antal primtal.

3.2. **Specialfall.** Vi börjar med att bevisa (8) för $m = 4$ för att få en bild av hur beviset kan göras för att sedan kunna generalisera detta i nästa sektion till ett fullvärdigt bevis. Första steget är lämpligtvis att dela upp termerna i Riemanns zetafunktion på ett sådant sätt att vi kan tillämpa grundteorin från sektion 2. Denna indelning varierar beroende på värdet på m men kan till en början förenklas för specialfallet $m = 4$ genom att definiera en funktion $\chi(n) : \mathbb{Z} \to \{0, \pm 1\}$ för alla $n \in \mathbb{Z}$ med följande tre indelningar:

i) $\chi(n) = 0$ om n är ett jämt tal.
ii) $\chi(n) = 1$ om $n = 1 \pmod 4$.
iii) $\chi(n) = -1$ om $n = 3 \pmod 4$.

Proposition 6. *Funktionen* $\chi(n) : \mathbb{Z} \to \{0, \pm 1\}$ *är en homomorfism eftersom det gäller att* $\chi(ab) = \chi(a)\chi(b)$ *för alla* $a, b \in \mathbb{Z}$.

Bevis. Om a eller b är jämt är enligt i) $\chi(ab) = \chi(a)\chi(b) = 0$ annars gäller att

$$\chi(ab) = [ab]_4 = [a]_4[b]_4 = \chi(a)\chi(b)$$

för alla $a, b \in \mathbb{Z}$ där $(a, m) = 1$ and $(b, m) = 1$. □

Denna funktion är en Dirichletkaraktär som vi kommer studera mer i nästa sektion. Genom att använda dessa homomorfier kan vi på ett naturligt sätt modifiera Riemanns zetafunktion för att kunna dela upp termerna. Det vi vill uppnå är att dela upp dem i $n = 1 \pmod 4$ och $n = 3 \pmod 4$ på ett smidigt sätt. Detta illustreras i ett enkelt exempel för $m = 4$.

Exempel 1. *Titta på funktionerna*

$$\psi_1(n) = \frac{\chi(n) + I(n)}{2}.$$

Om $n \equiv 1 \pmod 4$ *så* $\psi(n) = 1$.
Om $n \equiv 3 \pmod 4$ *så* $\psi(n) = 0$.
Om $n \equiv 0, 2 \pmod 4$ *så* $\psi(n) = 0$.

Alltså är

$$\psi_1(n) = 1 \Leftrightarrow n \equiv 1 \pmod 4$$

och

$$\psi_1(n) = 0 \Leftrightarrow n \not\equiv 1 \pmod 4.$$

På samma sätt är för

$$\psi_2(n) = \frac{I(n) - \chi(n)}{2},$$

$$\psi_2(n) = 1 \Leftrightarrow n \equiv 3 \pmod 4$$

och

$$\psi_2(n) = 0 \Leftrightarrow n \not\equiv 3 \pmod 4.$$

Vi ser att ψ_1, ψ_2 *är precis skilda från* 0 *och antar värdet* 1 *på varsin kongruensklass av de två som kan innehålla primtal.*

Nu ska vi utvidga exempel 1 med teori från sektion 2.
Vi börjar med att modifiera Riemanns zetafunkion med χ.

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots . \tag{9}$$

Denna funktion kallas Dirichlets L-funktion. Att $L(\chi, s)$ är en konvergerande funktion för $s > 1$ kan inses genom att den är begränsad av Riemanns zetafunktion. Definitionen av $\chi(n)$ ger att $|\chi(n)n^{-s}| \leq n^{-s}$ för $n \in \mathbb{Z}^+$ eftersom antingen är de lika eller då n är jämn, är $\chi(n) = 0$. Enligt Cauchys kriterium för serier konvergerar $L(\chi, s)$ eftersom Riemann-Zeta funktionen konvergerar för $s > 1$. Det är lämpligt att endast ta de udda termerna av Riemanns zetafunktion och definiera

$$\zeta^*(s) = \sum_{n \text{ udda}} n^{-s} = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \dots .$$

Vi observerade tidigare att de aritmetiska följderna inte endast genererar primtal. Detta problem kan elimineras genom att använda (2). Eftersom $\chi(n)$ är en multiplikativ funktion ger detta tillsammans med (2) att

$$L(\chi, n) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{p \text{ udda}} (1 - \chi(p) p^{-s})^{-1}.$$

För ζ^* gäller något liknande, som ses genom sambandet

$$\sum_{n \text{ udda}} n^{-s} = \sum_{n=1}^{\infty} n^{-s} - \sum_{n \text{ jmn}} n^{-s} = \sum_{n=1}^{\infty} n^{-s} - 2^{-s} \sum_{n=1}^{\infty} n^{-s} =$$

$$(1 - 2^{-s}) \sum_{n=1}^{\infty} n^{-s} = (1 - 2^{-s}) \zeta(s).$$

Detta tillsammans med (2) innebär då att

$$\sum_{n \text{ udda}} n^{-s} = (1 - 2^{-s}) \prod_{p} (1 - p^{-s})^{-1} = \prod_{p \text{ udda}} (1 - p^{-s})^{-1}.$$

Nu har vi uttryckt de båda funktionerna $L(\chi, s)$ och ζ^* som en produkt över udda primtal dvs. alla primtal förutom 2. Dock vill vi ha dessa funktioner uttryckt i summor för att kunna lägga ihop deras termerna som i Exempel 1. Detta gör vi genom att använda oss av (6) och gå till väga på samma sätt som i proposition 4. Detta ger oss att

i)
$$\ln L(\chi, s) = \sum_{p \text{ udda}} \chi(p) p^{-s} + R_1(s)$$

ii)
$$\ln \zeta^*(s) = \sum_{p \text{ udda}} p^{-s} + R_2(s)$$

där $R_1(s)$ och $R_2(s)$ är begränsade funktioner då $s \to 1$. Nu är termerna uppdelade på ett sådant sätt att vi kan lägga ihop respektive dra ifrån i) och ii). Detta ger vidare

iii)
$$\ln \zeta^*(s) + \ln L(\chi(p), s) = 2 \sum_{p \equiv 1 \,(4)} p^{-s} + R_3(s)$$

iv)
$$\ln \zeta^*(s) - \ln L(\chi(p), s) = 2 \sum_{p \equiv 3 \,(4)} p^{-s} + R_4(s)$$

där $R_3(s)$ och $R_4(s)$ är begränsade funktioner då $s \to 1$. För att visa att $\ln L(\chi, s)$ är begränsad då $s \to 1$ arrangerar vi om dess termer på följande sätt

$$L(\chi, s) = (1 - \frac{1}{3}) + (\frac{1}{5} - \frac{1}{7}) + \ldots$$

$$L(\chi, s) = 1 - (\frac{1}{3} - \frac{1}{5}) - (\frac{1}{7} - \frac{1}{9}) + \dots .$$

Från den första likheten kan vi konstatera att $L(\chi, s) > (1 - 1/3) = 2/3$ eftersom varje parentes vi lägger till är positiv för $s > 1$. Med omvänt resonemang ser vi från den andra likheten att $L(\chi, s) < 1$ då varje parentes vi drar ifrån är positiv. Tillsammans ger detta att $2/3 < L(\chi, s) < 1 \Rightarrow \ln(2/3) < \ln L(\chi, s) < \ln 1 = 0$ för $s > 1$. Så $L(\chi, s)$ är begränsad då $s \to 1$.

Nu är det lämpligt att undersöka hur termerna $\ln \zeta^*(s)$ och $\ln L(\chi(p), s)$ i iii) och iv) uppför sig då $s \to 1$. Eftersom vi har visat att $\zeta^*(s) = (1 - 2^{-s})\zeta(s)$ gäller att

$$\ln \zeta^*(s) = \ln((1 - 2^{-s})\zeta(s)) = \ln(1 - 2^{-s}) + \ln \zeta(s).$$

Vi dividerar med $\ln(s-1)^{-1}$ vilket ger

$$\frac{\ln \zeta^*(s)}{\ln(s-1)^{-1}} = \frac{\ln(1 - 2^{-s})}{\ln(s-1)^{-1}} + \frac{\ln \zeta(s)}{\ln(s-1)^{-1}}.$$

Detta tillsammans med (5) ger att $\ln \zeta^*(s)/\ln(s-1)^{-1} \to 1$ då $s \to 1$.

Om vi nu dividerar iii) och iv) med $\ln(s-1)^{-1}$ och låter $s \to 1$ för att kunna tillämpa dirichletdensiteten från (7) får vi

v)

$$\lim_{s\to 1} \frac{\ln \zeta^*(s)}{\ln(s-1)^{-1}} = 2 \lim_{s\to 1} \frac{\sum_{p\equiv 1\,(4)} p^{-s}}{\ln(s-1)^{-1}} = 2d(\mathscr{P}(1;4))$$

vi)

$$\lim_{s\to 1} \frac{\ln \zeta^*(s)}{\ln(s-1)^{-1}} = 2 \lim_{s\to 1} \frac{\sum_{p\equiv 3\,(4)} p^{-s}}{\ln(s-1)^{-1}} = 2d(\mathscr{P}(3;4))$$

där $R(s)$ och $\ln L(\chi(s), s)$ är begränsade funktioner vilket gör att deras bidrag till gränsvärdet försvinner.

Vi såg nyss att $\lim_{s\to 1} \ln \zeta^*(s)/\ln(s-1)^{-1} = 1$ vilket ger oss

vii)

$$d(\mathscr{P}(1;4)) = \frac{1}{2}$$

iix)

$$d(\mathscr{P}(3;4)) = \frac{1}{2}.$$

Det är två tal som är relativt prima till $m = 4$, nämligen 1 och 3, vilket ger att $\phi(4) = 2 \Rightarrow 1/\phi(4) = 1/2$ och alltså är

$$d(\mathscr{P}(n;4)) = \frac{1}{\phi(4)}$$

där $(n, 4) = 1$ och $n \in \mathbb{Z}$ och $\mathscr{P}(n;4)$ ges som tidigare av alla primtal p s.a. $p \equiv n \pmod 4$. Detta fullbordar beviset då $m = 4$.

För att kunna generalisera detta resonemang måste vi undersöka hur vi kan utvidga $\chi(n)$ och $L(\chi, s)$ så att beviset gäller för alla $m \in \mathbb{Z}$.

3.3. **Dirichletkaraktärer.** Vi börjar med att undersöka vilka problem vi stöter på när vi tittar på fallen $m = 6$ och $m = 5$ med tidigare definition av $\chi(n)$. Detta gör vi genom att titta på ett exempel.

Exempel 2. *För $m = 6$ är $\phi(6) = 2$, eftersom $1, 5$ är de enda relativt prima talen mellan 0 och 6. Alltså vill vi skapa de två aritmetiska följderna $1 + 6n$ och $5 + 6n$ för $n \in \mathbb{N}$.*

$\chi(n)$ där $n \in \mathbb{N}$ ges i detta fall av:

i) $\chi(n) = 0$ *om* $n = 0, 2, 3, 4 \pmod 6$.
ii) $\chi(n) = 1$ *om* $n = 1 \pmod 6$.
iii) $\chi(n) = -1$ *om* $n = 5 \pmod 6$.

Denna funktion genererar en sekvens $\chi(n)n$ bestående av

$$1, -5, 7, -11, 13, -17, \ldots$$

för alla $n \in \mathbb{N}$. Vi ser att de aritmetiska följderna $1 + 6\mathbb{N}$ och $5 + 6\mathbb{N}$ finns som termerna med udda respektive jämt ordningstal i följden $\chi(n)n$. För att kunna göra indelningen måste vi hitta en funktion som är symmetrisk motsatt $\chi(n)$ för n på jämn plats och lika för n på udda plats. Därför är det här lämpligt att använda ytterligare en funktion $\chi_1(n) = |\chi(n)|$ och använda samma metod som i Exempel 1 vilket ger

$$n\chi_1(n) + n\chi(n) = \begin{cases} 2n & \text{om } n \equiv 1 \pmod 6 \\ 0 & \text{om } n \not\equiv 1 \pmod 6 \end{cases}$$

$$n\chi_1(n) - n\chi(n) = \begin{cases} 2n & \text{om } n \equiv 5 \pmod 6 \\ 0 & \text{om } n \not\equiv 5 \pmod 6 \end{cases}$$

för alla $n \in \mathbb{N}$. $n(\chi_1(n) \pm \chi(n))/2$ returnerar n precis när $n \equiv 1 \pmod 6$ respektive då $n \equiv 5 \pmod 6$ vilket är analogt med Exempel 1.

I fallet då $m = p$ är ett primtal är $\phi(p) = p - 1$ eftersom $1, ..., p - 1$ är relativt prima p förutom 1 och p. Exempelvis för $m = 5$ är $\phi(5) = 4$. De relativt prima talen är $n = 1, 2, 3, 4$ och vi har alltså indelningen $1 + 5\mathbb{N}, 2 + 5\mathbb{N}, 3 + 5\mathbb{N}$ och $4 + 5\mathbb{N}$. Här är det därför lämpligt att ha fyra funktioner $\chi_i(n)$ där $i = 1, 2, 3, 4$. Tanken är här att som tidigare kombinera dessa för att få ut de sökta aritmetiska följderna. Problemet är här att det inte räcker med att endast addera och subtrahera om vi vill lyckas generera dessa följder. Här är det därför lämpligt att utvidga funktionerna med komplexa värden. Observera dock att tanken är att dela in i serier av tal vilket gör det lämpligt att $\chi(n)$ är periodisk och $|\chi(n)| = 1$ samt att antalet funktioner $\chi_i(n)$ $i = \phi(m)$. Vi måste definiera detta innan vi kan lösa fallet $m = 5$.

Vi vill att för våra funktioner $\chi(n) : \mathbb{Z} \to \mathbb{C}^*$ gäller att om

i) $(n, m) > 1$ är $\chi(n) = 0$.
ii) Om $(n, m) = 1$ är $\chi(n) = \chi(n + mk)$, för alla $k \in \mathbb{Z}$,

och att $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ är en homomorfism. Funktionen χ som definieras på detta sätt kallas *Dirichletkaraktär modulo m.* $(\mathbb{Z}/m\mathbb{Z})^*$ är modulusgruppen av alla restklasser som är relativt prima m. Följande tre påståenden gäller som ett resultat av definitionen

a) $\chi(n+m) = \chi(n)$
b) $\chi(kn) = \chi(k)\chi(n)$ där $k, n \in \mathbb{Z}$
c) $\chi(n) \neq 0$ omm $(n, m) = 1$.

a) och c) följer direkt från definitionen av Dirichletkarakärer.

Bevis. b) Om $(k, m) > 1$ eller $(n, m) > 1$ är enligt i) $\chi(kn) = \chi(k)\chi(n) = 0$ annars gäller att

$$\chi(kn) = [kn]_m = [k]_m[n]_m = \chi(k)\chi(n)$$

för alla $k, n \in \mathbb{Z}$ där $(k, m) = 1$ and $(n, m) = 1$. □

Observera att varje karaktär eller homomorfi $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}$ ger en Dirichletkaraktär $\tilde{\chi} : \mathbb{Z} \to \mathbb{C}^*$ genom

$$\tilde{\chi}(n) = \begin{cases} 0 & om\ (n, m) \neq 1 \\ \chi(n) & om\ (n, m) = 1 \end{cases}$$

Om χ , ψ är två karaktärer $A \to \mathbb{C}^*$ gäller att $(\chi\psi)(a) = \chi(a)\psi(a)$ där $a \in A$ också är en karaktär (mod m). Mängden av Dirichletkaraktärer är således sluten under multiplikation och vi kallar den $\hat{A}$. Vi definierar enhetselementet $\chi_0(a) = 1$ för alla $a \in A$ och inversen χ^{-1} ges då av $\chi^{-1}(a) = \chi(a)^{-1}$. Det är alltså en grupp. Om $a \in A$ har en ordning n gäller att $a^n = e$, så för en karaktär $\chi \in \hat{A}$ gäller

$$\chi(a)^n = \chi(a^n) = \chi(e) = 1.$$

Således blir värdena av en Dirichletkaraktär komplexa enhetsrötter, dvs. lösningar till ekvationen $z^n = 1, z \in \mathbb{C}^*$ och inversen är alltså det komplexa konjugatet $\chi^{-1} = \overline{\chi(a)} = \bar{\chi}(a)$.

Sats 5. *Om A är cyklisk och genereras av ett element g med ordningen n är* $A \cong \hat{A}$.

Bevis. Om $\chi \in \hat{A}$ har vi tidigare konstaterat att $x = \chi(g)$ är en lösning till ekvationen

$$x^n = 1 \Leftrightarrow x = (\zeta_n)^e$$

där $0 \leq e < n$ och $\zeta_n = e^{2\pi i/n}$ är en n:te enhetsrot. Men eftersom att $\chi(g^k) = \chi(g)^k$ gäller att χ är unikt bestämd av sitt värde på g. Omvänt utgår vi ifrån ett e s.a. $0 \leq e < n$ och definierar en karaktär χ_e s.a. $\chi_e(g) = \zeta_n^e$. Då g genererar hela gruppen för varje element g^k för $k = 0, 1, 2, ..., n-1$ har vi att

$$\chi_e(g)^r = (\zeta_n)^{r \cdot e}$$

och detta ger oss en Dirichletkaraktär. Alltså är mängden av Dirichletkaraktärer $\hat{A}$ precis χ_e, $e = 0, 1, ..., n-1$. Om vi listar dem får vi

$$\chi_0(g^r) = \chi_0(g^n) = 1$$
$$\chi_1(g^r) = (\zeta_n)^r$$
$$\chi_2(g^r) = (\zeta_n)^{2r}$$
$$\vdots$$
$$\chi_{n-1}(g^r) = (\zeta_n)^{(n-1)r}.$$

Utifrån listan ser vi tydligt att det finns n st Dirichletkaraktärer. Vidare är χ_1 en generator vilket innebär att

$$(\chi_1)^e(g^r) = \zeta_n^{er} = \chi_e(g^r)$$

för $r = 1, 2, ..., n-1$. Vi har hittat en generator vilket gör att $\hat{A} = 1, \chi_1, \chi_1^2, ..., \chi_1^{n-1}$ är cyklisk. Alla cykliska grupper med samma ordning är isomorfa. □

Exempel 3. *Nu när vi har definierat Dirichletkaraktärer kan vi göra indelningen för* $m = 5$ *med alla* $\chi : (\mathbb{Z}/5\mathbb{Z})^* \to \mathbb{C}$ *där* $(\mathbb{Z}/5\mathbb{Z})^* = \{1, 2, 3, 4\}$ *där antalet Dirichletkaraktärer är* $\phi(5) = 4$. *Gruppen* $(\mathbb{Z}/5\mathbb{Z})^*$ *är cyklisk med ordningen* $\phi(m)$. *Således gäller att för ett element* $g \in (\mathbb{Z}/5\mathbb{Z})^*$ *är* $\chi(g)^{\phi(m)} = \chi(g)^4 = 1$ *och alltså är* $\chi(g)$ *en lösning till ekvationen* $z^4 = 1$ *där* $z \in \mathbb{C}$. *En generator av* $(\mathbb{Z}/5\mathbb{Z})^*$ *är i detta fallet lätt att hitta eftersom* $2^4 \equiv 1 \pmod 5$. *Vi samlar våra lösningar i en tabell nedan där den andra kolumnen således definieras av*

$$\chi_j(2) = e^{2\pi ij/4} = e^{\pi ij/2}$$

för $j = 0, 1, 2, 3$ *på den* $j+1$*:te raden. För att fylla i den tredje kolumnen kan vi använda att* $\chi^{-1} = \bar{\chi}$

$$\chi_j(2) \cdot \chi_j(3) = 1 \Rightarrow \overline{\chi_j(2)} \cdot \chi_j(2) \cdot \chi_j(3) = \overline{\chi_j(2)} \Rightarrow$$

$$\chi_j(3) = \overline{\chi_j(2)} = e^{-\pi ij/2}.$$

Så vi ser att den tredje kolumnen är det komplexa konjugatet av den andra dvs. spegling i reella axeln. Den fjärde kolumnen fås lätt genom att inse

$$\chi_j(4) = \chi_j(2^2) = \chi_j(2)^2 = \left(e^{\pi ij/2}\right)^2 = e^{\pi ij} = (-1)^j.$$

n	*1*	*2*	*3*	*4*	*5*
$\chi_0(n)$	*1*	*1*	*1*	*1*	*0*
$\chi_1(n)$	*1*	*i*	*-i*	*-1*	*0*
$\chi_2(n)$	*1*	*-1*	*-1*	*1*	*0*
$\chi_3(n)$	*1*	*-i*	*i*	*-1*	*0*

Observera att vi här har utnyttjat att $A = (\mathbb{Z}/m\mathbb{Z})^*$ är cyklisk vilket inte alltid är fallet. Beroende på hur m väljs kommer strukturen på gruppen att variera. Här kommer vi inte göra stringenta bevis då detta skulle bli för omfattande utan titta på några exempel och resonera oss fram.

Exempel 4. *Då m=8 har vi* $\phi(8) = 4$ *relativt prima element då* $A := (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$. *Observera att kvadraten på varje element ger resten* 1 (mod 8) *dvs.*

$$3^2 \equiv 5^2 \equiv 7^2 \equiv 1$$

Alltså $\nexists g$ *s.a.* $g^4 \equiv 1 \pmod 8$ *och A är ej cyklisk.*

Exemplet visar att för $m = 8$ är $A = (\mathbb{Z}/m\mathbb{Z})^*$ inte cyklisk vilket gör att vår teori inte håller för generella värden på m. Vägen runt detta problem är att visa att det alltid går att hitta en isomorfism mellan A och en direkt produkt av cykliska grupper.

Exempel 5. *Om* $m = p \cdot q$ *är ett sammansatt tal, där* p, q *är primtal så gäller*

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

I vårt fall är vi endast intresserad av kongruenssklasser relativt prima m vilket ger den multiplikativa gruppen

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*.$$

Antalet element ges av

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1) = m(1-\frac{1}{p})(1-\frac{1}{q}) = p(1-\frac{1}{p})q(1-\frac{1}{q}).$$

Vi kan utvidga detta och säga att $(\mathbb{Z}/n\mathbb{Z})^*$ kan i likhet med alla ändliga abelska grupper skrivas som en produkt av cykliska grupper.[5]

Sats 6. *Antag att* $A \cong C_1 \times C_2 \times ... \times C_t$ *med ordning n är en direkt produkt av cykliska grupper* C_i *med ordning* n_i. *Då gäller att* $A \cong \hat{A}$.

Bevis. Om C_i är cykliska finns element $g_1, g_2, ..., g_t \in A$ där $< g_i >= C_i$ och då gäller att

i) varje element $a \in A$ kan uttryckas unikt som $a = g_1^{r_1} \cdot g_2^{r_2} \cdot ... \cdot g_t^{r_t}$ där $0 \leq r_i < n_i$ för alla i
ii) ordningen av g_i är n_i.

Om ordningen av A är n så är $n = n_i \cdot n_2 \cdot ... \cdot n_t$. Om $\chi \in \hat{A}$ är en karaktär gäller som tidigare att $\chi(g_i) = \zeta_{n_i}^{e_i}$ är unikt bestämd komplex n_i:te enhetslösning för $0 \leq e_i < n_i$.

Omvänt antar vi att $0 \leq e_i < n_i$ i en t-tupel $(e_1, e_2, ..., e_t)$ då kan vi definiera en karaktär χ genom

$$\chi(a) = \chi(g_1^{r_1} \cdot g_2^{r_2} \cdot ... \cdot g_t^{r_t}) = \chi(g_1)^{r_1}\chi(g_2)^{r_2} \cdot ... \cdot \chi(g_t)^{r_t} =$$
$$= (\zeta_{n_1}^{e_1})^{r_1} \cdot (\zeta_{n_2}^{e_2})^{r_2} \cdot ... \cdot (\zeta_{n_t}^{e_t})^{r_t}.$$

Det finns $n = n_1 \cdot n_2 \cdot ... \cdot n_t$ funktioner som kan definieras på detta sätt. Definiera nu χ_i som karaktären $\chi_i(a) = (\zeta_{n_i})^{r_1}$ för $a = g_1^{r_1}, ..., g_t^{r_t}$. Då är χ_i en generator till C_i med analogt resonemang som tidigare. Detta ger

[5]Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, 2nd ed. (1990) s. 254

att $\hat{A}$ är direktprodukten av cykliska delgrupper $C_i = <\chi_i>$. Alltså är $A \cong \hat{A}$.

□

Exempel 6. *Hitta alla Dirichletkaraktärer* (mod 15). *Eftersom* $m = 15 = 5 \cdot 3$ *finns en isomorfism*

$$(\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*.$$

Vi ska hitta våra två generatorer $g_1 \in (\mathbb{Z}/5\mathbb{Z})^*$, $g_2 \in (\mathbb{Z}/3\mathbb{Z})^*$ *där* $o(g_1) = \phi(5) = 4$ *och* $o(g_2) = \phi(3) = 2$ *så vi kan uttrycka varje element* $a = g_1^{r_1} g_2^{r_2}$. *Den första generatorn* $g_1 = 2$ *hittade vi redan i tidigare exempel och vi kan ta* $g_2 = 11$ *eftersom* $11^2 \equiv (-4)^2 \equiv 1 \pmod{15}$. *Observera att generatorerna inte är unika då t.ex.* $14^2 \equiv (-1)^2 \equiv 1$ *också är en generator till* $(\mathbb{Z}/3\mathbb{Z})^*$. *Dirichlet karaktärerna ges av*

$$\chi_{e_1,e_2}(a) = \chi_{e_1,e_2}(g_1^{r_1} g_2^{r_2}) = \chi_{r_1,r_2}(2^{r_1} \cdot 11^{r_2}) =$$

$$(\zeta_4^{e_1})^{r_1} (\zeta_2^{e_2})^{r_2} = (i^{e_1})^{r_1} ((-1)^{e_2})^{r_2} = i^{e_1 r_1} (-1)^{e_2 r_2}$$

där $0 \leq r_1, e_1 < 3$ *och* $0 \leq r_2, e_2 < 1$. *Om 2-tuppeln* (e_1, e_2) *genomlöper alla värden för* $e_1 = 0, 1, 2, 3$ *och* $e_2 = 0, 1$ *så kommer dessa motsvara alla Dirichletkaraktärer. T.ex. då* $2^2 \cdot 11^1 \equiv 4 \cdot (-4) \equiv 14 \pmod{15}$, *så ges sedan dirichletkaraktärerna av*

$$\chi_{e_1,e_2}(14) = i^{2e_1}(-1)^{e_2}.$$

Vi har samlat alla dessa lösningar i tabellen nedan.

a	*1*	*11*	*2*	*7*	*4*	*14*	*8*	*13*
(e_1, e_2)	*(0,0)*	*(0,1)*	*(1,0)*	*(1,1)*	*(2,0)*	*(2,1)*	*(3,0)*	*(3,1)*
$\chi_0 = \chi_{0,0}$	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
$\chi_1 = \chi_{0,1}$	*1*	*-1*	*1*	*-1*	*1*	*-1*	*1*	*-1*
$\chi_2 = \chi_{1,0}$	*1*	*1*	*i*	*i*	*-1*	*-1*	*-i*	*-i*
$\chi_3 = \chi_{1,1}$	*1*	*-1*	*i*	*-i*	*-1*	*1*	*-i*	*i*
$\chi_4 = \chi_{2,0}$	*1*	*1*	*-1*	*-1*	*1*	*1*	*-1*	*-1*
$\chi_5 = \chi_{2,1}$	*1*	*-1*	*-1*	*1*	*1*	*-1*	*-1*	*1*
$\chi_6 = \chi_{3,0}$	*1*	*1*	*-i*	*-i*	*-1*	*-1*	*i*	*i*
$\chi_7 = \chi_{3,1}$	*1*	*-1*	*-i*	*i*	*-1*	*1*	*i*	*-i*

Tittar man på tabellen ovan kan man se att de olika karaktärerna är ortogonala. Detta är den viktigaste egenskapen för karaktärerna för beviset av Dirichlets sats och dessa relationer bevisas nedan.

Proposition 7. *(Ortogonalitets relationerna för karaktärer) Låt* A *vara en abelsk grupp med elemenent* $a, b \in \mathbb{Z}$. $\chi, \psi \in \hat{A}$ *är dirichletkaraktärer.*

i)

$$\sum_{a \in A} \chi(a)\overline{\psi(a)} = \begin{cases} n & om\ \psi = \chi \\ 0 & om\ \psi \neq \chi. \end{cases}$$

ii)

$$\sum_{\chi\in\hat{A}}\chi(a)\overline{\chi(b)} = \begin{cases} n & om\ a = b \\ 0 & om\ a \neq b. \end{cases}$$

Bevis. i) Antag $\psi = \chi$. Då får vi

$$\sum_{a\in A}\chi(a)\chi^{-1}(a) = \sum_{a\in A}\left(\chi\cdot\chi^{-1}\right)(a) = \sum_{a\in A}\chi_0(a) = \sum_{a\in A}1 = n.$$

Antag $\psi \neq \chi \Rightarrow$

$$\sum_{a\in A}\chi(a)\overline{\psi(a)} = \sum_{a\in A}\left(\chi\cdot\psi^{-1}\right)(a).$$

Vi ser att det räcker med att visa att $\sum_{a\in A}\chi(a) = 0$ för en godtycklig karaktär $\chi \neq 1$, för då gäller det även för karaktären $\chi\cdot\psi^{-1}$ eftersom då måste hela summan bli noll. Det finns ett $b \in A$ s.a. $\chi(b) \neq 1$. Vi har då

$$\sum_{A}\chi(a) = \sum_{A}\chi(ab) = \chi(b)\sum_{a\in A}\chi(a) \ \Rightarrow\ (1-\chi(b))\sum_{a\in A}\chi(a) = 0.$$

Men eftersom vi antog

$$\chi(b) \neq 1 \ \Rightarrow\ (\chi(b)-1) \neq 0 \ \Rightarrow\ \sum_{a\in A}\chi(a) = 0.$$

ii) Antag $a = b$

$$\sum_{\chi\in\hat{A}}\chi(a)\overline{\chi(b)} = \sum_{\chi\in\hat{A}}\chi(a\cdot a^{-1}) = \sum_{\chi\in\hat{A}}\chi(1) = \sum_{\chi\in\hat{A}}1 = n.$$

Antag $a \neq b$

$$\sum_{\chi\in\hat{A}}\chi(a)\overline{\chi(b)} = \sum_{\chi\in\hat{A}}\chi(ab^{-1})$$

och det räcker med att visa att $\sum_{\chi\in\hat{A}}\chi(a) = 0$. Om $a = g_1^{m_1}g_2^{m_2}\cdot\ldots\cdot g_t^{m_t}$ där $m_i \neq 0$ för något i är $\chi_i(a) \neq 1$ eftersom

$$\chi_i(a) = \chi_i(g_i)^{m_i} = \zeta_{n_i}^{m_i} \neq 1.$$

Om vi sätter $\psi(a) = \chi_i(a)$ där $m_i \neq 0$ får vi

$$\sum_{\chi\in\hat{A}}\chi(a) = \sum_{\chi\in\hat{A}}\psi\chi(a) = \psi(a)\sum_{\chi\in\hat{A}}\chi(a) \ \Rightarrow\ (\psi(a)-1)\sum_{\chi\in\hat{A}}\chi(a) = 0.$$

Vi visste dock att

$$\psi(a) \neq 1 \ \Rightarrow\ (\psi(a)-1) \neq 0 \ \Rightarrow\ \sum_{\chi\in\hat{A}}\chi(a) = 0.$$

□

Proposition 8. *Låt χ, ψ vara Dirichletkaraktärer* (mod m) *och* $a, b \in \mathbb{Z}$.

$$i) \quad \sum_{a=0}^{m-1} \chi(a)\overline{\psi(a)} = \phi(m)\delta(\chi, \phi), \tag{10}$$

$$ii) \quad \sum_{\chi} \chi(a)\overline{\chi(a)} = \phi(m)\delta(a, b)$$

där summan i b) är över alla Dirichletkaraktärer (mod m) *samt* $\delta(a, b) = 1$ *om* $a \equiv b \pmod{m}$ *och* $\delta(a, b) = 0$ *om* $a \not\equiv b \pmod{m}$.

3.4. **Dirichlets L-funktion.** Om vi nu låter χ vara en Dirichlet karaktär kan vi definiera Dirichlets L-funktion analogt med specialfallet i (9) .

$$L(s, \chi) = \sum_{n}^{\infty} \chi(n)n^{-s} = \frac{\chi(1)}{1} + \frac{\chi(2)}{2^s} + \cdots . \tag{11}$$

På samma sätt som tidigare konvergerar denna funktion eftersom alla termer är dominerade av termerna från $\zeta(s)$,

$$\left|\chi(n)n^{-s}\right| \leq \left|n^{-s}\right| = n^{-s}.$$

Eftersom $L(s, \chi)$ är fullständigt multiplikativ kan vi använda samma grundteori som i specialfallet och vi har

$$L(s, \chi) = \prod_{p}(1 - \chi(p)p^{-s})^{-1}. \tag{12}$$

Observera dock att denna produkt innefattar endast de p som inte delar m eftersom $\chi(p) = 0$ om $p|m$. Detta gör att det är lätt att se ett samband mellan $L(s, \chi_0)$ och $\zeta(s)$ där χ_0 är enhetskaraktären.

$$L(s, \chi_0) = \prod_{p\nmid m}(1-p^{-s})^{-1} = \prod_{p|m}(1-p^{-s}) \prod_{p}(1-p^{-s})^{-1} = \prod_{p|m}(1-p^{-s})\zeta(s).$$

Observera att $L(s, \chi_0)$ är reell för alla $s > 1$ och $\ln L(s, \chi_0)$ är alltså väldefinierad. Om vi logaritmerar båda sidorna får vi

$$\ln L(s, \chi_0) = \sum_{p|m}(1 - p^{-s}) + \ln \zeta(s).$$

Om vi nu dividerar med $\ln(s-1)^{-1}$ och tar gränsövergång $s \to 1$ kommer vi fram till att

$$\lim_{s\to 1} \frac{\ln L(s, \chi_0)}{\ln(s-1)^{-1}} = \lim_{s\to 1} \left(\frac{\sum_{p|m}(1 - p^{-s})}{\ln(s-1)^{-1}} + \frac{\ln \zeta(s)}{\ln(s-1)^{-1}} \right).$$

Enligt (7a) och (5) är

$$\lim_{s\to 1} \frac{\ln L(s, \chi_0)}{\ln(s-1)^{-1}} = 1. \tag{13}$$

3.5. **Ett försök att bevisa Dirichlets Theorem.** För att nu generellt ge ett bevis av Dirichlets sats så är det precis som i specialfallet lämpligt att studera $\ln L(s,\chi)$. Problemet i detta fall är att $L(s,\chi)$ är en funktion som antar komplexa värden vilket ger flertydiga värden på logaritmen vilket illustreras i ett exempel.

Exempel 7. *Låt $z = re^{i\theta}$ vara ett komplext tal s.a. $z \in \mathbb{C}^*$. Logaritmen $\ln z$ borde ges av*

$$\ln z = \ln(re^{i\theta}) = \ln r + i\theta.$$

Vi jämför värdet av $\ln(z)$ för två punkter med en period 2π och fixt r. För ett komplext tal gäller

$$z = r = re^{i2\pi}.$$

Logaritmering ger

$$\ln z = \ln r = \ln r + 2\pi i$$

vilket är omöjligt eftersom vi får olika värden på $\ln(z)$ för samma komplexa tal z. Således är $\ln(z)$ inte en väldefinierad funktion.

I praktiken visar detta exempel oss att $\ln L(s,\chi)$ inte blir en väldefinierad funktion om vi använder samma metod som innan. Ett sätt att komma runt detta är att uttrycka $\ln L(s,\chi)$ som en oändlig serie. Vi gör detta genom att använda resultat från (3b) men denna gång med komplexa värden istället för reella. Vi har tidigare kommit fram till att

$$\sum_{k=1}^{\infty} k^{-1}z^k = \ln(1-z)^{-1}$$

för alla $|z| < 1$. En omskrivning ger

$$(1-z)^{-1} = \exp\left(\sum_{k=1}^{\infty} k^{-1}z^k\right).$$

Genom att substituera $z = \chi(p)p^{-s}$ ser vi att vi har uttryckt termerna i (12) som en oändlig serie,

$$(1-\chi(p)p^{-s})^{-1} = \exp\left(\sum_{k=1}^{\infty} k^{-1}\chi(p^k)p^{-ks}\right),$$

där $|\chi(p)p^{-s}| < 1$ vilket är giltigt för $s > 1$. Nu är vi i stånd att definiera en funktion

$$G(s,\chi) = \sum_{p}\sum_{k=1} k^{-1}\chi(p^k)p^{-ks} \tag{14}$$

där $\exp G(s,\chi) = L(s,\chi)$ och χ är en Dirichletkaraktär. Denna serie konvergerar eftersom dess termer $\left|k^{-1}\chi(p^k)p^{-ks}\right| \leq p^{-ks}$ och $\sum_{k=1}^{\infty} p^{-ks}$ konvergerar för $s > 1$. Då Riemanns zetafunktion är kontinuerlig för

$s > 1$ gäller detsamma för $G(s,\chi)$. Nu använder vi (14) och använder samma resonemang som i (6) och får

$$G(s,\chi) = \sum_p \chi(p)p^{-s} + R_\chi(s)$$

där $R_\chi(s)$ är en begränsad funktion när $s \to 1$. För att kunna använda oss av ortogonalitets relationerna multiplicerar vi med $\overline{\chi(a)}$ där $a \in \mathbb{Z}$ är relativt prima m och summerar över alla Dirichletkaraktärer (mod m) vilket ger

$$\sum_\chi \overline{\chi(a)}G(s,\chi) = \sum_p p^{-s} \sum_\chi \overline{\chi(a)}\chi(p) + \sum_\chi \overline{\chi(a)}R_\chi(s).$$

Enligt (14b) gäller att

$$\sum_\chi \overline{\chi(a)}\chi(p) = \begin{cases} 0 & \text{om } p \not\equiv a\,(m) \\ \phi(m) & \text{om } p \equiv a\,(m). \end{cases}$$

Om vi använder detta resultat får vi

$$\sum_\chi \overline{\chi(a)}G(s,\chi) = \phi(m) \sum_{p\equiv a\,(m)} p^{-s} + \sum_\chi \overline{\chi(a)}R_\chi(s).$$

Vi sätter $R_{\chi,a}(s) = \sum_\chi \overline{\chi(a)}R_\chi(s)$ som är en begränsad funktion eftersom $\sum_\chi \overline{\chi(a)}$ är begränsad. För att tillämpa Dirichletdensitet dividerar vi båda leden med $\ln(s-1)^{-1}$,

$$\sum_\chi \overline{\chi(a)}\frac{G(s,\chi)}{\ln(s-1)^{-1}} = \phi(m)\frac{\sum_{p\equiv a\,(m)} p^{-s}}{\ln(s-1)^{-1}} + \frac{R_{\chi,a}(s)}{\ln(s-1)^{-1}}.$$

Om vi nu låter $s \to 1$ så får vi enligt (7)

$$\lim_{s\to 1} \sum_\chi \overline{\chi(a)}\frac{G(s,\chi)}{\ln(s-1)^{-1}} = \phi(m)d(\mathscr{P}(a;m)).$$

Den första termen i summan av alla Dirichletkaraktärer i vänster led är

$$\lim_{s\to 1} \frac{G(s,\chi_0)}{\ln(s-1)^{-1}} = 1$$

enligt (13). Om vi använder detta resultat och löser ut $d(\mathscr{P}(a;m))$ får vi

$$d(\mathscr{P}(a;m)) = \frac{1}{\phi(m)} \cdot (1 + \epsilon(s,\chi))$$

där

$$\epsilon(s,\chi) = \lim_{s\to 1} \sum_{r=2}^{\phi(m)} \overline{\chi_r(a)}\frac{G(s,\chi_r)}{\ln(s-1)^{-1}}.$$

Vi konstaterar att om vi lyckas visa att $\epsilon = 0$ har vi visat (8) och är färdiga med beviset för Dirichlets sats. Vi ser att $\epsilon = 0$ om $G(s,\chi_r)$ är

begränsad för varje χ_r, $r = 2, 3, \ldots, \phi(m)$ då $s \to 1$. För att visa detta är det lämpligt att göra en analytisk utvidgning till $s > 0$.

3.6. **Analytisk utvidgning till s > 0.** Vårat mål med denna sektion är att visa att $G(s, \chi)$ är begränsad för varje icketrivial Dirichletkaraktär då $s \to 1$. Vi kommer visa att det finns en analytisk fortsättning på Riemanns zetafunktion och Dirichlets L-funktion för $s > 0$. Det viktiga i denna sektion är dock att visa att dessa funktioner är nollställesfria i en liten omgivning till polen $s = 1$ och i slutet av denna sektion visar vi att $L(1, \chi) \neq 0$.

Vi definierar s som en komplex variabel med $s = \sigma + it$ för $\sigma, t \in \mathbb{R}$. För att Riemanns zetafunktion och L-funktionen ska fortsätta att vara väldefinierade måste restriktionen $\mathrm{Re}(s) > 1$ göras så att summorna konvergerar. Inledningsvis vill vi utvidga Riemann-Zeta funktionen till en analytisk funktion för komplexa s. För att göra detta behöver vi använda oss av Abels lemma för partiell summation.

Lemma 2. *(Partiell Summation) Antag att $\{a_n\}$ och $\{b_n\}$ för $n = 1, 2, 3, \ldots$ är sekvenser av komplexa tal s.a. $\sum_{n=1}^{\infty} a_n b_n$ är en konvergent summa. Låt $A_n = \sum_{k=1}^{n} a_k$ och antag att $A_n b_n \to 0$ då $n \to \infty$ då gäller*

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=1}^{\infty} A_n (b_n - b_{n+1}). \tag{15}$$

Bevis. Sätt $s_N = \sum_{n=1}^{N} a_n b_n$. (15) kan visas gälla genom att lägga till och dra ifrån termer av a_n för att sedan omfördela dem på lämpligt sätt. Vi har att

$$A_n - A_{n-1} = \sum_{k=1}^{n} a_k - \sum_{k=1}^{n-1} a_k = a_n$$

där alla termer tar ut varandra förutom den sista. Därför kan vi skriva om s_N som

$$s_N = \sum_{n=1}^{N} a_n b_n = \sum_{n=1}^{N} (A_n - A_{n-1}) b_n.$$

Nu kan vi skriva om det högra ledet till två summor och ändra indexeringen.

$$s_N = \sum_{n=1}^{N} A_n b_n - \sum_{n=1}^{N} A_{n-1} b_n = a_N b_N + \sum_{n=1}^{N-1} A_n b_n - \sum_{n=1}^{N} A_{n-1} b_n.$$

Den andra summan ovan kan vi slänga ut den första termen och ändra indexeringen $\sum_{n=1}^{N} A_{n-1} b_n = A_0 b_1 + \sum_{n=1}^{N-1} A_n b_{n+1}$. Om vi sätter $A_0 = 0$ kan vi bryta ut A_n

$$s_N = a_N b_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1}).$$

Genom att låta $N \to \infty$ får vi

$$\lim_{N\to\infty} s_N = \sum_{n=1}^{\infty} A_n(b_n - b_{n+1})$$

då $a_N b_N \to 0$. Således är (15) bevisad. □

Nu är vi i stånd till att utvidga Riemanns zetafunktion för komplexa värden på s med restriktionen $\mathrm{Re}(s) > 1$.

Proposition 9. *$\zeta(s) - (s-1)^{-1}$ har en väldefinierad analytisk fortsättning på området $\{s \in \mathbb{C} | \sigma > 0\}$*

Bevis. Genom att använda (15) där med $a_n = 1$ och $b_n = n^{-s}$ kan vi skriva om Riemann-Zeta funktionen som

$$\zeta(s) = \sum_{n=1}^{\infty} 1 \cdot n^{-s} = \sum_{n=1}^{\infty}(\sum_{k=1}^{n} 1)(n^{-s} - (n+1)^{-s}) = \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}).$$

Om vi integrerar en funktion $f(x) = sx^{-s}$ på ett litet intervall dx där vi låter $n \leq x \leq n+1$ ser vi att

$$\int_n^{n+1} sx^{-s-1}dx = \left[-x^{-s}\right]_n^{n+1} = n^{-s} - (n+1)^{-s}.$$

Således kan vi skriva om Riemann-zeta funktionen som

$$\zeta(s) = s\sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1}dx$$

där $n \leq x \leq n+1$. Om x är ett reellt tal kan vi skriva $[x]$ som det största heltal mindre eller lika med x och $< x >= x - [x]$ är den resterande delen. I vårat fall är $[x] = n$ då $n \leq x \leq n+1$.

$$\zeta(s) = s\sum_{n=1}^{\infty} \int_n^{n+1} [x]x^{-s-1}dx = s\int_1^{\infty} [x]x^{-s-1}dx =$$

$$s\int_1^{\infty} x^{-s}dx - s\int_1^{\infty} < x > x^{-s-1}dx$$

där vi har adderat ihop alla integreringsintervall i den andra likheten och använt att $[x] = x - < x >$ i den tredje. Vi har tidigare visat (i beviset av (4)) att värdet av första integralen i högerled är

$$\int_1^{\infty} x^{-s}dx = (s-1)^{-1}.$$

Således kan vi skriva

$$\zeta(s) = s(s-1)^{-1} - s\int_1^{\infty} < x > x^{-s-1}dx$$

där $< x > \leq 1$ gör att integralen konvergerar för alla komplexa s med $\mathrm{Re}(s) > 0$. Avslutningsvis konstaterar vi att högerledet i likheten

$$\zeta(s) - (s-1)^{-1} = 1 - s\int_1^{\infty} < x > x^{-s-1}dx,$$

är en analytisk funktion för $\mathrm{Re}(s+1) > 1$ och alltså är en analytisk utvidgning definierad i området $\{s \in \mathbb{C} | \sigma > 0\}$. Propositionen är således visad. □

Innan vi kan fortsätta att visa att även Dirichlets L-funktion kan utvidgas för $\mathrm{Re}(s) > 0$ med analogt resonemang formulerar vi ett lemma som visar att beloppet av summan av ett ändligt antal värden av en Dirichletkaraktär är begränsad.

Lemma 3. *Låt χ vara en icketrivial Dirichlet karaktär mod m. För alla $N > 0$ har vi att*

$$\left| \sum_{n=0}^{N} \chi(n) \right| \leq \phi(m). \tag{16}$$

Bevis. Vi kan skriva $N = qm + r$ där $0 \leq r < q$. Eftersom $\chi(n)$ är komplexa m-te enhetslösningar kan vi istället för att summera över N, summera över q hela cykler och lägga till de resterande r termerna. Från ortogonalitetsrelationerna vet vi att summan av en hel cykel alltid är noll, dvs.

$$\sum_{n=0}^{m-1} \chi(n) = 0$$

vilket gör att det räcker med att begränsa resttermen när vi studerar beloppet $|\chi(n)|$.

$$\sum_{n=0}^{N} \chi(n) = q \left(\sum_{n=0}^{m-1} \chi(n) \right) + \sum_{n=0}^{r} \chi(n) = \sum_{n=0}^{r} \chi(n).$$

Detta ger oss att beloppet av summan blir

$$\left| \sum_{n=0}^{N} \chi(n) \right| = \left| \sum_{n=0}^{r} \chi(n) \right| \leq \sum_{n=0}^{m-1} |\chi(n)| = \phi(m)$$

där olikheten beror på triangelolikheten för komplexa tal samt att $r \leq m - 1$. □

Med detta lemma kan vi nu visa att även $L(s, \chi)$ kan utvidgas analytiskt för $s > 0$.

Proposition 10. *Låt χ vara en icketrivial Dirichletkaraktär mod m. $L(s, \chi)$ kan då utvidgas till en analytisk funktion i området $\{s \in \mathbb{C} | Re(s) > 0\}$.*

Bevis. Detta bevis görs på samma sätt som utvidgningen på Riemanns zetafunktion till $\mathrm{Re}(s) > 0$. Sätt $S(x) = \sum_{n \leq x} \chi(n)$ som är summan av alla Dirichletkaraktärer upp till ett tal $x \in \mathbb{R}$. Från (11) ser vi att vi kan använda (15) med $a_n = \chi(n)$ och $b_n = n^{-s}$ vilket ger

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \sum_{n=1}^{\infty} S(n)(n^{-s} - (n+1)^{-s})$$

där $n \leq x \leq n+1$. Som tidigare kan vi för varje n uttrycka $n^{-s} - (n+1)^{-s}$ som en integral,

$$\sum_{n=1}^{\infty} S(n)(n^{-s} - (n+1)^{-s}) = s\sum_{n=1}^{\infty} S(n) \int_n^{n+1} x^{-s-1}dx.$$

Eftersom $n \leq x \leq n+1$ gäller att

$$s\sum_{n=1}^{\infty} S(n) \int_n^{n+1} x^{-s-1}dx = s\sum_{n=1}^{\infty} \int_n^{n+1} S(x)x^{-s-1}dx = s\int_1^{\infty} S(x)x^{-s-1}dx.$$

Enligt (16) vet vi att $S(x) \leq \phi(m)$ vilket ger att

$$L(s,\chi) = s\int_1^{\infty} S(x)x^{-s-1}dx$$

konvergerar för alla s med $\mathrm{Re}(s) > 0$ vilket fullbordar beviset. □

Proposition 11. *Låt $F(s) = \prod_\chi L(s,\chi)$ där produkten tas över alla Dirichletkaraktärer modulo m. Då gäller att om s är reellt och $s > 1$ är $F(s) > 1$*

Bevis. Enligt (14) gäller att $G(s,\chi(s))$ ges av de oändliga serierna

$$G(s,\chi(s)) = \sum_p \sum_{k=1}^{\infty} \frac{1}{k}\chi(p^k)p^{-ks}.$$

Om vi summerar $G(s,\chi)$ över alla Dirichletkaraktärer så vet vi från ortogonalitetsrelationerna (8a) att alla termer försvinner förutom de som uppfyller att $p^k \equiv 1\ (m)$ där $\sum_{p^k \equiv 1\ (m)} \chi(p^k) = \phi(m)$. Detta ger

$$\sum_\chi G(s,\chi) = \sum_p \sum_{k=1}^{\infty} \frac{1}{k}p^{-ks}\left(\sum_\chi \chi(p^k)\right) = \phi(m) \sum_{p^k \equiv 1\ (m)} \frac{1}{k}p^{-ks}$$

där den sista summan är över alla tal $p \in \mathscr{P}, k \in \mathbb{N}$ s.a. $p^k \equiv 1\ (m)$. Vi ser att denna summa är uppenbart positiv och alltså är $\sum_\chi G(s,\chi) \geq 0$. Om tar exponentialen av båda sidorna kommer vi fram till resultatet

$$\exp(\sum_\chi G(s,\chi)) = \prod_\chi \exp(G(s,\chi)) = \prod_\chi L(s,\chi) \geq 1,$$

där första likheten ges av räknelagen för exponentialer och den andra av definitionen $\exp(G(s,\chi)) = L(s,\chi)$. Således är $F(s) \geq 1$ och beviset fullbordat. □

För att underlätta delas beviset av $L(1,\chi) \neq 0$ upp i två delar: när χ antar komplexa värden samt när χ är reell dvs. då $\chi = 0, \pm 1$. Vi börjar nedan med att visa detta då χ är en icketrivial komplex karaktär mod m.

Proposition 12. *Om χ är en icketrival komplex karaktär mod m gäller $L(1,\chi) \neq 0$.*

Bevis. Antag motsatsen: att $L(1,\chi) = 0$ om χ är komplex och s reell, $s > 1$. Då χ är komplex följer det att det komplexa konjugatet $L(s,\chi) = L(s,\bar{\chi})$ är också noll då $s = 1$. Om vi nu studerar $F(s) = \prod_\chi L(s,\chi)$ vet vi att $L(s,\chi_0) = \zeta(s)$ har en simpel pol i $s = 1$ enligt (4) och de andra faktorerna är analytiska. Således måste $F(1) = 0$. Detta är en motsägelse mot proposition 11 vilket innebär att $L(1,\chi) \neq 0$. □

Nu har vi fallet kvar att visa $L(1,\chi) \neq 0$ där χ är reell, dvs. antar värdena $0, 1, -1$. För att visa detta behöver vi ytterligare ett lemma.

Lemma 4. *Låt f vara en ickenegativ funktion som uppfyller $f(nm) = f(n)f(m)$ för $(n,m) = 1, n, m \in \mathbb{Z}^+$. Antag att varje primtalspotens $p^k < c$ är begränsad för en konstant c. Då gäller att för reella $s > 1$ konvergerar $\sum_{n=1}^{\infty} f(n)n^{-s}$ där*

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k)p^{-ks}\right). \tag{17}$$

Bevis. Antag $s > 1$ och sätt $a(p) = \sum_{k=1}^{\infty} f(p^k)p^{-ks}$. För att visa att $\sum_{n=1}^{\infty} f(n)n^{-s}$ konvergerar räcker det med att visa att $\prod_{p\leq N}(1 + a(p))$ är begränsad för $N \to \infty$. Detta eftersom $\sum_{n=1}^{\infty} f(n)n^{-s} < \prod_{p\leq N}(1 + a(p))$ pga. de multiplikativa egenskaperna f har samt att $f > 0$ vilket gör att denna summa är inspärrad och konvergerar således. För $a(p)$ gäller det att

$$a(p) = \sum_{k=1}^{\infty} f(p^k)p^{-ks} < c\sum_{k=1}^{\infty} p^{-ks} = cp^{-s}\sum_{k=0}^{\infty} p^{-ks}$$

där vi har först använt $p^k < c$ och sedan ändrat indexeringen i summan. Eftersom $s > 1$ kan vi använda (3a)

$$cp^{-s}\sum_{k=0}^{\infty} p^{-ks} = cp^{-s}(1 - p^{-s})^{-1} < 2cp^{-s}$$

där olikheten förklaras med $(1 - p^{-s})^{-1} \approx 2$ då $p_1 = 2$ och $s \approx 1$ i den största (första) termen. Således har vi $a(p) < 2cp^{-s}$ för alla primtal p. Om vi multiplicerar över alla $p \leq N$ får vi

i)

$$\prod_{p\leq N} a(p) < 2c\prod_p p^{-s} = M$$

vilket innebär att vi har hittat en begränsning för $a(p)$. Vidare gäller för $x > 0$ att

$$1 + x < \exp x$$

eftersom exponentialfunktioner växer snabbare än linjära funktioner för värden större än 1. Om vi använder $x = a(p)$ och multiplicerar över

alla $p \leq N$ får vi

$$\prod_{p\leq N}(1+a(p)) < \prod_{p\leq N}(\exp a(p)) = \exp \sum_{p\leq N} a(p) < \exp M$$

där likheten ges av räkneregler för potenser och den sista likheten ifrån i). Således har vi att även $\sum_{n\leq N} < \exp M$ för alla N. Eftersom f från antagande är ickenegativ följer att

$$\sum_{n=1}^{\infty} f(n)n^{-s}$$

konvergerar. Att uttrycket i (17) gäller visas sedan på samma sätt som i beviset av (2). □

Nu är vi i stånd att visa $L(s,\chi) \neq 0$ för reella karaktärer χ.

Proposition 13. *Låt χ vara en icketrivial Dirichletkaraktär mod m. Då gäller $L(1,\chi) \neq 0$.*

Bevis. Vi visar detta med hjälp av motsägelse. Antag att $L(1,\chi) = 0$ och studera funktionen

$$\psi(s) = \frac{L(s,\chi)L(s,\chi_0)}{L(2s,\chi_0)}.$$

Vi vet från tidigare att $L(s,\chi_0)$ har en simpel pol i $s = 1$ men eftersom $L(s,\chi) = 0$ hävs denna pol och således är täljaren i $\psi(s)$ analytisk på hela $\mathrm{Re}(s) > 0$. Nämnaren har en pol i $2s = 1 \Rightarrow s = 1/2$ vilket innebär att $\psi(s) \to 0$ då $s \to 1/2$. Nämnaren är alltså analytisk för $\mathrm{Re}(s) > 1/2$ vilket således innebär att $\psi(s)$ är analytisk för alla $\mathrm{Re}(s) > 1/2$. Om vi nu antar tillfälligt att s är reell för $s > 1$ kan vi med (12) skriva om $\psi(s)$ som

$$\psi(s) = \prod_p (1-\chi(p)p^{-s})^{-1}(1-\chi_0(p)p^{-s})^{-1}(1-\chi_0(p)p^{-2s}).$$

Vi har tidigare konstaterat att denna produkt endast gäller för alla primtal som inte delar m eftersom dessa termer blir noll. Insatt $\chi_0 = 1$ och över alla $p \nmid m$ vilket ger

$$\psi(s) = \prod_{p\nmid m} \frac{(1-p^{-2s})}{(1-p^{-s})(1-\chi(p)p^{-s})}.$$

Eftersom $p \nmid m$ så vet vi att $\chi(p) = \pm 1$. Om $\chi(p) = -1$ ser vi att

$$\psi(s) = \prod_{\chi(p)=-1} \frac{(1-p^{-2s})}{(1-p^{-s})(1+p^{-s})} = 1.$$

När $\chi(p) = 1$ får vi

$$\psi(s) = \prod_{\chi(p)=1} \frac{(1-p^{-s})(1+p^{-s})}{(1-p^{-s})(1-p^{-s})} = \prod_{\chi(p)=1} \frac{1+p^{-s}}{1-p^{-s}}.$$

Om vi studerar denna faktorkvot kan vi skriva om den som

$$\frac{1+p^{-s}}{1-p^{-s}} = (1+p^{-s})\sum_{k=0}^{\infty} p^{-ks} = \sum_{k=0}^{\infty} p^{-ks} + \sum_{k=0}^{\infty} p^{-(k+1)s} =$$

$$= 1 + \sum_{k=1}^{\infty} p^{-ks} + \sum_{k=1}^{\infty} p^{-ks} = 1 + 2\sum_{k=1}^{\infty} p^{-ks}$$

där (3a) ger den första likheten. Nu kan vi skriva $\psi(s)$ som

$$\psi(s) = \prod_{\chi(p)=1} \left(1 + 2\sum_{k=1}^{\infty} p^{-ks}\right)$$

där $s > 1$ och s är reell. Anledningen till denna omskrivning är att nu kan vi använda (17) från tidigare lemma. Detta vill säga att vi kan skriva $\psi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ som är konvergent för $s > 1$ och där $a_n \geq 0$. Observera att $a_1 = 1$. Om vi nu låter s anta komplexa värden kan vi göra en potensutveckling kring $s = 2$ med hjälp av Taylorutveckling. Detta ger oss

$$\psi(s) = \sum_{m=0}^{\infty} \frac{\psi^{(m)}(2)}{m!}(s-2)^m$$

där $\psi^{(m)}(2)$ är m:te derivatan av ψ. Derivatan beräknas enkelt genom omskrivningen $\psi(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} a_n e^{(-\ln n)s}$,

$$\psi^{(m)}(2) = \sum_{n=1}^{\infty} a_n (-1)^m (\ln n)^m n^{-2} = (-1)^m c_m,$$

där $c_n \geq 0$. Om vi nu kombinerar dessa får vi

$$\psi(s) = \sum_{m=0}^{\infty} \frac{c_m}{m!}(2-s)^m$$

där $c_0 = \phi(2) = \sum_{n=1}^{\infty} a_n n^{-2} > a_1 = 1$. Eftersom $\psi(s)$ växer för avtagande värden på s kommer $\psi(s) \geq 1$ då $s \in (1/2, 2)$. Detta är en motsägelse eftersom $\psi(s) \to 0$ då $s \to 1/2$. Alltså måste $L(1,\chi) \neq 1$. □

Vi kan nu bevisa att $G(s,\chi_r)$ är begränsad för varje icketrivial dirichletkaraktär χ_r, $r = 2, 3, ..., \phi(m)$ då $s \to 1$ för reella $s > 1$. Eftersom $L(1,\chi_r) \neq 0$ existerar det en disk D runt $L(1,\chi_r)$ s.a. $0 \notin D$. Låt $\ln z$ vara gren av logaritmen på D som är kontinuerlig och ger entydiga värden[6]. Det finns ett $\delta > 0$ så att $L(s,\chi_r) \in D$ för $s \in (1, 1+d)$. Exponentialen av både $G(s,\chi_r)$ och $\ln L(s,\chi_r)$ är $L(s,\chi_r)$ vilket innebär att det finns ett tal N så att

$$G(s,\chi_r) = 2\pi i N + \ln L(s,\chi_r)$$

[6]E.B. Saff, A.D. Snider, Fundamentals of Complex Analysis, 3rd ed., Pearsson Education(2003), s. 122

för $s \in (1, 1+d)$. Detta medför att $\lim_{s\to 1} G(s,\chi_r) = 2\pi iN + \ln L(s,\chi_r)$ existerar. Eftersom $G(s,\chi_r)$ har ett gränsvärde då $s \to 1$ är den begränsad. Vi har alltså visat att $G(s,\chi)$ är begränsade för alla dirichletkaraktärer och alltså visat (8) som är Dirichlets theorem för aritmetisk progression.

4. Bunyakowskis hypotes och primtal i kvadratiska polynom

I denna avslutande sektion kommer vi att visa att Dirichlets sats för aritmetiska följder är endast ett specialfall av en större hypotes. Här kommer vi att studera hur primtal fördelar sig över ickelinjära polynom. Viktor Bunyakowsky var en rysk matematiker som 1857 gav en hypotes om att polynom genererar oändligt antal primtal för positiva heltal under vissa omständigheter.

Hypotes 1. *(Bunyakowsky) Låt $f(x)$ vara polynom av en variabel med $grad(f(x)) = k > 0$ på formen*

$$f(x) = \sum_{i=0}^{k} a_{k-i}x^{k-i} = a_k x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0$$

för koefficenter $a_i \in \mathbb{Z}$ för alla i. Då gäller att $f(n)$ antar oändligt antal primtalsvärden för $n \in \mathbb{Z}^+$ om följande tre påståenden gäller:

i) $a_k > 0$.
ii) $f(x)$ *är irreducibelt över* $\mathbb{Z}$.
iii) $\text{sgd}\{f(n) : \forall n \geq 1, n \in \mathbb{Z}^+\} = 1$.

i) är det svagaste antagandet eftersom det endast reglerar ett teckenproblem. Om $a_k < 0$ kommer $f(x) < 0$ för stora x vilket gör att $f(n)$ har inte har primtalsvärden för stora heltal n. Men om vi tillåter primtal på formen $-p$ så kan i) försummas.

ii) Anta att $f(x)$ är reducibelt över $\mathbb{Z}$ och kan då faktoriseras enligt faktorsatsen som

$$f(x) = g(x)h(x).$$

Men för heltalskoefficenter har vi därför att $h(n) \mid f(n)$ och $g(n) \mid f(n) \Rightarrow f(n)$ ger endast primtalsvärde om $g(n), h(n) = \pm 1$. Detta kommer endast att inträffa ett ändligt antal gånger så för stora n är $f(n)$ sammansatt och genererar sammantaget endast ett ändligt antal primtal.

iii) Detta är detsamma som att säga att för alla heltalsvärden på n har $f(1), f(2), f(3), ...$ inte några gemensamma delare. Om vi antar att $\text{sgd}\{f(n) : n \geq 1\} = \alpha > 1$ så gäller för varje heltal n att $\alpha \mid f(n)$. Detta innebär att $f(n)$ genererar max ett primtal. Observera att iii) inte är detsamma som att alla koefficenter a_i är relativt prima vilket vi illustrerar i ett exempel.

Exempel 8. *Polynomet* $f(x) = x^2 - x + 2$ *har relativt prima koefficenter. Men vi ser att* $f(2m) = 2(2m^2 - m + 1)$ *samt* $f(2m+1) = 2(2m^2 + m + 1)$ *alltså är* $\text{sgd}(f(n)) = 2$ *för alla* $n \geq 1$. *Detta innebär att* $f(n), n \in \mathbb{N}$ *har endast ett primtal då* $f(1) = 2$ *men då* $n > 1$ *är polynomet alltid delbart med* 2.

Om vi nu tittar på Bunyakowskis hypotes för $k = 1$ så reduceras problemet till att för ett polynom $f(x) = mx + a$ antar $f(n)$ oändligt antal primtalsvärden för positiva n om $(m, a) = 1$. Detta är Dirichlets sats vilket innebär att vi har bevisat fallet $k = 1$ av hypotesen eftersom vi har visat (8). För $k \geq 2$ finns numeriska beräkningar för många specialfall som tyder på att hypotesen är sann men något allmänt bevis finns inte. Med största sannolikhet kommer hypotesen inte bevisas inom en snar framtid, då ingen ens har lyckats bevisa den för $k = 2$. Anledningen till att det är betydligt lättare att bevisa det linjära fallet beror på att primtalen ligger jämt distribuerade över de relativt prima aritmetiska följderna. Som vi tidigare har sett går det således att på ett förhållandevis enkelt sätt dela in och extrahera termer. För att få större förståelse av när kvadratiska funktioner ger primtalslösningar och hur de distribueras kan vi titta på ett exempel.

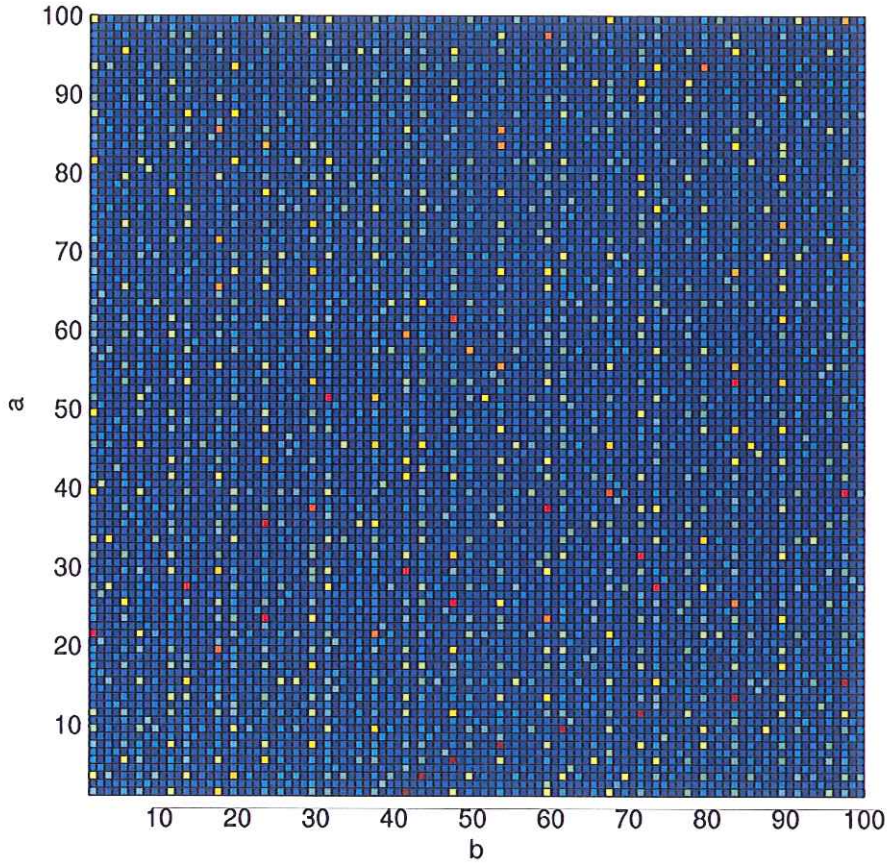
Exempel 9. *Om vi låter den ledande* x^2*-termen vara* 1 *så har vi ett polynom med två varierande parametrar* $f(x) = x^2 + ax + b$ *där vi är intresserade av* $f(n)$, $n \in \mathbb{Z}^+$, *som ger primtalslösningar. Vi plottar detta i en graf där vi låter* $1 \leq a, b \leq 100$ *för* n *upp till* $N = 100$ *där vi utgår från polynom med Bunyakowskiegenskaper dvs. är irreducibla och har inga gemensamma delare. Vi observerar från Figur 6 att vissa polynom genererar ovanligt stora mängder primtal såsom t.ex.* $x^2 + x + 41$ *som ger hela 86 primtalslösningar på de 100 första! Detta polynom är välkänt och studerades av Euler. Tabellen nedan visar de polynomen som ger flest primtalsvärden för koefficenterna* $0 < a, b \leq 100$ *för* $n \leq 100$

a	b	# *primtal*
1	41	86
3	43	86
5	47	85
7	53	85
9	61	84
11	71	84
13	83	84
15	97	84

Kvadratkomplettering ger

$$x^2 + ax + b = 0 \Rightarrow \left(x + \frac{a}{2}\right)^2 = \frac{a^2 - 4b}{2^2} \Rightarrow x = \frac{-a \pm \sqrt{\Delta}}{2}$$

där $\Delta = a^2 - 4b$ *är diskriminanten. Om* Δ *kan uttryckas som en kvadrat kan* $f(n)$ *faktoriseras över heltalen och är därför reducibelt. T.ex. om*



FIGUR 6. Grafen visar antalet primtal i de kvadratiska polynomen $f(x) = x^2 + ax + b$ för alla heltal $n \leq 100$ där $1 \leq a, b \leq 100$ är heltal. Primtalsdensitet i färger: röd(högst),orange,gul,ljusblå, mörkblå(minst).

vi antar att $a = 2m + 1$ *och* $b = 2m$

$$\Delta = (2m+1)^2 - 4(2m) = (2m-1)^2 = A^2.$$

Det finns 50 *udda och* 50 *jämna koefficenter för* $a, b \leq 100$ *vilket innebär att polynom med dessa* $50^2 = 1500$ *koefficenter kommer ej ge några primtalslösningar (se figur 6). Totalt finns det finns det* 1626 *reducibla*

polynom av 10000 *vilket gör att det finns* $10000 - 1626 = 8484$ *polynom som är irreducibla. Dessa polynom är alltså de som uppfyller att* Δ *har en kvadratisk residy vilket vi kommer fördjupa oss i i nästa avsnitt.*

Vi börjar med att studera en ännu starkare hypotes av Bateman-Horn som ger ett mått på antalet positiva tal $n \leq N$ s.a. en mängd polynom med Bunyakowskiegenskaper $f_1(n), f_2(n), ..., f_m(n)$ alla samtidigt antar primtalslösningar.[7]

Hypotes 2. *(Bateman-Horn) Låt* $f_1, f_2, ..., f_m$ *vara polynom av en variabel med grad* $k_1, k_2, ..., k_m$ *som uppfyller Bunyakowskiegenskaper dvs. i)-iii) i Hypotes 1.* $P(x)$ *är antalet positiva tal* $n \leq N$ *s.a.* $f_1(n), f_2(n), ..., f_m(n)$ *alla är prima. Då gäller att*

$$P(x) \sim \frac{C}{D} \int_2^x \frac{dt}{(\log t)^m} \tag{18}$$

där $D = k_1^{-1} k_2^{-1} \cdot ... \cdot k_m^{-1}$ *och*

$$C(f_1, f_2, ..., f_m) = \prod_p \left(1 - \frac{\omega(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-m} \tag{19}$$

där $\omega(p)$ *är antalet lösningar till ekvationen*

$$f_1(x) f_2(x) \cdot ... \cdot f_n(x) \equiv 0 \pmod{p} \tag{20}$$

med $x \in \{0, 1, 2, ..., p-1\}$.

Vi ska diskutera vad denna formel innebär utifrån ett heuristiskt resonemang och visa några enklare specialfall. Vi har tidigare visat att sannolikheten att q är primtal för ett stort tal är $q \sim 1/\log q$. Om vi skulle behandla $f_i(n)$ som en slumpvis variabel skulle sannolikheten att $\sim 1/\log f_i(n)$. Men om $grad(f_i(n)) = k_i$ är $\log f_i(n) \approx \log n^{k_i} = h_i \log n$vilket skulle innebära att

$$\frac{1}{k_i \log n}$$

ge sannolikheten för att $f_i(n)$ antar primtalsvärde. Om vi utvidgar resonemanget och behandlar polynomen $f_1, f_2, ..., f_m$ som självständiga slumpvisa variabler borde sannolikheten för polynomen samtidigt är prima vid n vara

$$\prod_{i=1}^{m} \frac{1}{k_i (\log n)^i} = k_1^{-1} k_2^{-1} \cdot ... \cdot k_m^{-1} (\log n)^{-m}.$$

Antalet värden av n med $0 < n \leq N$ som ger primtal borde med detta resonemang vara

$$k_1^{-1} k_2^{-1} \cdot ... \cdot k_m^{-1} \sum_n^N (\log n)^{-m}.$$

[7] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, Math. Comp. 16 (1962), 363-367

Dock är det osannolikt att $f_1(n), f_2(n), ..., f_m(n)$ är slumpmässiga tal vilket korrigeras med en faktor $C(f_1, f_2, ..., f_m)$. För varje primtal p multiplicerar vi med förhållandet r_p/s_p där r_p är sannolikheten att ingen av $f_1(n), f_2(n), ..., f_m(n)$ är delbart med p och s_p är sannolikheten att p inte delar en av m slumpvalda tal dvs. vi korrigerar genom att multiplicera med ett mått på hur långt i från slumpartade värdena är. Men då borde $r_p = 1 - \omega(p)/p$ och $s_p = (1 - 1/p)^m$ vilket då skulle ge

$$C(f_1, f_2, ..., f_m)k_1^{-1}k_2^{-1} \cdot ... \cdot k_m^{-1} \sum_n^N (\log n)^{-m},$$

med korrigeringsfaktorn

$$C(f_1, f_2, ..., f_m) = \prod_p r_p/s_p = \prod_p \frac{1 - \omega(p)/p}{(1 - 1/p)^m},$$

vilket för stora N är i stort sett samma formel vi började med. Vi illustrerar Bateman-Horn hypotesen med några enkla exempel.

Exempel 10. *Om $f(n) = n$ finns endast en lösning då $n \equiv 0 \pmod p$ vilket gör att $\omega(p) = 1$ för alla p. Detta ger $C = 1$ och vi får primtalssatsen*

$$\pi(N) \sim \int_2^N \frac{dn}{\log n}.$$

Exempel 11. *Om $f_1(n) = n$ och $f_2(n) = (n + 2)$ kan vi hitta konstanten C_{tv} för alla primtalstvillingar $p(p + 2)$. Antalet lösningar till ekvationen*

$$x(x + 1) \equiv 0 \pmod p$$

för $x \in \{0, 1, ..., p - 1\}$ ges av

$$\omega(p) = \begin{cases} 1 & om\ p = 2 \\ 2 & om\ p \geq 3. \end{cases}$$

Från (19) får vi således uttrycket

$$2C_{tv} = \prod_p \frac{1 - \omega(p)/p}{(1 - 1/p)^2} = \frac{(1 - 1/2)}{(1 - 1/2)^2} \prod_{p \geq 3} \frac{1 - 2/p}{(1 - 1/p)^2} =$$

$$2 \prod_{p \geq 3} \frac{(p - 2)/p}{(p - 1)^2/p^2} = 2 \prod_{p \geq 3} \frac{p(p - 2)}{(p - 1)^2} \approx 2 \cdot 0.66 = 1.32.$$

Hypotes 3. *(Första Hardy-Littlewood om tvillingprimtal) Låt $\pi_{tv}(N)$ vara antalet primtal $p \leq N$ s.a. $p+2$ också är primtal. Konstanten C_{tv} är då*

$$\prod_{p \geq 3} \frac{p(p - 2)}{(p - 1)^2} \approx 0.6601618158$$

och hypotesen säger då att

$$\pi_{tv}(n) \sim 2C_{tv}\frac{n}{(\ln n)^2} \sim 2C_{tv}\int_2^n \frac{dt}{(\ln n)^2}. \tag{21}$$

Exempel 12. *Om vi nu studerar* $f(n) = n^2 + 1$ *observerar vi att för ett jämt och udda tal*

$$f(2m) = 4(m^2) + 1\ ,\ f(2m+1) = 2(2m^2 + 2m + 1)$$

ligger alla primtal distribuerade på formen $4n+1$ *för jämna tal eftersom alla* $f(n)$ *för udda tal är delbara med* 2 *och genererar inga primtal. Antalet lösningar* $\omega(p)$ *för kongruensen*

$$n^2 + 1 \equiv 0 \pmod{p} \quad \Rightarrow \quad n^2 \equiv -1 \pmod{p}$$

ger, förutom $\omega(2) = 1$, *endast lösningar på formen* $p = 4n + 1$.

Innan vi går vidare är det lämpligt att introducera ett verktyg för att lösa kongruenser av typen $x^2 \equiv a \pmod{p}$ och vi måste införa mer teori för att kunna lösa problemet.

4.1. **Kvadratisk residy.** Att lösa en polynomekvation av typen

$$f(x) \equiv 0 \pmod{p}$$

där $f(x)$ är ett kvadratiskt polynom kan reduceras till att lösa

$$x^2 \equiv a \pmod{p}. \tag{22}$$

Observera att om x är en lösning så är även $-x$ en lösning till (22).

Definition 3. Om (22) har en lösning så säger vi att a är en kvadratisk residy mod p. Om (22) inte har någon lösning säger vi att a är en ickekvadratisk residy.

Definition 4. Med ett *reducerat residysystem modulo* p menar vi någon mängd av $\phi(p)$ tal som inkongruent med varandra modulo p och varje tal är relativt prima p.

Exempel 13. *Hitta alla kvadratiska residyer* (mod 13). *Vi ska hitta alla lösningar* x *till*

$$x^2 \equiv a \pmod{13}$$

där $a \in (\mathbb{Z}/13\mathbb{Z})^*$ *med antalet element är* $\phi(p-1) = 12$ *men det endast nödvändigt att kvadrera hälften av elementen eftersom vi kan skriva* $(\mathbb{Z}/13\mathbb{Z})^* = \{\pm 1 \pm 2 \pm 3 \pm 4 \pm 5 \pm 6\}$.

$$1^2 = 1\ ,\ 2^2 = 4\ ,\ 3^2 = 9\ ,\ 4^2 = 3\ ,\ 5^2 = 12\ ,\ 6^2 = 10$$

vilket gör att elementen i $(\mathbb{Z}/13\mathbb{Z})^*$ *har* $12/2 = 6$ *kvadratisk residyer* $\{1, 3, 4, 9, 10, 12\}$ *och* $12/2 = 6$ *ickekvadratiska residyer* $\{2, 5, 6, 7, 8, 11\}$.

Sats 7. *Låt p vara ett udda primtal. Varje reducerat residysystem mod p består av $(p-1)/2$ kvadratiska residyer och $(p-1)/2$ ickekvadratiska residyer. De kvadratiska residyerna tillhör residyklasserna som ges av talen*

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right). \tag{23}$$

Bevis. Först visar vi att varje tal som fås av (23) är unikt (mod p). Om x, y är två kvadratiska residyer s.a. $x^2 \equiv y^2 \pmod{p}$ där $1 \leq x \leq (p-1)/2$ och $1 \leq y \leq (p-1)/2$ gäller att

$$x^2 - y^2 = (x-y)(x+y) \equiv 0 \pmod{p}.$$

Men $1 < x+y < p$ så $x - y \equiv 0 \pmod{p}$ alltså är $x = y$. Eftersom det gäller att

$$(p-k)^2 \equiv k^2 \pmod{p},$$

är varje kvadratisk residy (mod p) till exakt en av talen i (23) vilket fullbordar beviset. □

Definition 5. Låt p vara ett udda primtal. Då definieras Legendresymbolen som

$$(a|p) = \begin{cases} 1 & \text{om } a \text{ är en kvadratisk residy (mod } p) \\ -1 & \text{om } a \text{ är en ickekvadratisk residy (mod } p) \\ 0 & \text{om } p|a. \end{cases} \tag{24}$$

Sats 8. *(Eulers kriterium) Låt p vara ett udda primtal. Då har vi att*

$$(a|p) = a^{(p-1)/2} \pmod{p}. \tag{25}$$

Bevis. Vi delar in i tre fall utifrån Legendresymbolens definition. Anta först att $p|a$. Då är båda sidorna är kongruenta med 0 (mod p). Anta att $(a|p) = 1$. Detta innebär att a är en kvadratisk residy och att $x^2 \equiv a \pmod{p}$. Detta ger att

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{(p-1)} = 1 \pmod{p}$$

vilket visar satsen för $(a|p) = 1$. Anta att $(a|p) = -1$ och att a är ickekvadratisk residy. Om vi betraktar polynomet

$$f(x) = x^{(p-1)/2} - 1,$$

har det maximalt $(p-1)/2$ lösningar till kongruensen

$$f(x) \equiv 0 \pmod{p}.$$

Men eftersom $(p-1)/2$ lösningar ges av de element som har kvadratisk residy är $a^{(p-1)/2} \not\equiv 1$. Men $a^{(p-1)/2} = \pm 1$ vilket innebär att $a^{(p-1)/2} = -1$ vilket färdigställer beviset. □

(25) gör att vi kan dra vissa slutsatser om Legendresymbolens egenskaper.

Sats 9. *Legendresymbolen $(a|p)$ har egenskaperna:*

i) $(a|p)$*är en fullständigt multiplikativ funktion av* a.
ii) $(a|p)$*är periodisk av* a *med perioden* p.
iii) $(a|p) = \chi(p)$ *är en kvadratisk Dirichetkaraktär mod* p.

Bevis. i) Visa att $(ab|p) = (a|p)(b|p)$. Vi börjar med att anta $a \mid p$ eller $b \mid p \Rightarrow ab \mid p$ så $(ab|p)$. Alltså måste antingen $(a|p) = 0$ eller $(b|p) = 0$ så $(ab|p) = (a|p)(b|p)$. Anta nu att $a \nmid p$ och $b \nmid p$ så $ab \nmid p$ vilket ger

$$(ab|p) = (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} = (a|p)(b|p) \pmod{p}.$$

Eftersom $(ab|p) = (a|p) = (b|p) = \pm 1$ är differansen i

$$(ab|p) - (a|p)(b|p) \pmod 2$$

antingen $0, \pm 2$ men eftersom den är delbar med p måste den vara noll.

ii) Det är uppenbart att när $(a|p) = (b|p)$ är $a \equiv b \pmod p$ så $(a|p)$ är en periodisk funktion med perioden p.

iii) Enligt i) och ii) är $(a|p)$ är periodisk av a med period p, fullständigt multiplikativ och eliminerar termer när $a \mid p$ och det följer att $(a|p) = \chi(a)$ där χ är en primitiv karaktär som endast antar reella värden dvs. ± 1. □

Sats 10. *För varje udda primtal gäller att*

$$(-1|p) = \begin{cases} 1 & om\ p \equiv 1 \pmod 4 \\ -1 & om\ p \equiv 3 \pmod 4. \end{cases} \tag{26}$$

Bevis. Genom (25) har vi att $(-1|p) = (-1)^{(p-1)/2} \pmod p$. □

Sats 11.

$$(2|p) = \begin{cases} 1 & om\ p \equiv \pm 1 \pmod 8 \\ -1 & om\ p \equiv \pm 3 \pmod 8. \end{cases} \tag{27}$$

Bevis. Vi börjar med att undersöka följande $(p-1)/2$ kongruenser:

$$\begin{aligned} p - 1 &\equiv 1(-1)^1 \pmod p \\ 2 &\equiv 2(-1)^2 \pmod p \\ p - 3 &\equiv 3(-1)^3 \pmod p \\ 4 &\equiv 4(-1)^4 \pmod p \\ &\vdots \\ r &\equiv \tfrac{p-1}{2}(-1)^{(p-1)/2} \pmod p. \end{aligned}$$

Observera att även $p-k$ är jämt tal om k är udda. Om vi multiplicerar ihop alla kongruenser får vi

$$\prod_{n=1}^{p-1}(2n) \equiv \prod_{n=1}^{(p-1)/2} n(-1)^n \Rightarrow$$

$$2^{(p-1)/2} \prod_{n=1}^{(p-1)/2} n \equiv (-1)^{\sum_n^{(p-1)/2} n} \prod_{n=1}^{(p-1)/2} n.$$

Om vi beräknar $\sum_{n=1}^{(p-1)/2} n = (p^2-1)/8$ med aritmetisk summa, samt stryker produkterna får vi

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \Rightarrow (2|p) \equiv (-1)^{(p^2-1)/8},$$

där vi har använt (25) vilket fullbordar beviset. □

Dessa två resultat är de första två specialfallen av *Kvadratiska reciprocitetslagen.* Både Euler och Legendre försökte bevisa detta men det var Gauss som år 1796 var den första som lyckades. Han var mycket stolt över detta resultat och kallade det *Theorema Aureum*, det gyllene theoremet[8]. Denna lag beskriver en generell metod för att bestämma $(q|p)$ där p, q är primtal.

Sats 12. *(Kvadratiska reciprocitetslagen) Om p, q är distinkta udda primtal gäller*

$$(p|q)(q|p) = (-1)^{((p-1)/2)((p-1)/2)}. \tag{28}$$

Vi ger inget bevis för (28) då detta är för omfattande. Om $a = q_1 q_2 q_3 \cdot \ldots \cdot q_n$ är ett sammansatt tal kan vi utnyttja att $(a|p)$ är multiplikativ

$$(a|p) = (q_1|p)(q_2|p) \cdot \ldots \cdot (q_n|p)$$

och sedan använda (28).

4.2. Polynom på formen $f(x) = x^2 + a$. [9]

Hypotes 4. *(Hardy-Littlewood) Låt $f(n) = n^2 + a$ för alla $a \neq 0$ där $n \neq -m^2$ och $1 \leq n < N$ då ges antalet primtal av*

$$P_a(N) \sim \frac{1}{2} C_a \int_2^N \frac{dn}{(\log n)}, \tag{29}$$

där C_a är en konstant som ges av den oändliga produkten

$$C_a = \prod_{p \text{ udda}}^{\infty} \left(1 - \frac{(-a|p)}{1-p}\right) \tag{30}$$

och $(-a|p)$ är Legendre symbolen

$$(-a|p) = \begin{cases} 1 & om\ p \equiv -a \pmod p \\ -1 & om\ p \not\equiv -a \pmod p. \end{cases}$$

Vi visar att detta är ett specialfall av Bateman-Horn hypotesen (18) med endast en funktion $f(x) = x^2 + a$ med $grad(f(x)) = 2 \Rightarrow D = 1/2$. Då gäller att

$$p \mid f(x) \Rightarrow f(x) \equiv 0 \pmod p \Rightarrow x^2 + a \equiv 0 \pmod p \Rightarrow$$
$$x^2 \equiv -a \pmod p.$$

[8] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, 2nd ed. (1990) s.50

[9] D. Shanks, On the conjecture of hardy & littlewood concerning the number of primes of the form $n^2 + a$, Math. Comp. (1962), p.321-332.

Enligt definitionen av kvadratisk residy samt Legendresymbolens definition (24) gäller att antalet lösningar i (20) ges av

$$\omega(p) = 1 + (-a|p) = \begin{cases} 2 & om\ p \equiv -a \pmod{p} \\ 0 & om\ p \not\equiv -a \pmod{p}. \end{cases}$$

Vi kan skriva om (19) som

$$C = \prod_p \left(\frac{1 - \frac{\omega(p)}{p}}{1 - \frac{1}{p}} \right) = \prod_p \left(\frac{p - \omega(p)}{p - 1} \right)$$

$$\prod_p \left(\frac{p - (1 + (a|p))}{p - 1} \right) = \prod_p \left(1 - \frac{(-a|p)}{p - 1} \right) = C_a$$

genom att först multiplicera täljare och nämnare med p, sätta in $\omega(p) = 1 + (a|p)$ och sedan göra bråkuppdelning. Alltså är (29) ett specialfall av (19).

4.3. **Polynom på formen x^2+1 och x^2-2.** Om $f_1(x) = x^2+1$ samt $f_2(x) = x^2 - 2$ kan vi skriva om (30) med (26) och (27) vilket för $p \neq 2$ ger oss

$$C_{-1} = \prod_{p \equiv 1(4)} \left(1 - \frac{1}{p-1} \right) \prod_{p \equiv 3(4)} \left(1 + \frac{1}{p-1} \right) =$$

$$\left(1 + \frac{1}{2}\right)\left(1 - \frac{1}{4}\right)\left(1 + \frac{1}{6}\right)\left(1 + \frac{1}{10}\right)\left(1 - \frac{1}{12}\right) \cdot \ldots$$

$$C_2 = \prod_{p \equiv \pm 1(8)} \left(1 - \frac{1}{p-1} \right) \prod_{p \equiv \pm 3(8)} \left(1 + \frac{1}{p-1} \right) =$$

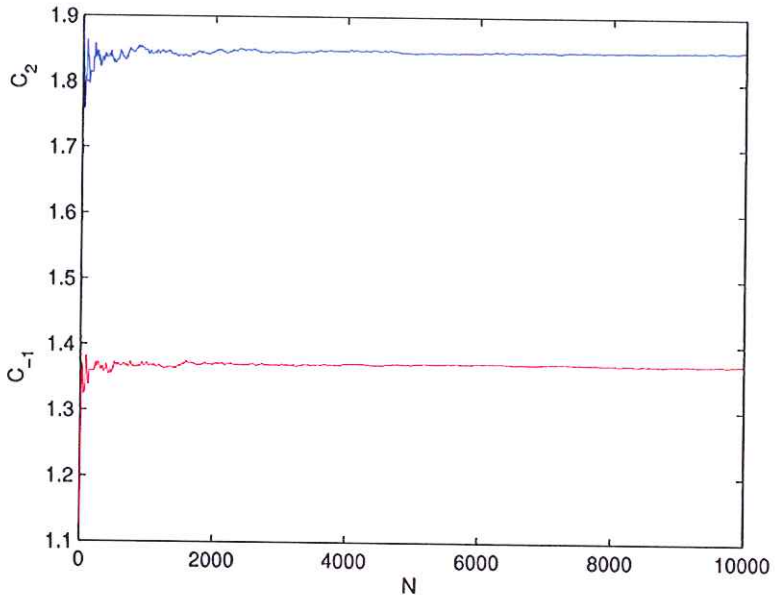
$$\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{4}\right)\left(1 - \frac{1}{6}\right)\left(1 + \frac{1}{10}\right)\left(1 - \frac{1}{12}\right) \cdot \ldots .$$

Vi observerar att C_a konvergerar långsamt eftersom den alternerar tecken. För alla $p \leq N = 10000$ har vi att

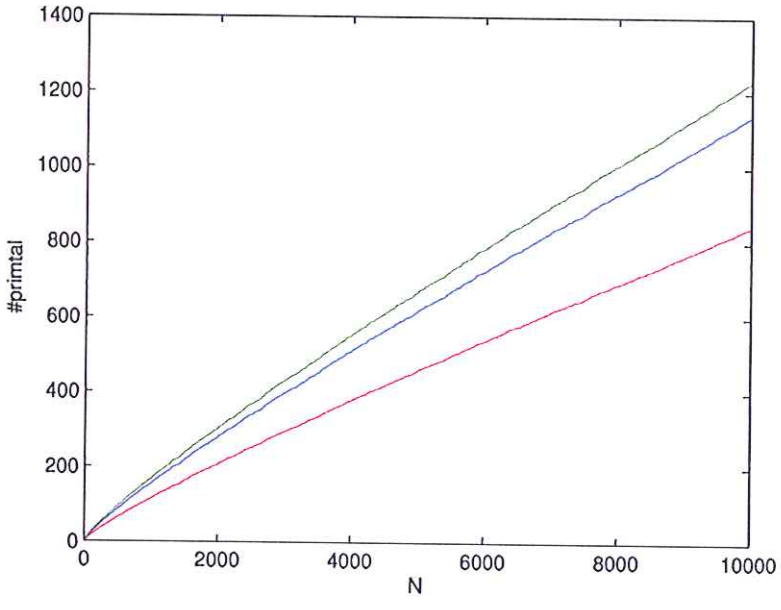
$$C_{-1} = 1.2710$$
$$C_2 = 1.8495.$$

Från (29) får vi sedan

$$P_{-1}(N) = \tfrac{1}{2} C_{-1} \pi(N) = 0.6355\pi(N)$$
$$P_2(N) = \tfrac{1}{2} C_2 \pi(N) = 0.9247\pi(N).$$



FIGUR 7. Konstanten C_{-1} och C_2 för alla $p \leq N$ för $N = 10000$.



FIGUR 8. Jämförelse mellan antalet primtal av formen $f_1(n) = n^2 + 1$(röd kurva), $f_2(n) = n^2 - 2$ (blå kurva)och $\pi(n)$ (grön kurva) för $n < N$ där $N = 10000$.

REFERENSER

[1] Apostol, Tom M., Introduction to analytic number theory, Undergraduate Texts in Mathematics, Springer-Verlag, (1976)
[2] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, 2nd ed. (1990).
[3] E.B. Saff, A.D. Snider, Fundamentals of Complex Analysis, 3rd ed., Pearsson Education(2003)
[4] John A. Beachy, William D. Blair, Abstract Algebra,3rd edtion, Waveland (2006),
[5] John Derbyshire, Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics, Plume (2004)
[6] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, Math. Comp. 16 (1962), 363-367.
[7] D. Shanks, On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$, Math. Comp. (1962), p.321-332.
[8] D. Shanks, A sieve method for factoring numbers of the form $n^2 + 1$, MTAC, v. 13, (1959), p. 78-86.
[9] D.Shanks , Solved and Unsolved Problems in Number Theory, Chelsea Publishing Company (1978), p. 1-47
[10] R. Guy, Unsolved problems in number theory, 3rd ed., Springer (2005) p.3-69
[11] Ian Stewart ,From here to infinity a guide to today's mathematics Retitled and rev. ed. Oxford Univ. (1996), 310 s.