CHALMERS | GÖTEBORGS UNIVERSITET

Matematiska såll, primtalstvillingar och Chens sats

Mathematical sieves, twin primes and Chen's theorem

Examensarbete för kandidatexamen i matematik vid Göteborgs universitet

Victor Ahlquist
Alf Söderberg

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2021

Matematiska såll, primtalstvillingar och Chens sats

Examensarbete för kandidatexamen i matematik inom Matematikprogrammet vid Göteborgs universitet

Victor Ahlquist   Alf Söderberg

Handledare:
Lucile Devin
Anders Södergren

Institutionen för Matematiska vetenskaper
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2021

Förord

Idén att skriva ett kandidatarbete om matematiska såll ska tillskrivas våra handledare. Resultatet är en litteraturstudie av Heini Halberstams och Hans-Egon Richerts bok *Sieve Methods*. Vårt mål är att presentera olika sorters matematiska såll och några tillämpningar i studiet av primtalstvillingar. Vi avslutar med att presentera Chens sats och studera dess bevis.

Rapporten ska först och främst betraktas som en gruppprestation. För att underlätta en individuell bedömning har vi under arbetets gång fört en loggbok över varje medförfattares insats. Detta omfattar dels en dagbok som varje vecka lämnats in till examinatorerna, dels en individuell tidslogg där var och en angett vad de arbetat med och hur länge.

De olika avsnitten i den slutliga rapporten har författats enligt följande:

- Victor Ahlquist: Sammanfattning, kapitel 1, avsnitt 2.1, 2.3, 4.2, 4.3, 4.5, kapitel 5, avsnitt 6.3 till och med ekvation (6.12), avsnitt 6.4, appendix A, avsnitt B.1, B.3.1, B.4.2, B.4.3 och B.4.5.
- Alf Söderberg: Förord, populärvetenskaplig presentation, avsnitt 2.2, 3.3, 3.4, 4.1, 4.4, 6.1, 6.2, 6.3 från och utan ekvation (6.12), avsnitt B.2, B.3.2, B.4.1 och B.4.4.
- Avsnitt 3.1 och 3.2 har skrivits gemensamt.

Arbetet med att anpassa Chens sats, såsom den behandlas i [HR, kapitel 11], till fallet med primtalstvillingar har både Victor och Alf utfört.

I synnerhet i arbetets slutskede har vi bidragit till den slutliga utformningen även på varandras delar.

Vi vill framföra vårt varma tack till våra handledare, Lucile Devin och Anders Södergren. Utan deras värdefulla hjälp och stöd hade projektet inte varit genomförbart. De har vid flera tillfällen läst igenom texten, bidragit med värdefulla insikter och gett förslag på relevanta förbättringar.

Populärvetenskaplig presentation

Såll används av de flesta till vardags i någon form, till exempel när man brygger kaffe eller kokar pasta. Principen för ett såll är enkel: den handlar om att skilja saker åt, ofta något vi vill ha från något vi inte vill ha. Också inom matematiken förekommer såll, och även om de skiljer sig från vad de flesta är vana vid bygger de på samma princip.

Matematiska såll används inom talteorin, ett område ägnat åt att studera heltalen och deras egenskaper. Centrala i talteorin är *primtal*, som enbart är delbara med sig själva och 1. Tal som inte är primtal kallas *sammansatta*. De första primtalen är $2, 3, 5, 7, 11, 13, ...$ (Talet 1 räknas inte som ett primtal). Differensen mellan två primtal kan inte vara mindre än 2, förutom i undantagsfallet $3 - 2 = 1$. Par av primtal $(p, p + 2)$ vars avstånd till varandra är precis 2 kallas *primtalstvillingar*. De första primtalstvillingarna är $(3, 5), (5, 7), (11, 13)$ och $(17, 19)$.

En stor del av talteorin går ut på att undersöka primtal. Redan den grekiske matematikern Euklides (325-265 f.v.t.) visste att det finns ett oändligt antal primtal. Vi kan ställa samma fråga om primtalstvillingar: finns det ett oändligt antal primtal p sådana att också $p + 2$ är ett primtal? Frågan är, trots sin enkelhet, ännu inte besvarad.

Ett annat fenomen är att det verkar som om alla jämna tal större än 2 kan skrivas som en summa av två primtal. Vi har till exempel att $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$ och $10 = 5 + 5$, och så vidare. Inte heller detta har kunnat bevisas än, även om många matematiker tror att det är så.

Dessa båda problem kallas *primtalstvillingsförmodan* och *Goldbachs förmodan*. De ansågs länge vara nästan omöjliga att angripa, men under 1900-talet togs de första stegen mot en lösning. I denna process har matematiska såll visat sig oumbärliga.

Matematiska såll finns i flera olika varianter, och det är vårt syfte att studera några av dem. Vi kommer se hur vart och ett av sållen relaterar till problemet om primtalstvillingar. I nuläget kan de inte användas för att bevisa den ursprungliga frågan, men de kan visa närliggande resultat.

Det första sållet vi studerar är det äldsta och härrör från den grekiske matematikern Eratosthenes (276-194 f.v.t.). Tillvägagångssättet är relativt enkelt, och handlar om att på ett effektivt sätt hitta alla primtal i en given talmängd. Som illustration kan vi betrakta talen $1, 2, 3..., 100$. Den första observationen vi gör är att vart och ett av dessa tal som *inte* är ett primtal har minst två primtalsfaktorer. Av dessa är minst en faktor mindre än eller lika med 10, för om båda vore större än 10 skulle talet vara större än $10 \cdot 10 = 100$. Genom att stryka alla tal delbara med primtal mindre än eller lika med 10 kan vi därmed hitta alla primtal mellan 10 och 100.

Efter Eratosthenes dröjde det länge innan andra sållmetoder introducerades, och de flesta som vi studerar härrör från 1900-talet. De är mer komplicerade, men konceptet är detsamma. Generella sållmetoder arbetar med en ändlig talmängd, och syftar att ur denna sovra vad som är intressant, och uppskatta storleken av detta. I Eratosthenes såll skiljer vi till exempel primtal från sammansatta. I nyare sållmetoder är det inte säkert att det är lika effektivt. Mer generellt kanske man intresserar sig för tal med två, tre eller fem primtalsfaktorer. Ibland betraktar vi också primtal p till vilka vi adderar en konstant h. Den naturliga frågan är då att undersöka om $p + h$ också är ett primtal. Primtalstvillingsförmodan handlar om fallet $h = 2$, men man kan även undersöka saken för andra h.

Två av de nyare sållmetoderna har namngivits efter norrmännen Viggo Brun (1885-1978) och Atle Selberg (1917-2007). Bruns metod bygger på att på ett intrikat sätt välja vilka tal som ska sållas bort efter hur deras primtalsfaktorer är fördelade. På så sätt kan man visa att det finns ett oändligt antal heltal n så att både n och $n - 2$ har som mest sju primtalsfaktorer. Det kan jämföras med primtalstvillingsförmodan, som säger samma sak fast med *en* istället för sju faktorer. I sitt historiska sammanhang utgjorde Bruns insatser en viktig milstolpe i arbetet med förmodan. Selbergs idé bygger istället på att reella tal, när man multiplicerar dem med sig själva, aldrig är mindre än 0. Det använde Selberg genom att till varje element i talmängden vi vill undersöka tillskriva en så kallad *vikt* som är större än eller lika med 0.

Selbergs metoder används bland annat för att visa Chens sats, som vårt arbete avslutas med. Den är namngiven efter den kinesiska matematikern Jingrun Chen (1933-1996) och säger att det finns ett oändligt antal primtal p så att $p + 2$ har en eller två primtalsfaktorer. När den publicerades rönte den stor uppmärksamhet, och är än idag en av de skarpaste approximationerna till primtalstvillingsförmodan.

Sammanfattning

Matematisk sållteori har varit ett viktigt verktyg för många nutida resultat inom analytisk talteori. Med hjälp av Halberstam och Richerts *Sieve Methods* redogör vi för grundläggande sållteori med fokus på tillämpningar i studiet av primtalstvillingar. Vi bevisar och tillämpar varianter av Eratosthenes-Legendres såll, Bruns såll och Selbergs såll. Vi formulerar också de viktigaste resultaten från en utveckling av Selbergs såll för linjära problem. Avslutningsvis återger vi delar av beviset av Chens sats, som implicerar existensen av oändligt många par $(p, p+2)$ där p är ett primtal och $p+2$ en produkt av maximalt 2 primtal.

Abstract

Mathematical sieve theory has been an important tool for many recent results in analytic number theory. Using Halberstam and Richert's *Sieve Methods*, we present the fundamentals of sieve theory with a focus towards applications to the study of twin primes. We prove and apply forms of Eratosthenes-Legendre's sieve, Brun's sieve, and Selberg's sieve. We also formulate the most important results from a development of Selberg's sieve for linear problems. We conclude with a partial proof of Chen's theorem which shows the infinitude of pairs $(p, p+2)$ with p a prime and $p+2$ a product of at most two primes.

Innehåll

1 Inledning

Vi ger en beskrivning av sållteorins utveckling, presenterar rapportens upplägg samt rekommenderade förkunskapskrav och lässtrategi för rapporten. Avslutningsvis förklarar vi notation och återger elementär talteori som används i senare kapitel.

1.1 Bakgrund och rapportens mål

Studiet av primtal har alltid varit en central del av talteorin och det finns idag många öppna problem gällande talföljder kopplade till primtalen. Euklides (325-265 f.v.t.) visade tidigt existensen av oändligt många primtal. Ett relaterat, men svårare, problem är frågan om existensen av oändligt många primtalstvillingar, det vill säga oändligt många primtal p sådana att även $p+2$ är ett primtal. Problemet kallas primtalstvillingsförmodan och är olöst, men ett av de mest fruktsamma verktygen för att angripa problemet har hittills varit sållteori.

Sållteori kan sägas utgöra en utvidgning av Eratosthenes (276-194 f.v.t.) ursprungliga algoritm för att finna primtalen upp till en viss gräns. Legendre (1752-1833) utvecklade Eratosthenes metod till det som idag kallas Eratosthenes-Legendres såll och en formulering av sållet återfinns nedan i form av Sats 2.1. Brun (1885-1978) kan sägas ha inlett den moderna sållteorin med [Br] där Bruns kombinatoriska såll, som utgör ett förbättring gentemot Eratosthenes-Legendres såll, presenteras. Ett resultat baserat på Bruns idéer finner läsaren i Sats 3.2.

Selberg (1917-2007) utvecklade 1947 en version av det vi idag kallar Selbergs såll [S]. Metoden har i utökad form kunnat användas för att erhålla undre begränsningar för många följder och speciellt följder kopplade till primtalstvillingar. Förutom Brun och Selberg, som har lagt grunden för sållteorin, bör även bidragen från Bombieri och Vinogradov nämnas där Bombieri-Vinogradovs sats ger en begränsning på en felterm som ofta uppkommer i sållteorin. Satsen bevisades i den form vi behöver den av Bombieri i [Bo], och leder nästan direkt till vårt Lemma 4.3.

Vårt mål är att redogöra för delar av beviset för en approximation av primtalstvillingsförmodan. Specifikt kommer vår kvantitativa Sats 6.1 implicera följande kvalitativa resultat, som först bevisades av Chen (1933-1996) i [C]. Fallet $h = 2$ är speciellt intressant på grund av kopplingen till primtalstvillingar.

Sats 1.1. *För varje jämnt $h \neq 0$ existerar det oändligt många primtal p sådana att $p + h$ är ett primtal, eller en produkt av maximalt två primtal.*

Bland mer nutida bidrag till sållteorin återfinns ett anmärkningsvärt resultat från Zhang [Z]. Zhang bevisade att det existerar något h mindre än 70 miljoner sådant att det finns oändligt många primtalspar vars avstånd till varandra är mindre än h. Konstanten h har ytterligare begränsats, och speciellt kan Maynards bidrag [M] nämnas där han med nya metoder begränsade h till 600. Polymath-projektet, där bland annat Maynard och Tao deltog, använde i [P] idéerna från [M] och [Z] för att begränsa h till 246. Vi ser att om konstanten h kan begränsas till 2 är primtalstvillingsförmodan bevisad.

1.2 Rapportens upplägg och avgränsningar

I samtliga kapitel följer vi ungefär presentationen i [HR]. Vi inleder med att i kapitel 2 ge sållteoretiska exempel, samt beskriva Eratosthenes-Legendres såll. Vi utelämnar beviset, men det återfinns i appendix B.1. Kapitel 3 är fristående från framställningen i resterande kapitel, men vi lyckas här visa intressanta tillämpningar. Vi inleder med att behandla kombinatoriska såll i allmänhet och härleder olikheten (3.8). Vi presenterar sedan Bruns såll i form av Sats 3.2, tillsammans med tillämpningar på primtalstvillingar. Ett bevis av Sats 3.2 finns i appendix B.2.

Vi ger i kapitel 4 en noggrann introduktion till Selbergs såll i form av Sats 4.1 som senare kopplas till studiet av primtalstvillingar. Eftersom Selbergs såll är det viktigaste grundläggande sållet för Chens sats ges ett bevis för Sats 4.1 direkt i kapitel 4. Vi studerar sedan det linjära sållet, som har stor betydelse för primtalstvillingar, i kapitel 5. De viktigaste resultaten som används i Chens sats formuleras, men fullständiga bevis utelämnar vi. Förhoppningsvis förmedlas dock den koppling satserna har till den övriga sållteorin.

Avslutningsvis behandlar vi beviset av Chens sats för primtalstvillingar. Här skiljer vår framställning sig från [HR], som istället behandlar Chens sats för Goldbachs förmodan, men många argument är lika. Vi beskriver noggrant de delar av beviset som har koppling till rapportens tidigare avsnitt. Vi ställer upp ett såll för att approximera antalet element i $\{p+h : p \leq N,\ p+h \in P_2\}$, där P_2 betecknar mängden av alla heltal med maximalt två primtalsdelare och p betecknar primtal. I nästa steg använder vi satserna från kapitel 5 för att erhålla en undre begränsning för mängden. För att slutföra beviset behöver vi uppskatta tre summor, men en av uppskattningarna kräver mer teori än omfånget av rapporten tillåter och vi hänvisar läsaren till [HR, kapitel 11.4-11.6] för detaljerna. Uppskattningarna av de andra summorna redogörs för i appendix B.4.5 och tillsammans med den utelämnade uppskattningen slutför det beviset av Chens sats.

1.3 Rekommenderade förkunskaper och lässtrategi

För att tillgodogöra sig innehållet i texten bör läsaren ha god förståelse av elementär talteori, till exempel i form av innehållet i [R]. Några viktiga talteoretiska resultat som vi använder finns i appendix A, tillsammans med användbara uppskattningar. Vi poängterar dock att en fullständig introduktion till elementär talteori ligger utanför rapportens ramar. Rapporten kan läsas sammanhängande från början till slut, men vi har utelämnat vissa bevis och tekniska detaljer från huvudtexten. Vi markerar tydligt i texten om detaljerna återfinns i appendix.

1.4 Talteoretiska definitioner och notation

Vi återger här viktiga definitioner från elementär talteori. Vi använder notationen från [HR] som med få undantag är standardnotation inom talteori. För ett positivt heltal n betecknar $\nu(n)$ antalet primtalsdelare utan multiplicitet, och $\Omega(n)$ antalet primtalsdelare med multiplicitet. Vi låter $\nu(1) = \Omega(1) = 0$. Den naturliga logaritmen betecknas med log och om k är ett positivt heltal skriver vi $\log^k x$ för $(\log x)^k$. Ett positivt heltal n kallas kvadratfritt om ingen primtalskvadrat delar n. Vi betecknar Eulers konstant, som är gränsvärdet av skillnaden mellan den n:te delsumman av den harmoniska serien och $\log n$, med γ. Funktionen $\mu(n)$ betecknar Möbiusfunktionen, definierad enligt

$$\mu(n) = \begin{cases} (-1)^{\nu(n)} & \text{om } n \text{ är kvadratfritt,} \\ 0 & \text{annars.} \end{cases} \tag{1.1}$$

Vi låter $\phi(n)$ beteckna antalet positiva heltal mindre än eller lika med n som är relativt prima till n. För två heltal a, b betecknar (a, b) deras största gemensamma delare, och $[a, b]$ deras minsta gemensamma multipel. Låt f vara en komplexvärd funktion, definierad på de positiva heltalen, som inte är konstant lika med 0. Vi kallar då f multiplikativ om $f(mn) = f(m)f(n)$ för relativt prima tal m, n. Det följer från definitionen att μ är multiplikativ och från elementär talteori vet vi att även ϕ är det. Vi låter alltid p beteckna ett primtal. Vidare låter vi $\pi(x)$ beteckna antalet primtal mindre än eller lika med x och $\pi(x; d, a)$ motsvarande antal primtal i restklassen a modulo d. Speciellt är $\pi(x) = \sum_{p \leq x} 1$. Funktionen $\operatorname{li} x$ definieras som

$$\operatorname{li} x = \int_2^x \frac{1}{\log t} dt, \ \ x \geq 2.$$

Vi har ofta nytta av ordo-notation. När vi skriver

$$f(x) = \mathcal{O}(g(x)), \ \text{eller } f(x) \ll g(x),$$

menar vi att det finns en konstant $C \geq 1$ så att $|f(x)| \leq C|g(x)|$ för alla x i en underförstådd mängd. Ofta kommer det vara mängden av alla x så att $x \geq 2$, men villkoret $x \geq 3$ kan vara underförstått om vi hanterar funktionen $\log \log x$, som är 0 för $x = e$. I de flesta fall är det intervallet $[K, \infty)$ där K är ett stort tal som är den intressanta mängden. Notationen $f(x) \gg g(x)$ betyder $g(x) \ll f(x)$. På liknande sätt skriver vi

$$f(x) = h(x) + \mathcal{O}(g(x)), \tag{1.2}$$

om det existerar något $\ell(x) = \mathcal{O}(g(x))$ så att $f(x) = h(x) + \ell(x)$ för alla x i någon mängd. Istället för likhetstecken kommer vi ibland skriva $\leq$ eller $\geq$ i (1.2) med analog betydelse. Ett index, till exempel i $\mathcal{O}_h(1)$, anger vad den implicerade konstanten C tillåts bero på. Ibland utelämnas index om det framgår av kontexten vad C beror på.

2 Definitioner och inledande sållteori

Nedan följer det första sållteoretiska innehållet. Vi ger grundläggande definitioner och presenterar två viktiga villkor. Avslutningsvis formulerar vi och tillämpar en utveckling av Eratosthenes ursprungliga algoritm i form av Eratosthenes-Legendres såll.

2.1 Sållteoretiska definitioner

Vi inleder med att redogöra för grundläggande definitioner [HR, s. 14-15 och 24-25]. Heltalen utgör om inget annat anges grundmängden då vi bildar nya mängder. För en mängd eller följd $\mathcal{C}$ skriver vi $|\mathcal{C}|$ för antalet element i $\mathcal{C}$. Vi låter $\mathcal{A}$ beteckna en ändlig följd av heltal och $X > 1$ vara en approximation av $|\mathcal{A}|$. En speciell delföljd till $\mathcal{A}$ är $\mathcal{A}_d$, med d kvadratfri, definierad som mängden av de element i $\mathcal{A}$ som delas av d. Vi noterar att $\mathcal{A}_1 = \mathcal{A}$.

Till $\mathcal{A}$ kommer vi definiera en icke-negativ reellvärd funktion ω_0 på mängden av primtal som definieras så att $|\mathcal{A}_p|$ approximeras av $X\omega_0(p)/p$. Vi utökar ω_0 till en multiplikativ funktion definierad på mängden av kvadratfria tal genom $\omega_0(d) := \prod_{p|d} \omega_0(p)$. I praktiken definierar vi dock alla tal $\omega_0(d)$ samtidigt så att ω_0 blir multiplikativ. Till kvadratfria d definierar vi även en felterm $r_d = |\mathcal{A}_d| - X\omega_0(d)/d$.

Vi låter $\mathfrak{P}$ vara en mängd av primtal. För heltal K definierar vi $\mathfrak{P}_K$ som mängden av primtal som inte delar K. Speciellt är $\mathfrak{P}_1$ mängden av alla primtal och givet ett $\mathfrak{P}$ låter vi $\overline{\mathfrak{P}}$ beteckna dess komplement i $\mathfrak{P}_1$. Till $\mathfrak{P}$ definierar vi $P(z)$ som produkten av alla primtal i $\mathfrak{P}$ strikt mindre än z.

För att knyta samman $\mathcal{A}$ och $\mathfrak{P}$ definierar vi en funktion $\omega(p)$ enligt

$$\omega(p) = \begin{cases} \omega_0(p) & \text{om } p \in \mathfrak{P}, \\ 0 & \text{annars.} \end{cases}$$

Som tidigare utvidgar vi ω till en multiplikativ funktion på mängden av kvadratfria tal. Givet ω introducerar vi feltermen $R_d = |\mathcal{A}_d| - X\omega(d)/d$ och produkten

$$W(z) = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right). \tag{2.1}$$

En naturlig koppling mellan $W(z)$ och Möbiusfunktionen ges i beviset av Sats 2.1 i appendix B.1.

Betrakta $z \geq 2$ och kvadratfria q sådana att $(q, P(z)) = 1$ där q inte har någon primtalsfaktor i $\overline{\mathfrak{P}}$, vilket vi skriver som $(q, \overline{\mathfrak{P}}) = 1$. Till sådana q, z definierar vi

$$S(\mathcal{A}_q; \mathfrak{P}, z) = |\{a \in \mathcal{A}_q : (a, P(z)) = 1\}|. \tag{2.2}$$

Vårt huvudsakliga mål kommer vara att uppskatta $S(\mathcal{A}_q; \mathfrak{P}, z)$ för olika val av $\mathcal{A}$, q, $\mathfrak{P}$, och z. Ett vanligt val av q är $q = 1$.

2.2 Uppskattning av $|\mathcal{A}_d|$

Vi presenterar här ett exempel på hur vi kan uppskatta $|\mathcal{A}_d|$ [HR, exempel 3, avsnitt 1.3]. För det låter vi x och y vara reella tal som uppfyller $1 < y \leq x$. Därefter låter vi F vara ett polynom med heltalskoefficienter och betraktar $\mathcal{A} = \{F(n) : x - y < n \leq x\}$. För att uppskatta $|\mathcal{A}_d|$ introducerar vi funktionen $\rho(d)$, vilken betecknar antalet inkongruenta lösningar till ekvationen $F(n) \equiv 0 \bmod d$. Varje sådan restklass modulo d bidrar med $y/d + \theta$ element till $|\mathcal{A}_d|$, där $|\theta| \leq 1$. Det kan vi motivera heuristiskt med att n ligger i ett intervall av längd y och talen i restklasserna förekommer med avstånd d från varandra. Totalt får vi att

$$|\mathcal{A}_d| = \rho(d)\left(\frac{y}{d} + \theta\right)$$

där $|\theta| \leq 1$. När F har grad 2 eller mer är ρ i allmänhet svår att beräkna systematiskt men man kan visa att den är multiplikativ [HR, s. 17-18], till exempel genom att använda kinesiska restsatsen. Det innebär att det här är lämpligt att välja

$$X = y, \quad \omega_0(d) = \rho(d), \text{ varpå } |r_d| \leq \omega_0(d). \tag{2.3}$$

Av särskilt intresse är då F är en produkt av linjära heltalspolynom. I nästa avsnitt kommer vi låta $F(n) = n(n+2)$ och i Sats 3.3 låter vi $F(n) = n(n-2)$.

2.3 Två villkor på ω och ett första såll

Vi återger från [HR, s. 30] två villkor (R) och (Ω_0) som är uppfyllda för vissa $\mathcal{A}$, $\mathfrak{P}$ och ω. Båda används i Sats 2.1. Villkoren lyder

$$|R_d| \leq \omega(d), \text{ om } \mu(d) \neq 0,\ (d, \overline{\mathfrak{P}}) = 1, \tag{R}$$

samt

$$\omega(p) \leq A_0 \text{ för alla } p \text{ och för något } A_0 \geq 1. \tag{Ω_0}$$

Nu är vi redo att formulera Eratosthenes-Legendres såll och presentera en tillämpning. Formuleringen är hämtad från [HR, Sats 1.1].

Sats 2.1. *Vi har alltid $S(\mathcal{A}_q; \mathfrak{P}, z) = XW(z)\omega(q)/q + \theta \sum_{d|P(z)} |R_{qd}|$. Förutsatt att villkoren (R) och (Ω_0) håller gäller även $S(\mathcal{A}; \mathfrak{P}, z) = XW(z) + \theta(1 + A_0)^z$. I båda fall är $|\theta| \leq 1$.*

Vi utelämnar beviset och nöjer oss med att notera att det inleds med observationen

$$S(\mathcal{A}_q; \mathfrak{P}, z) = \sum_{a \in \mathcal{A}_q} \sum_{\substack{d|a \\ d|P(z)}} \mu(d) = \sum_{d|P(z)} \mu(d) \sum_{\substack{a \in \mathcal{A} \\ a \equiv 0 \bmod qd}} 1 = \sum_{d|P(z)} \mu(d) |\mathcal{A}_{qd}|, \tag{2.4}$$

eftersom den första inre summan är 0 om $(a, P(z)) > 1$ och annars 1 enligt Lemma A.1. Summan som involverar Möbiusfunktionen fungerar alltså som en indikator för de sökta talen. I den andra likheten har vi bytt summationsordning, använt $d \mid P(z)$ och $(q, P(z)) = 1$, vilket följer ur definitionen av $S(\mathcal{A}_q, \mathfrak{P}, z)$, så att $(q, d) = 1$. Den sista likheten är definitionen av $\mathcal{A}_{qd}$. Ett fullständigt bevis återfinns i appendix B.1. Som det påpekas i [HR, s. 31] blir Sats 2.1 endast användbar för små z i förhållande till X, eftersom feltermen är exponentiell i z. Trots feltermen lyckas Sats 2.1 ge en icke-trivial övre begränsning av antalet primtalstvillingar mindre än ett tal x.

Vi betraktar talföljden $\mathcal{A} = \{n(n+2) : n \leq x\}$ beskriven i avsnitt 2.2, med $y = x$ så att $X = x$. Vi väljer $\mathfrak{P} = \mathfrak{P}_1$ och ser från (2.3) att (R) är uppfyllt. En av faktorerna i $n(n + 2)$ måste vara delbar med p för att produkten ska vara det så att $\rho(p) \leq 2$, vilket tillsammans med (2.3) medför att (Ω_0) är uppfyllt med $A_0 = 2$. Vi kan räkna ut $\rho(p)$ explicit för alla primtal och ser att $\rho(2) = 1$, men $\rho(p) = 2$ för $p > 2$.

Om $(p, p + 2)$ är ett par av primtal med $z \leq p \leq x$ kommer $p(p + 2)$ och $P(z)$ vara relativt prima. Därmed har vi $|\{p \leq x : p + 2 \text{ är ett primtal}\}| \leq S(\mathcal{A}, \mathfrak{P}, z) + z$. Tillämpning av Sats 2.1 ger

$$|\{p \leq x : p + 2 \text{ är ett primtal}\}| \leq S(\mathcal{A}, \mathfrak{P}, z) + z \leq XW(z) + 3^z + z = xW(z) + 3^z + z.$$

Från Korollarium A.10 och $\omega(p) = \rho(p)$ följer $W(z) \ll 1/\log^2 z$. Vi låter $z = (\log x)/2$ så att

$$|\{p \leq x : p + 2 \text{ är ett primtal}\}| \ll \frac{x}{\log^2(\frac{1}{2}\log x)} + x^{(\log 3)/2} + \frac{\log x}{2} \ll \frac{x}{\log^2 \log x}$$

eftersom $(\log 3)/2 < 1$. Eftersom det ännu är okänt om det finns oändligt många primtalstvillingar skulle det vara mer intressant med en undre begränsning. Med hjälp av en variant av Bruns såll kan åtminstone undre begränsningar för par som nästan är primtalstvillingar härledas, se Sats 3.3.

3 Kombinatoriska såll

Eratosthenes-Legendres såll formulerar den algoritm som Eratosthenes använde i ett modernt språk. En nackdel med Eratosthenes-Legendres såll är att summan av feltermer är svår att kontrollera. Vi kommer i detta kapitel presentera den grundläggande idén bakom kombinatoriska såll och ge ett exempel i form av Bruns såll. De utgör ett sätt att hantera problemet med feltermerna och därmed erhålla starkare resultat än tidigare. Materialet är hämtat från [HR, avsnitt 2.1-2.4].

3.1 Introduktion till kombinatoriska såll

Vi följer här [HR, avsnitt 2.1]. I Eratosthenes-Legendres såll använder vi den första inre summan i (2.4) som en indikatorfunktion för att avgöra om ett element a räknas till $S(\mathcal{A};\mathfrak{P},z)$. Vi kallar nu den inre summan $\sigma_0((a,P(z)))$. Kombinatoriska såll generaliserar σ_0 genom att införa funktioner χ och σ, där σ definieras enligt

$$\sigma(n)=\sum_{d|n}\mu(d)\chi(d). \tag{3.1}$$

Fallet där χ är den konstanta funktionen 1 ger $\sigma_0(n)$.

Vårt syfte är nu att härleda undre och övre begränsningar för $S(\mathcal{A};\mathfrak{P},z)$ med hjälp av definitionen (3.1). Vi inleder med likheten

$$\mu(d)\chi(d)=\sum_{\delta|d}\mu\left(\frac{d}{\delta}\right)\sigma(\delta), \tag{3.2}$$

som följer genom att utveckla $\sigma(\delta)$ enligt (3.1) i högerledet, byta summationsordning och sedan använda Lemma A.1. Vi kan använda (3.2) för att se att

$$\sum_{d|P(z)}\mu(d)\chi(d)|\mathcal{A}_d|=\sum_{d|P(z)}|\mathcal{A}_d|\sum_{\delta|d}\mu\left(\frac{d}{\delta}\right)\sigma(\delta)=\sum_{\delta|P(z)}\sigma(\delta)\sum_{t|P(z)/\delta}\mu(t)|\mathcal{A}_{\delta t}|,$$

där vi i sista steget bytt summationsordning och skrivit $d=\delta t$. Idén är nu att dela upp summan ovan i de två fallen $\delta=1$ respektive $\delta>1$. Vi skriver $\mathfrak{P}^{(d)}$ för de tal i $\mathfrak{P}$ som inte delar d, byter variabeln δ till d och använder (2.4) på de inre summorna i högerledet ovan för att erhålla

$$S(\mathcal{A};\mathfrak{P},z)=\sum_{d|P(z)}\mu(d)\chi(d)|\mathcal{A}_d|-\sum_{1<d|P(z)}\sigma(d)S(\mathcal{A}_d;\mathfrak{P}^{(d)},z). \tag{3.3}$$

Här observerade vi även att $P(z)/d$ är produkten av alla tal i $\mathfrak{P}^{(d)}$ strikt mindre än z.

Vi fortsätter att följa [HR, avsnitt 2.1] för att härleda två hjälpekvationer som kommer behövas för att begränsa $S(\mathcal{A};\mathfrak{P},z)$. Först noterar vi att för kvadratfria d och ett $p\mid d$ kan vi dela upp d:s delare utefter om de delar p eller inte enligt

$$\sigma(d)=\sum_{\ell|d/p}\mu(\ell)\chi(\ell)+\sum_{\ell|d/p}\mu(p\ell)\chi(p\ell)=\sum_{\ell|d/p}\mu(\ell)(\chi(\ell)-\chi(p\ell)). \tag{3.4}$$

I det sista steget använde vi $\mu(p\ell)=-\mu(\ell)$ eftersom $(p,\ell)=1$. För att härleda den sista hjälpekvationen låter vi $z_1\le z$ och definierar $P_{z_1,z}$ som produkten av de tal i intervallet $[z_1,z)$ som tillhör $\mathfrak{P}$. För ett tal d skriver vi $q(d)$ för den minsta primtalsdelaren till d, med $q(1)=\infty$. Vi kan då genom att summera över alla möjliga delare till $P_{z_1,z}$ skriva

$$S(\mathcal{A};\mathfrak{P},z_1)=\sum_{t|P_{z_1,z}}\sum_{\substack{a\in\mathcal{A}\\(a,P(z_1))=1\\(a,P_{z_1,z})=t}}1=\sum_{t|P_{z_1,z}}\sum_{\substack{a\in\mathcal{A}_t\\(a,P(z)/t)=1}}1=\sum_{t|P_{z_1,z}}S(\mathcal{A}_t;\mathfrak{P}^{(t)},z), \tag{3.5}$$

där vi använt $P(z)=P(z_1)P_{z_1,z}$ och definitionen av $\mathfrak{P}^{(t)}$. Nu är vi redo att skriva om (3.3) på den form som kan ge oss övre och undre begränsningar. Vi använder först (3.4) och sätter $p\delta=d$, där p är det minsta primtalet i d, för att skriva andra summan i högerledet från (3.3) till

$$\sum_{\delta|P(z)}\sum_{\substack{p|P(z)\\p<q(\delta)}}S(\mathcal{A}_{p\delta};\mathfrak{P}^{(p\delta)},z)\sum_{\ell|\delta}\mu(\ell)(\chi(\ell)-\chi(p\ell)).$$

Notera att $p\delta>1$ eftersom p är ett primtal. Fallet $\delta=1$ ger inga problem eftersom $q(1)=\infty$. Om vi nu byter summationsordning ovan och skriver $\delta=t\ell$ erhåller vi

$$\begin{aligned}&\sum_{\ell|P(z)}\sum_{\substack{p|P(z)\\p<q(\ell)}}\mu(\ell)(\chi(\ell)-\chi(p\ell))\sum_{\substack{t|P(z)/\ell\\p<q(t)}}S(\mathcal{A}_{p\ell t};\mathfrak{P}^{(p\ell t)},z)\\&=\sum_{\ell|P(z)}\sum_{\substack{p|P(z)\\p<q(\ell)}}\mu(\ell)(\chi(\ell)-\chi(p\ell))S(\mathcal{A}_{p\ell};\mathfrak{P}^{(p\ell)},p),\end{aligned}$$

där det sista steget är (3.5) med p i rollen som z_1, $\mathcal{A}_{(p\ell)}$ i rollen som $\mathcal{A}$ och $\mathfrak{P}^{(p\ell)}$ som $\mathfrak{P}$. Här har vi använt att villkoren på p, ℓ, t medför att de är parvis relativt prima eftersom $P(z)$ är kvadratfri.

Till slut kan vi alltså skriva (3.3), med d i rollen som ℓ ovan, som

$$S(\mathcal{A}, \mathfrak{P}, z) = \sum_{d|P(z)} \mu(d)\chi(d)|\mathcal{A}_d| - \sum_{d|P(z)} \sum_{\substack{p|P(z) \\ p<q(d)}} \mu(d)(\chi(d) - \chi(pd))S(\mathcal{A}_{pd}; \mathfrak{P}, p).$$

Som [HR, s. 39] påpekar behövs inte indexet (pd) i $\mathfrak{P}$, eftersom det följer av $q(d) > p$ och att det tredje argumentet i $S(\mathcal{A}_{pd}; \mathfrak{P}, p)$ är p. Poängen med omskrivningen är att vi får en övre respektive en undre begränsning om tecknet på $\mu(d)(\chi(\ell) - \chi(p\ell))$ är konstant för de element som förekommer i summationen, se även [HR, s. 40]. Vi har alltså olikheten

$$\sum_{d|P(z)} \mu(d)\chi_2(d)|\mathcal{A}_d| \leq S(\mathcal{A}; \mathfrak{P}, z) \leq \sum_{d|P(z)} \mu(d)\chi_1(d)|\mathcal{A}_d|, \tag{3.6}$$

för två funktioner χ_1 och χ_2 givet att de uppfyller

$$(-1)^{v-1}\mu(d)(\chi_v(d) - \chi_v(pd)) \geq 0, \text{ för } pd \mid P(z),\ p < q(d), \tag{3.7}$$

där v är 1 eller 2. Om vi använder definitionen av R_d i (3.6) får vi en undre och övre begränsning för $S(\mathcal{A}; \mathfrak{P}, z)$ som

$$X \sum_{d|P(z)} \mu(d)\chi_2(d)\frac{\omega(d)}{d} - \sum_{d|P(z)} |\chi_2(d)||R_d| \leq S(\mathcal{A}, \mathfrak{P}, z) \leq X \sum_{d|P(z)} \mu(d)\chi_1(d)\frac{\omega(d)}{d} + \sum_{d|P(z)} |\chi_1(d)||R_d|. \tag{3.8}$$

Vi vill hitta en klass av funktioner χ_v som uppfyller (3.7), vilket motiverar följande definition [HR, s. 43].

Definition 3.1. Två funktioner $\chi_v, v = 1, 2$, definierade för alla $d|P(z)$ sägs ge upphov till ett kombinatoriskt såll om det för $v = 1, 2$, gäller att

1. $\chi_v(d) \in \{0, 1\}$ för alla $d|P(z)$,
2. $\chi_v(1) = 1$,
3. om $\chi_v(d) = 1$ gäller det att $\chi_v(t) = 1$ då $t \mid d$ och $d \mid P(z)$,
4. om $\chi_v(t) = 1$, $\mu(t) = (-1)^v$, $p < q(t)$ och $pt \mid P(z)$ gäller det att $\chi_v(pt) = 1$.

Lemma 3.1. *Om två funktioner $\chi_v, v = 1, 2$, genererar ett kombinatoriskt såll uppfyller de* (3.7).

Bevis. Antag att $pd \mid P(z)$ och att $p < q(d)$. Vi ska visa att $(-1)^{v-1}\mu(d)(\chi_v(d) - \chi_v(pd))$ inte kan vara negativt. Eftersom $\chi_v(d)$ antingen är lika med 0 eller 1 måste $\chi_v(d) - \chi_v(pd)$ vara lika med -1, 0 eller 1. Det finns därför bara två fall där $(-1)^{v-1}\mu(d)(\chi_v(d) - \chi_v(pd))$ kan vara negativt.

Det första fallet är om $\chi_v(d) = 0$, $\chi_v(pd) = 1$ och $\mu(d) = (-1)^{v+1}$. Eftersom $d \mid pd$ är emellertid $\chi_v(d) = 1$ om $\chi_v(pd) = 1$ enligt den tredje egenskapen i Definition 3.1. Detta fall kan därför inte inträffa. Det andra fallet är om $\chi_v(d) = 1$, $\chi_v(pd) = 0$ och $\mu(d) = (-1)^v$. Det motsäger emellertid den fjärde egenskapen i Definition 3.1. Beviset är därför klart. □

En omedelbar konsekvens av Lemma 3.1 är att att funktioner som ger upphov till kombinatoriska såll uppfyller (3.8). För ett kombinatoriskt såll har vi alltså direkt en övre och en undre begränsning av $S(\mathcal{A}; \mathfrak{P}, z)$.

3.2 Nya villkor på ω

Vi ska i nästa avsnitt undersöka Bruns såll, som är en instans av ett kombinatoriskt såll. Innan dess behöver vi några tekniska hjälpmedel som vi presenterar här [HR, avsnitt 1.4 och 2.3].

Vi börjar med att introducera ett nytt villkor (Ω_1) på ω. Villkoret säger

$$0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1} \tag{Ω_1}$$

för någon konstant $A_1 \geq 1$. Efter omordning av termerna erhåller vi det ekvivalenta uttrycket

$$1 \leq \frac{1}{1 - \omega(p)/p} \leq A_1. \tag{3.9}$$

Vi introducerar även $(\Omega_2(\kappa))$, som är en viktig generalisering av villkoret (Ω_0). Det säger att

$$\sum_{w \leq p < z} \frac{\omega(p) \log p}{p} \leq \kappa \log \frac{z}{w} + A_2, \quad 2 \leq w \leq z, \tag{$\Omega_2(\kappa)$}$$

för två konstanter $\kappa > 0$ och $A_2 \geq 1$. En tolkning av $(\Omega_2(\kappa))$ är att $\omega(p)$ i genomsnitt är begränsad av parametern κ. I själva verket gäller det att (Ω_0), som begränsar $\omega(p)$ för varje p, implicerar $(\Omega_2(\kappa))$ med $\kappa = A_2 = A_0$ [HR, Lemma 2.2]. Vi ser att Lemma A.7 medför ett liknande resultat, men där A_2 då blir en multipel av A_0.

Om både (Ω_1) och $(\Omega_2(\kappa))$ är uppfyllda har vi även en uppskattning av $W(z)$ enligt [HR, Lemma 2.3]

$$\frac{1}{W(z)} = \mathcal{O}(\log^{\kappa} z). \tag{3.10}$$

Jämför med Lemma A.10 som är ett specialfall.

3.3 Bruns såll

Bruns såll är ett exempel på ett kombinatoriskt såll och ger en metod för att hitta både en övre och en undre begränsning till $S(\mathcal{A}; \mathfrak{P}, z)$. Vi ska här presentera de funktioner χ_v som ger upphov till det. För det påminner vi om att $P_{z_1, z}$ definieras som produkten av alla primtal p i $\mathfrak{P}$ sådana att $z_1 \leq p < z$. Nästa steg är att vi inför tal z_n, $n = 0, 1, ..., r$ så att $2 = z_r < z_{r-1} < ... < z_1 < z_0 = z$ och låter b vara ett positivt heltal. Vi definierar nu för $v = 1, 2$,

$$\chi_v(d) = \begin{cases} 1 & \text{om } \nu((d, P_{z_n, z})) \leq 2b - v + 2n - 1,\ n = 1, 2, ..., r, \\ 0 & \text{annars,} \end{cases} \tag{3.11}$$

då $d \mid P(z)$. Detta begränsar antalet primtalsfaktorer hos de d vi inkluderar såväl som hur de är fördelade. Även om funktionerna kan tyckas invecklade tillåter de oss att begränsa storleken på summan av resttermer $\chi_v(d)|R_d|$.

Man kan visa att χ_v, $v = 1, 2$ uppfyller kraven för ett kombinatoriskt såll (se Lemma B.1). Vi presenterar nu det centrala resultatet [HR, Sats 2.1]. Ett nästan fullständigt bevis finns i appendix B.2.

Sats 3.2. *Låt b vara ett positivt heltal och λ en konstant som uppfyller $0 < \lambda e^{1+\lambda} < 1$. Antag vidare att villkoren $(\Omega_1), (\Omega_2(\kappa))$ och (R) är uppfyllda. Då gäller det att*

$$S(\mathcal{A}; \mathfrak{P}, z) \leq XW(z)\left(1 + 2\frac{\lambda^{2b+1}e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} e^{(2b+3)c_1/(\lambda \log z)}\right) + \mathcal{O}\left(z^{2b+2{,}01/(e^{2\lambda/\kappa}-1)}\right)$$

och

$$S(\mathcal{A}; \mathfrak{P}, z) \geq XW(z)\left(1 - 2\frac{\lambda^{2b}e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} e^{(2b+2)c_1/(\lambda \log z)}\right) + \mathcal{O}\left(z^{2b-1+2{,}01/(e^{2\lambda/\kappa}-1)}\right) \tag{3.12}$$

där

$$c_1 = \frac{A_2}{2}\left(1 + A_1\left(\kappa + \frac{A_2}{\log 2}\right)\right).$$

Anmärkning. De implicerade $\mathcal{O}$-konstanterna beror inte på b eller λ. De kan dock bero på κ, A_1 och A_2, konstanterna i villkoren (Ω_1) och $(\Omega_2(\kappa))$. I framtiden tillåts alla $\mathcal{O}$-konstanter bero på konstanterna A_i.

En förbättring jämfört med Eratosthenes-Legendres såll är den sista feltermen, där vi finner z i basen istället för exponenten. En annan anmärkningsvärd aspekt är att vi får en undre begränsning. Sådana är ofta svårare att erhålla än övre begränsningar, men ger ofta intressanta resultat. Vi kommer se ett exempel på det i nästa avsnitt.

3.4 Användning av Bruns såll på primtalstvillingar

Vi presenterar nu [HR, s. 62-63].

Sats 3.3. *Det finns ett oändligt antal positiva heltal n sådana att n och $n-2$ har högst 7 primtalsfaktorer.*

Anmärkning. Vi betraktar heltal n och $n-2$ istället för n och $n+2$ för att underlätta räkningarna i bevisets slutskede.

Bevis. Vi låter $\mathcal{A} = \{n(n-2) : n \leq x\}$ och $\mathfrak{P} = \mathfrak{P}_1$, mängden av alla primtal. Vi betraktar nu $S(\mathcal{A}; \mathfrak{P}, z)$. Detta uttryck betecknar antalet heltal $n(n-2)$, där $n \leq x$, sådana att $n(n-2)$, och därför även n och $n-2$, saknar primtalsfaktorer p sådana att $p < z$. Enligt vad vi såg i avsnitt 2.2 kan vi välja $X = x$ och

$$\omega(p) = \rho(p) = \begin{cases} 1 & \text{om } p = 2, \\ 2 & \text{om } p > 2. \end{cases}$$

I likhet med vad vi såg i avsnitt 2.3 beror det på att kongruensen $n(n-2) \equiv 0 \bmod p$ har exakt två lösningar, $n \equiv 0 \bmod p$ och $n \equiv 2 \bmod p$, som sammanfaller då $p = 2$. Alltså har vi att $\omega(p) \leq 2$, varför (Ω_0) är uppfyllt. Från avsnitt 3.2 är därför även $(\Omega_2(\kappa))$ uppfyllt, med $\kappa = A_2 = 2$. Vidare har vi att

$$1 \leq \frac{1}{1 - \omega(p)/p} \leq \frac{1}{1 - 2/3} \leq 3,$$

så (Ω_1) är uppfyllt med $A_1 = 3$. Slutligen är $|R_d| \leq \omega(d)$ enligt (2.3), så (R) är uppfyllt. Därför kan vi tillämpa Sats 3.2. Med $b = 1$ erhåller vi ur (3.12) att

$$S(\mathcal{A}; \mathfrak{P}, z) \geq xW(z) \left(1 - 2\frac{\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} e^{4c_1/(\lambda \log z)}\right) + \mathcal{O}\left(z^{1+2{,}01/(e^\lambda - 1)}\right).$$

För vårt val av ω är $W(z) = \frac{1}{2}\prod_{2<p<z}(1 - 2/p)$. Enligt Lemma A.10 är $W(z) \gg 1/\log^2 z$. Vi får därför att

$$S(\mathcal{A}; \mathfrak{P}, z) \geq \frac{x}{2} \prod_{2<p<z} \left(1 - \frac{2}{p}\right) \left(\left(1 - 2\frac{\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} e^{4c_1/(\lambda \log z)}\right) + \mathcal{O}\left(\frac{\log^2 z \cdot z^{1+2{,}01/(e^\lambda - 1)}}{x}\right)\right).$$

Vi vill säkerställa en positiv undre begränsning då $x \to \infty$. Det är möjligt om den sista resttermen begränsas, samt om

$$1 - 2\frac{\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} > 0. \tag{3.13}$$

Detta kommer medföra att faktorn

$$1 - 2\frac{\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} e^{4c_1/(\lambda \log z)}$$

förblir positiv då $z \to \infty$, eftersom faktorn $e^{4c_1/(\lambda \log z)}$ då går mot 1. För $\lambda = \log(1{,}288)$ uppfylls (3.13) såväl som satsens krav. Vi kan även finna en konstant u sådan att $1 + 2{,}01/(e^\lambda - 1) < u < 8$ för detta val av λ. Om vi låter $z = x^{1/u}$ får den sista resttermen formen $\mathcal{O}\left(\log^2 x/(u^2 x^\varepsilon)\right)$, där $\varepsilon > 0$. Eftersom $W(z) \gg 1/\log^2 z$ följer det att $S(\mathcal{A}; \mathfrak{P}, z) \to \infty$ då $x \to \infty$. Alltså finns det ett oändligt antal n sådana att samtliga primtalsfaktorer p hos n eller $n-2$ uppfyller $p \geq z = x^{1/u}$. Låter vi $\Omega(n)$ beteckna antalet primtalsfaktorer hos n (med multiplicitet) får vi alltså

$$x \geq n \geq z^{\Omega(n)} = x^{\Omega(n)/u} \text{ och } x \geq n - 2 \geq z^{\Omega(n-2)} = x^{\Omega(n-2)/u}.$$

Detta beror på att n respektive $n-2$ är produkter av $\Omega(n)$ respektive $\Omega(n-2)$ primtalsfaktorer som var och en är större än eller lika med z. Därmed kan vi dra slutsatsen att

$$\frac{\Omega(n)}{u} \leq 1 \text{ och } \frac{\Omega(n-2)}{u} \leq 1,$$

så att

$$\Omega(n) \leq u < 8 \text{ och } \Omega(n-2) \leq u < 8.$$

Eftersom både $\Omega(n)$ och $\Omega(n-2)$ är heltal måste de därför vara mindre än eller lika med 7. Det avslutar beviset. □

4 Selbergs såll

Efter Bruns arbete har flera andra såll konstruerats. Ett av de viktigaste är Selbergs såll, och de flesta av de resterande resultaten som presenteras här bygger på dess grundidé. I likhet med Bruns sållmetoder ger Selbergs motsvarigheter oss metoder för att finna övre och undre begränsningar till $S(\mathcal{A}_q;\mathfrak{P},z)$. Oftast sker det under samma sorts förutsättningar som tidigare. Det vanligaste är att vi sätter villkor på funktionen ω eller resttermerna $|R_d|$.

I det här kapitlet presenterar vi Selbergs såll i form av Sats 4.1, tillsammans med en härledning. Vi ser också hur satsen kan användas för att finna en övre gräns i studiet av primtalstvillingar. Vi avslutar med att introducera generaliserade villkor för funktionen ω och resttermerna $|R_d|$.

4.1 En grundläggande olikhet

Selbergs såll bygger på att vi för varje positivt kvadratfritt heltal d definierar ett reellt λ_d, med kravet att $\lambda_1 = 1$. Vi har då den grundläggande olikheten

$$S(\mathcal{A}_q;\mathfrak{P},z) \leq \sum_{a\in\mathcal{A}_q}\Bigg(\sum_{d|(a,P(z))}\lambda_d\Bigg)^2 = \sum_{a\in\mathcal{A}_q}\Bigg(\sum_{\substack{d|a\\ d|P(z)}}\lambda_d\Bigg)^2. \tag{4.1}$$

Denna har sin grund i att om $(a,P(z)) = 1$ har vi endast en term i den inre summan, nämligen $\lambda_1 = 1$. I alla andra fall ger termerna a ett icke-negativt bidrag eftersom vi kvadrerar en summa av reella tal. Idén kan synas enkel men har visat sig effektiv.

Det övergripande problemet är att välja lämpliga konstanter λ_d så att uppskattningen i (4.1) blir så bra som möjligt. Utan några begränsningar är problemet svårt, så det är vanligt att man förenklar situationen genom att införa en parameter $\xi > 1$, och sätta $\lambda_d = 0$ då $d \geq \xi$ [HR, s. 97]. I nästa avsnitt bygger vi vidare på (4.1) och inför samtidigt några av de viktigaste hjälpmedlen.

4.2 Beräkningar och ett första resultat

Ett naturligt val av parametern ξ är att sätta $\xi = z$, vilket är fallet som behandlas i [HR, avsnitt 3.1]. När undre begränsningar härleds är det dock sällan möjligt att välja variabeln z fritt. Därmed är det fördelaktigt om vi kan välja ξ fritt för att behålla viss flexibilitet [HR, s. 189]. Speciellt i samband med villkoret $R(1,\alpha)$ som definieras i avsnitt 4.5 kommer flexibiliteten som ξ ger vara användbar. Vi följer därför utvecklingen av teorin i [HR, avsnitt 6.1] och inleder med att utveckla kvadraten i (4.1) enligt

$$S(\mathcal{A}_q;\mathfrak{P},z) \leq \sum_{a\in\mathcal{A}_q}\sum_{\substack{d_1|a\\ d_1|P(z)}}\sum_{\substack{d_2|a\\ d_2|P(z)}}\lambda_{d_1}\lambda_{d_2},$$

för kvadratfria q med $(q,P(z)) = 1$ och $(q,\overline{\mathfrak{P}}) = 1$, som i avsnitt 2.1. Nyckelidén är nu att ändra summationsordning för att erhålla den övre begränsningen i form av en huvudterm och en restterm. Vi skriver därför om högerledet ovan till

$$\sum_{d_1|P(z)}\sum_{d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\sum_{\substack{a\in\mathcal{A}_q\\ [d_1,d_2]|a}}1.$$

Eftersom $[d_1,d_2] \mid P(z)$ och $(q,P(z)) = 1$ enligt villkoren på q i $S(\mathcal{A}_q;\mathfrak{P},z)$ från (2.2), är den innersta summan $|\mathcal{A}_{q[d_1,d_2]}|$ enligt kinesiska restsatsen. Vi sätter $D = [d_1,d_2]$ för att förenkla notationen.

Vi använder nu att $|\mathcal{A}_{qD}| = X\omega(qD)/qD + R_{qD}$ per definition och delar upp uttrycket ovan enligt

$$\frac{\omega(q)}{q}X\sum_{d_1|P(z)}\sum_{d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\frac{\omega(D)}{D} + \sum_{d_1|P(z)}\sum_{d_2|P(z)}\lambda_{d_1}\lambda_{d_2}R_{qD}, \tag{4.2}$$

där vi i första termen utnyttjat att ω är multiplikativ. Vi använder notationen från [HR, avsnitt 6.1] och betecknar den vänstra dubbelsumman Σ_1 och den högra Σ_2 så att vår uträkning har visat att

$$S(\mathcal{A}_q;\mathfrak{P},z) \leq X\frac{\omega(q)}{q}\Sigma_1 + \Sigma_2.$$

Eftersom Σ_1 multipliceras med X är den första termen relativt stor och vi väljer därför λ_d för att minimera den. Valet $\lambda_d = 0$ för $d \geq \xi$ minskar dock storleken av Σ_2 [HR, s. 189], eftersom inte alla delare till $P(z)$ bidrar till summan. Till skillnad från [HR, avsnitt 6.1] väntar vi med att specificera λ_d tills vi kan se vad det optimala valet är, men vi följer deras omskrivning av Σ_1.

Den fortsatta uträkningen inleds med observationen

$$\frac{\omega(D)}{D} = \frac{\omega(d_1)\omega(d_2)}{d_1 d_2}\frac{(d_1,d_2)}{\omega((d_1,d_2))}, \tag{4.3}$$

som följer ur multiplikativiteten hos ω, aritmetikens fundamentalsats och den elementära likheten $d_1d_2 = [d_1,d_2](d_1,d_2)$. Givetvis gäller inte likheten om $\omega((d_1,d_2)) = 0$, men i sådana fall är $\omega(D)$ också noll enligt multiplikativiteten, så vi kan bortse från detta fall.

För nollskilda $\omega(p)$ har vi även

$$\frac{p}{\omega(p)} = 1 + \frac{p(1-\frac{\omega(p)}{p})}{\omega(p)} =: 1 + \frac{1}{g(p)}, \tag{4.4}$$

där $g(p)$ definieras som den multiplikativa inversen av bråket i det mittersta uttrycket. Vi utvidgar g till en multiplikativ funktionen definierad på kvadratfria d enligt

$$g(d) = \frac{\omega(d)}{d}\prod_{p|d}\frac{1}{(1-\omega(p)/p)}, \tag{4.5}$$

jämför [HR, ekvation (1.4.17)]. Den uppmärksamma läsaren noterar att $g(p)$ inte är definierad om $\omega(p)/p = 1$ och vi kräver därför villkoret (Ω_1) som förhindrar det. Från (4.5) följer $g(d) = 0$ om och endast om $\omega(d) = 0$.

Vi förenklar nu andra faktorn i (4.3) med hjälp av Lemma A.3 enligt

$$\frac{(d_1,d_2)}{\omega((d_1,d_2))} = \prod_{p|(d_1,d_2)}\frac{p}{\omega(p)} = \prod_{p|(d_1,d_2)}\left(1+\frac{1}{g(p)}\right) = \sum_{\ell|(d_1,d_2)}\frac{1}{g(\ell)} = \sum_{\substack{\ell|d_1\\ \ell|d_2}}\frac{1}{g(\ell)}. \tag{4.6}$$

Tillsammans med (4.3) kan (4.6) användas för att skriva om första summan Σ_1 i (4.2) till

$$\sum_{d_1|P(z)}{}' \sum_{d_2|P(z)}{}' \lambda_{d_1}\lambda_{d_2}\frac{\omega(d_1)\omega(d_2)}{d_1d_2}\sum_{\substack{\ell|d_1\\ \ell|d_2}}{}'\frac{1}{g(\ell)} = \sum_{\substack{\ell|P(z)\\ \ell<\xi}}{}'\frac{1}{g(\ell)}\Bigg(\sum_{\substack{d|P(z)\\ l|d<\xi}}\lambda_d\frac{\omega(d)}{d}\Bigg)^2. \tag{4.7}$$

I den yttre summan behöver vi endast ta hänsyn till $\ell < \xi$ eftersom $\ell \mid d$ annars medför att $d \geq \ell > \xi$ så att $\lambda_d = 0$. Symbolen $'$ betyder att vi endast summerar över heltal k med $\omega(k) \neq 0$.

Nu följer vi [HR, s. 121] för att finna optimala λ_d. Vi definierar y_ℓ som summan innanför kvadraten i (4.7) så att

$$\Sigma_1 = \sum_{\substack{\ell|P(z)\\ \ell<\xi}}{}'\frac{y_\ell^2}{g(\ell)}, \quad y_\ell = \sum_{\substack{d|P(z)\\ l|d<\xi}}\lambda_d\frac{\omega(d)}{d} \tag{4.8}$$

En beräkning, se appendix B.3.1, visar att kravet $\lambda_1 = 1$ är ekvivalent med

$$1 = \sum_{\substack{\ell<\xi\\ \ell|P(z)}}\mu(\ell)y_\ell = \sum_{\substack{\ell<\xi\\ \ell|P(z)}}{}'\frac{y_\ell}{\sqrt{g(\ell)}}\mu(\ell)\sqrt{g(\ell)}. \tag{4.9}$$

Cauchy-Schwarz olikhet och (4.8) visar nu att högerledet ovan är mindre än $\Sigma_1 \cdot G_1(\xi,z)$, där

$$G_k(\xi,z) := \sum_{\substack{\ell<\xi\\ \ell|P(z)\\ (\ell,k)=1}}\mu^2(\ell)g(\ell). \tag{4.10}$$

Vi betecknar $G_1(\xi, z)$ med $G(\xi, z)$ och har då en undre begränsning av Σ_1 som $1/G(\xi, z)$. De optimala y_ℓ väljs så att Cauchy-Schwarz olikhet ger likhet, det vill säga så att alla $y_\ell/\sqrt{g(\ell)}$ är multiplar av $\mu(\ell)\sqrt{g(\ell)}$ för alla ℓ, med samma proportionalitetskonstant. Tillsammans med (4.9) visar detta att $y_\ell = g(\ell)\mu(\ell)/G(\xi, z)$, vilket medför att

$$\lambda_d = \frac{\mu(d)}{\prod_{p|d}(1 - \omega(p)/p)} \frac{G_d(\xi/d, z)}{G(\xi, z)}, \tag{4.11}$$

samt $|\lambda_d| \leq 1$. Detaljerna återfinns i appendix B.3.1. Med hjälp av denna observation kan vi hitta en övre begränsning för Σ_2, enligt metoden i [HR, avsnitt 6.1], genom att ta absolutbelopp i (4.2). Vi ser därför att

$$\Sigma_2 \leq \sum_{\substack{d_1|P(z) \\ d_1<\xi}} \sum_{\substack{d_2|P(z) \\ d_2<\xi}} |R_{q[d_1,d_2]}| \leq \sum_{\substack{D<\xi^2 \\ D|P(z)}} |R_{qD}| \sum_{\substack{d_1,d_2 \\ [d_1,d_2]=D}} 1. \tag{4.12}$$

Vi har i den första summan använt att den minsta gemensamma multipeln av två delare till $P(z)$ måste dela $P(z)$, samt vara mindre än ξ^2 på grund av storleksbegränsningarna på d_1, d_2. Vi tar mellan andra och tredje summan bort kravet $d_1, d_2 < \xi$ vilket ger olikhet. Vi beräknar den innersta summan till $3^{\nu(D)}$ med hjälp av ett kombinatoriskt argument. För att bilda två tal vars minsta gemensamma multipel är precis D har vi för varje primtalsfaktor i D precis tre val. Vi kan antingen låta den ingå i d_1, d_2, eller båda. Vi får alltså följande sats [HR, Sats 6.1].

Sats 4.1. *Om (Ω_1) är uppfyllt och $\xi > 1$ har vi den övre begränsningen*

$$S(\mathcal{A}_q; \mathfrak{P}, z) \leq \frac{\omega(q)}{q} \frac{X}{G(\xi, z)} + \sum_{\substack{d<\xi^2 \\ d|P(z)}} 3^{\nu(d)}|R_{qd}|. \tag{4.13}$$

Sats 4.1 gäller under svaga förutsättningar vilket gör den användbar. Eftersom vi inte har något villkor på storleken av R_{qd} kan dock inte summan i (4.13) förenklas direkt. Vi kommer längre fram se att resttermen kan uppskattas väl om ett villkor $(R(\kappa, \alpha))$, som är mindre strikt än (R), är uppfyllt. Utöver resttermen kommer vi även uppskatta $G(\xi, z)$ nedifrån för att kunna använda Sats 4.1 i praktiken. Vi avslutar med att notera att en alternativ, svagare form på resttermen i (4.13) är

$$\sum_{\substack{d<\xi^2 \\ (d,\overline{\mathfrak{P}})=1}} \mu^2(d)3^{\nu(d)}|R_{qd}|, \tag{4.14}$$

eftersom alla d som delar $P(z)$ uppfyller att $(d, \overline{\mathfrak{P}}) = 1$ samt är kvadratfria, jämför [HR, ekvation (3.1.14)].

4.3 Aritmetiska primtalsföljder

Vi avviker tillfälligt från undersökningen av Selbergs såll för att studera ett exempel av särskilt intresse i samband med primtalstvillingar [HR, exempel 5, avsnitt 1.3]. Vi låter $\mathcal{A} = \{ap+h : p \leq x\}$ med a, h heltal, $(a, h) = 1$ och $x \geq 1$ reellt. När vi behöver uppskatta $|\mathcal{A}_d|$ kommer alltid $(a, d) = 1$ och vi kommer alltid använda $\mathfrak{P} = \mathfrak{P}_h$ så att vi endast undersöker d med $(d, ah) = 1$.

Vi har $|\mathcal{A}_d| = |\{ap + h : p \leq x, p \equiv -ha^{-1} \bmod d\}| = \pi(x; d, -ha^{-1})$, där a^{-1} är den multiplikativa inversen modulo d till a. Eftersom $(d, ah) = 1$ växer $|\mathcal{A}_d|$ obegränsat då $x \to \infty$, enligt Dirichlets sats [D, kapitel 1]. En kvantitativ form av Dirichlets sats i [D, kapitel 22] ger $\operatorname{li} x/\phi(d)$ som en uppskattning för $\pi(x; d, -ha^{-1})$.

Om vi sätter $d = 1$ får vi uppskattningen $X = \operatorname{li} x$. Vi får även naturliga val för ω_0, och i förlängningen ω. Totalt får vi

$$X = \operatorname{li} x, \ \omega(d) = \begin{cases} \frac{d}{\phi(d)} & \text{om } (d, h) = 1, \\ 0 & \text{annars.} \end{cases} \tag{4.15}$$

Speciellt är ω multiplikativ eftersom ϕ är det. Vi ser också att $\omega(p) = p/(p-1)$. Nu följer också $R_d = \pi(x; d, -ha^{-1}) - \operatorname{li} x/\phi(d)$ om d är kvadratfri och $(d, ah) = 1$. Feltermen beror på både d och h vilket inte kommer vara önskvärt i framtiden. Vi definierar därför

$$E(x, q) = \max_{2 \le y \le x} \max_{(c,q)=1} \left| \pi(y; q; c) - \frac{\operatorname{li} y}{\phi(q)} \right|, \tag{4.16}$$

så att

$$|R_d| \le E(x, d), \ \ d \text{ kvadratfritt}, \ (d, h) = 1.$$

4.4 Användning av Selbergs såll på primtalstvillingar

Vi ger nu ett exempel på hur Sats 4.1 kan användas i arbetet med primtalstvillingar, och följer i stort sett tillvägagångssättet i [HR, avsnitt 3.6-3.7].

Vi låter N och h vara positiva jämna heltal, och betraktar mängden $\mathcal{L} = \{p + h : p \le N\}$. Vi ser att $\mathcal{L}$ är ett specialfall av följden $\mathcal{A}$ vi studerade i avsnitt 4.3, med $a = 1$ och $x = N$. Då har vi enligt (4.15) att

$$\omega(p) = \begin{cases} \frac{p}{p-1} & \text{om } p \nmid h, \\ 0 & \text{annars.} \end{cases} \tag{4.17}$$

Låter vi $\xi = z$ i $G(\xi, z)$ har vi med $G(z, z) =: G(z)$ att

$$\frac{1}{G(z)} \le 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{1}{\log z} \left(1 + \mathcal{O}\left(\frac{1}{\log z}\right)\right). \tag{4.18}$$

För tillräckligt stora z följer olikheten av att vi begränsar $G(z)$ underifrån, se appendix B.3.2. För begränsade z är (4.18) trivial eftersom $G(z) \ge 1$ och vi därför kan välja en tillräckligt stor $\mathcal{O}$-konstant.

Den första produkten i (4.18) kallas ibland *primtalstvillingskonstanten* och har ett oändligt antal faktorer. Vi kan hantera frågan om konvergens av den oändlig produkten genom att ta logaritmen av den N:te delprodukten. På så sätt reducerar vi problemet till en fråga om konvergens av serier. Därefter Taylorutvecklar vi $\log(1-1/(p-1)^2)$ och låter $N \to \infty$. Produktens konvergens följer då av att serien $\sum_{n=1}^{\infty} 1/n^2$ är konvergent. Primtalstvillingskonstanten har beräknats vara approximativt lika med 0,6607 [W, avsnitt 3].

Sätter vi $q = 1$ och använder Sats 4.1 erhåller vi resultatet [HR, Sats 3.10]

$$S(\mathcal{A}; \mathfrak{P}_h, z) \le 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{X}{\log z} \left(1 + \mathcal{O}\left(\frac{1}{\log z}\right)\right) + \sum_{\substack{d<z^2 \\ (d,h)=1}} \mu^2(d) 3^{\nu(d)} |R_d|. \tag{4.19}$$

Summan av resttermerna är på formen (4.14).

För att motivera användandet av Sats 4.1 måste vi verifiera att (Ω_1) är uppfyllt. Därför observerar vi att villkoret på $\omega(p)$ är trivialt sant om $p \mid h$. Om $p \nmid h$ är $p \ge 3$ eftersom h är jämnt. Det följer då från $1/(p-1) \le 1/2$ att (Ω_1) är uppfyllt med $A_1 = 2$.

Vi använder detta på $\mathcal{L}$ och får då Sats 4.2, som ger en övre begränsning av antalet primtalspar $(p, p+h)$ där $p \le N$ [HR, Sats 3.11].

Sats 4.2. *Då $N \to \infty$ gäller det att*

$$|\{p : p \le N, p + h = p'\}| \le 8 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{N}{\log^2 N} \left(1 + \mathcal{O}\left(\frac{\log\log N}{\log N}\right)\right).$$

I beviset behöver vi begränsa resttermerna, vilket vi gör med hjälp av följande resultat [HR, Lemma 3.5]. Det är också därför vi skriver dem på formen (4.14).

Lemma 4.3. *Låt k vara ett positivt heltal. Antag att*

$$k \le \log^A x$$

och att $E(x,q)$ är definierat som i (4.16). Givet en positiv konstant U finns det en positiv konstant C så att

$$\sum_{d<x^{1/2}/(k\log^C x)} \mu^2(d)3^{\nu(d)}E(x,dk) = \mathcal{O}\left(\frac{x}{\phi(k)\log^U x}\right).$$

Den av $\mathcal{O}$-notationen implicerade konstanten, liksom C, beror på U och A.

Lemma 4.3 är en version av Bombieris sats. Satsen behandlats i exempelvis [D, kapitel 28], om än i ett annat utförande.

4.5 Tvillingprimtal och fler villkor

Det är nu lämpligt att introducera två nya villkor [HR, s. 142, 219]. Vi inleder med $(\Omega_2(\kappa, L))$, som är en utökning av $(\Omega_2(\kappa))$ från avsnitt 3.2, men med krav på undre begränsning. Villkoret lyder

$$-L \leq \sum_{w\leq p<z} \frac{\omega(p)\log p}{p} - \kappa \log\frac{z}{w} \leq A_2,\ 2\leq w\leq z \qquad (\Omega_2(\kappa, L))$$

för något $L \geq 1$. Villkoret är ett viktigt verktyg i härledningen av undre begränsningar.

Det andra villkoret vi introducerar behandlar istället resttermen R_d, och är svagare än (R). Det är dock användbart eftersom det ger en begränsning på medelvärdet av resttermerna, vilket ofta är det enda som behövs. Vi definierar villkoret $(R(\kappa,\alpha))$ enligt

$$\sum_{\substack{d<X^\alpha/(\log X)^{A_4}\\ (d,\mathfrak{P})=1}} \mu^2(d)3^{\nu(d)}|R_d| \leq A_5\frac{X}{\log^{\kappa+1} X},\ X\geq 2, \qquad (R(\kappa,\alpha))$$

där A_4 och A_5 är några konstanter. Notera att samma κ förekommer i både $(\Omega_2(\kappa, L))$ och i $R(\kappa,\alpha)$, men det kommer inte medföra någon inskränkning i de fall vi studerar.

Vi visar nu att följden $\mathcal{L} = \{p+h : p\leq N\}$ från avsnitt 4.3, med $\mathfrak{P} = \mathfrak{P}_h$, uppfyller båda villkor. Lemma 4.3, med $U = 2$ visar direkt att $(R(\kappa,\alpha))$ är uppfyllt med några konstanter A_4, A_5, $\alpha = 1/2$ och $\kappa = 1$. Genom att välja U annorlunda hade vi kunnat välja vilket κ vi vill, men för våra ändamål är detta tillräckligt.

Om vi använder $1/(p-1) = 1/p + 1/(p(p-1))$, Lemma A.7, tillsammans med definitionen (4.17) av ω, ser vi att den övre begränsningen för $(\Omega_2(1, L))$ håller för något $A_2 = \mathcal{O}(1)$. För den undre begränsningen noterar vi att summanden i $(\Omega_2(\kappa, L))$ precis är summanden i Lemma A.7, med undantag för en term av storleken $(\log p)/p^2$, vars summa konvergerar, samt ett antal uteslutna termer. De termer som uteslutits är de där p delar h, alltså maximalt $\nu(h) = \mathcal{O}_h(1)$ termer. Totalt får vi en undre begränsning med $L = \mathcal{O}_h(1)$. Begränsningen kan göras mer specifik i h, men för oss räcker resultaten ovan.

5 Det linjära sållet

Linjära såll är de såll som kan användas för att undersöka följder $\mathcal{C}$, tillsammans med något $\mathfrak{P}$, som uppfyller $(\Omega_2(1, L))$. Vi såg i avsnitt 4.5 att följden $\mathcal{L}$ kopplad till primtalstvillingarna är en sådan följd, vilket är anledningen till att linjära såll är av intresse. Vi inleder med att presentera två funktioner f och F som kommer vara användbara för teorin om linjära såll och presenterar sedan två satser, utan bevis, som kommer vara nödvändiga i beviset av Chens sats.

5.1 Funktionerna f och F

Vi följer nedan [HR, avsnitt 8.2], med undantag för små förändringar i notation, för att definiera och undersöka funktionerna f och F. Vi inleder med att betrakta differentialekvationer för två funktioner $\eta(u)$, $\rho(u)$, enligt

$$\begin{aligned} &\eta(u) = \frac{1}{u},\ \rho(u) = 1, \quad 0<u\leq 2,\\ &(u\eta(u))' = \eta(u-1),\ (u-1)\rho'(u) = -\rho(u-1), \quad u\geq 2. \end{aligned} \tag{5.1}$$

Vi anmärker att η och ρ existerar unikt, vilket framgår implicit i [HR, avsnitt 8.2]. Vi definierar nu

$$\begin{aligned} F(u) &= e^{\gamma}\left(\eta(u) + \frac{\rho(u)}{u}\right), \quad u > 0, \\ f(u) &= e^{\gamma}\left(\eta(u) - \frac{\rho(u)}{u}\right), \quad u > 0. \end{aligned} \tag{5.2}$$

Då $0 < u \leq 2$ kan vi se direkt från definitionen att $f(u) = 0$ och $F(u) = 2e^{\gamma}/u$. För att undvika längre avvikelser från studiet av primtalstvillingar nöjer vi oss med att formulera de egenskaper hos f och F som krävs för beviset av Chens sats utan bevis och hänvisar den intresserade läsaren till [HR, avsnitt 8.2] för detaljer.

Två viktiga egenskaper hos f och F är att f växer monotont från 0 till 1 och att F avtar monotont mot 1. Man kan också med mer information om η, ρ, visa att konvergensen mot 1 sker exponentiellt så att $f(u) = 1 + \mathcal{O}(e^{-u})$ och $F(u) = 1 + \mathcal{O}(e^{-u})$. Från definitionen av f, F följer även

$$\begin{aligned} \int_{u_1}^{u} f(t-1)dt &= uF(u) - u_1F(u_1), \\ \int_{u_1}^{u} F(t-1)dt &= uf(u) - u_1f(u_1), \end{aligned} \tag{5.3}$$

för $2 \leq u_1 \leq u$. Nyckeln till beviset är att se att vi för $u \geq 2$ har $(uF(u))' = f(u-1)$ och $(uf(u))' = F(u-1)$.

Den sista egenskapen vi behöver är en medelvärdesegenskap som vi kommer använda i Chens sats för att kontrollera beteendet hos f och F mellan två närliggande punkter. För godtyckliga $0 < u_1 < u_2$ har vi nämligen

$$\begin{aligned} 0 < F(u_1) - F(u_2) &\leq F(u_1)\frac{u_2 - u_1}{u_1}, \\ 0 < f(u_2) - f(u_1) &\leq 2e^{\gamma}\frac{u_2 - u_1}{u_1}. \end{aligned} \tag{5.4}$$

Vi noterar här att om u_1 väljs större än exempelvis 1 är $F(u_1) = \mathcal{O}(1)$ på grund av monotoniciteten.

5.2 Linjära sållresultat

Nu är vi redo att formulera de två resultat om linjära såll från [HR, avsnitt 8.3-8.4] som vi kommer använda i beviset av Chens sats. I båda resultaten kräver vi utöver $(\Omega_2(1, L))$ även (Ω_1). För att bevisa de två resultaten krävs en utvidgning av Selbergs såll från kapitel 4, som låter oss erhålla undre begränsningar. Härledningen av det utvidgade sållet sker genom att introducera funktioner liknande η och ρ ovan, men framställningen blir teknisk och hamnar utanför rapportens omfång. Vi presenterar därför resultaten nedan utan bevis. Det första resultatet är [HR, Sats 8.3].

Sats 5.1. *Låt (Ω_1) och $(\Omega_2(1, L))$ vara uppfyllda. Om $\xi \geq z$, eller $1 < \xi < z$ med $z \ll \xi^{\lambda}$ för något λ, har vi*

$$\begin{aligned} S(\mathcal{A}_q; \mathfrak{P}, z) &\leq \frac{\omega(q)}{q}XW(z)\left(F\left(\frac{\log \xi^2}{\log z}\right) + C_1\frac{L}{(\log \xi)^{1/14}}\right) + \sum_{\substack{n<\xi^2 \\ n|P(z)}} 3^{\nu(n)}|R_{qn}|, \\ S(\mathcal{A}_q; \mathfrak{P}, z) &\geq \frac{\omega(q)}{q}XW(z)\left(f\left(\frac{\log \xi^2}{\log z}\right) - C_2\frac{L}{(\log \xi)^{1/14}}\right) - \sum_{\substack{n<\xi^2 \\ n|P(z)}} 3^{\nu(n)}|R_{qn}|, \end{aligned} \tag{5.5}$$

där vi explicit har skrivit ut $\mathcal{O}$-konstanten C_i. Som vanligt tillåts den bero på alla A_i och α, men inte på L. Om $\xi < z$ måste konstanten C_1 tillåtas bero på λ.

Med medelvärdesegenskapen (5.4) kan vi härleda en utvidgning av Sats 5.1 utan resttermer [HR, Sats 8.4]. Detta kräver dock att vi introducerar villkoret $R(1, \alpha)$. Nyckeln till beviset är att sätta $\xi^2 = X^{\alpha}/(\log X)^{A_4}$, använda $(R(1, \alpha))$, (3.10) och sedan tillämpa (5.4).

Sats 5.2. *Låt* $(\Omega_1), (\Omega_2(1, L))$ *och* $(R(1, \alpha))$ *vara uppfyllda. Om* $z \le X$ *existerar det ett* X_0 *så att vi för* $X \ge X_0$ *har*

$$\begin{aligned} S(\mathcal{A}; \mathfrak{P}, z) &\le XW(z)\Big(F\Big(\alpha\frac{\log X}{\log z}\Big) + C\frac{L}{(\log X)^{1/14}}\Big) \\ S(\mathcal{A}; \mathfrak{P}, z) &\ge XW(z)\Big(f\Big(\alpha\frac{\log X}{\log z}\Big) - C\frac{L}{(\log X)^{1/14}}\Big) \end{aligned} \tag{5.6}$$

där konstanten C *tillåts bero på* A_i *och* α *men inte* L. *Konstanten* X_0 *kan bero på* A_4 *och* α.

6 Chens sats

Vi ska nu formulera och presentera ett bevis av Chens sats [HR, Sats 11.1]. Satsen utgör i ett specialfall den i sitt slag närmaste approximationen av primtalstvillingsförmodan.

6.1 Formulering av Chens sats

Sats 6.1 (Chens sats)**.** *Låt* h *vara ett nollskilt jämnt heltal. Då finns en konstant* N_0 *så att om* $N > N_0$ *gäller det att*

$$|\{p : p \le N, p + h \in P_2\}| > 0{,}66 \prod_{p>2}\Big(1 - \frac{1}{(p-1)^2}\Big) \prod_{2<p|h} \frac{p-1}{p-2}\frac{N}{\log^2 N}. \tag{6.1}$$

Som vi formulerat satsen beror N_0 på h. Från Sats 6.1 följer omedelbart Sats 1.1.

Bevis av Sats 1.1. Välj ett jämnt $h \ne 0$. Enligt (6.1) har vi att

$$|\{p : p \le N, p + h \in P_2\}| \to \infty \text{ då } N \to \infty,$$

vilket avslutar beviset. □

Låter vi $h = 2$ ser vi att Chens sats ligger mycket nära primtalstvillingsförmodan. Det fullständiga beviset till satsen använder en omfattande mängd begrepp och resultat och att presentera dem alla ligger utanför rapportens omfång. Vi kommer i första hand fokusera på de aspekter som knyter an till den sållteori vi tidigare har behandlat.

Nedan följer vi beviset i [HR, kapitel 11], som dock behandlar Chens sats i en version som ligger nära Goldbachs förmodan. Bevisen liknar varandra, men en del detaljer behöver anpassas till den nya situationen med primtalstvillingar.

6.2 Inledande uppskattningar

Vi arbetar med följden $\mathcal{L} = \{p + h : p \le N\}$ och låter $\mathfrak{P} = \mathfrak{P}_h$. Det första steget i beviset av Sats 6.1 är att introducera en viktad summa W, som till varje element $a = p + h$ som vi summerar över tillskriver en vikt w_a som är högst 1. Vi vill också att de element vars vikter är positiva högst kan ha två primtalsfaktorer. Meningen med det är att vi då kan dra slutsatsen att $|\{p : p \le N, p + h \in P_2\}| \ge W$. Detta beror på att vänsterledet summerar *alla* element $p + h \in P_2$ där $p \le N$ med vikten 1. Summan W innehåller som *mest* alla element i vänsterledet, men med en vikt som eventuellt är mindre, tillsammans med andra element vars vikt är negativ.

Vi ska visa att den viktade summan

$$W = \sideset{}{'}\sum_{\substack{p+h \le N \\ (p+h,\, P(N^{1/10}))=1}} \Bigg(1 - \frac{1}{2}\sum_{\substack{N^{1/10} \le p_1 < N^{1/3} \\ p_1|p+h,\, p_1 \in \mathfrak{P}_h}} 1 - \frac{1}{2}\sum_{\substack{N^{1/10} \le p_1 < N^{1/3} \\ p_1|p+h,\, p_1 \in \mathfrak{P}_h}} \sum_{\substack{N^{1/3} \le p_2 < (N/p_1)^{1/2} \\ p_2|p+h,\, p_2 \in \mathfrak{P}_h \\ p+h = p_1p_2p_3}} 1\Bigg) \tag{6.2}$$

uppfyller våra villkor, så när som på två undantag. Symbolen $'$ betyder att vi enbart summerar över element p sådana att $(p + h, h) = 1$, det vill säga $(p, h) = 1$. Den betyder också att talen $p + h$ är kvadratfria med avseende på alla primtal som uppfyller villkoren i de inre summorna.

Uttrycket innanför parentesen är den vikt w_a, som hör till varje element $a = p + h$ som vi summerar över. Vi ser direkt att en positiv vikt måste vara lika med 1 eller 1/2. Det återstår att visa att de element vars vikter är positiva har högst två primtalsfaktorer. Vi undersöker de båda fallen $w_a = 1$ och $w_a = 1/2$ separat.

Om $w_a = 1$ är de två inre summorna i (6.2) tomma, och då saknar $p + h$ primtalsfaktorer mindre än $N^{1/3}$. Möjligheten $p + h = N$ är uppfylld för högst ett element. I annat fall kan $p + h$ ha högst två primtalsfaktorer, eftersom $p + h \leq N$.

Om $w_a = 1/2$ måste den första summan innehålla exakt en term, samtidigt som den inre summan i den sista dubbelsumman måste vara tom. Det betyder att $p+h$ har *exakt* en primtalsfaktor p_1 sådan att $N^{1/10} \leq p_1 < N^{1/3}$, och vi skriver $p + h = p_1 m$, med $(m, P(N^{1/3})) = 1$. Det innebär att m kan ha antingen en eller två primtalsfaktorer. Vi ska visa att förutom undantaget då m är en primtalskvadrat $m = q^2$, där $q = (N/p_1)^{1/2}$, kan det senare fallet inte inträffa.

Skriv därför $m = p_2 p_3$, med $p_3 > p_2$. Eftersom den inre summan är tom måste $p_2 \geq (N/p_1)^{1/2}$. Men då får vi att $p_2 p_3 > N/p_1$ och därmed att $p + h > N$. Detta är uppenbarligen en motsägelse, och alltså har $p + h$ med ett undantag högst två primtalsfaktorer om dess vikt är lika med 1/2.

Vi såg att det finns två undantag från regeln att ett element i W med positiv vikt måste höra till P_2: Dels om $p + h = N$, dels om $p + h = p_1 q^2$ där $q = (N/p_1)^{1/2}$ är ett primtal. Dessa två undantag orsakar inga problem, eftersom de endast introducerar en felterm $\mathcal{O}(1)$.

Högerledet i (6.2) förenklas om vi ändrar den yttre summationsgränsen till $p \leq N$. Det kommer medföra att en felterm $\mathcal{O}_h(1)$ läggs till. Därefter multiplicerar vi in i parentesen i den modifierade versionen av (6.2) och erhåller då tre summor. I var och en av dessa undersöker vi hur stor felterm som uppkommer om vi även avlägsnar de restriktioner som impliceras av symbolen $'$. Den kommer att få formen $\mathcal{O}(N^{9/10})$.

I den första summan lägger vi som mest till $\mathcal{O}_h(1)$ termer, eftersom kravet $(p, h) = 1$ har hävts, och $\sum_{p|h} 1 = \mathcal{O}_h(1)$. I den andra summan betraktar vi för varje p_1 en följd av N på varandra följande heltal och undersöker vilka som är delbara med p_1^2, eftersom kravet på kvadratfrihet hävts. Avlägsnandet av $'$ ger därför som mest ett bidrag på $N/p_1^2 + 1$ för varje p_1. I den tredje summan resonerar vi på liknande sätt, men med $p_1 p_2^2$. Totalt får vi ett bidrag på (jämför [HR, s. 322])

$$\mathcal{O}_h(1) + \mathcal{O}\left(\sum_{N^{1/10} \leq p_1 < N^{1/3}} \left(\frac{N}{p_1^2} + 1 \right) \right) + \mathcal{O}\left(\sum_{N^{1/10} \leq p_1 < N^{1/3}} \sum_{N^{1/3} \leq p_2 < (N/p_1)^{1/2}} \left(\frac{N}{p_1 p_2^2} + 1 \right) \right) = \mathcal{O}(N^{9/10}). \quad (6.3)$$

Eftersom h är fixt kan den första feltermen absorberas i högerledet utan problem. Detsamma gäller för de två undantagen som nämndes ovan. Den andra feltermen kan delas upp i två summor där den första kan uppskattas med en integraljämförelse. Vi får att den är $\mathcal{O}(N^{9/10})$ eftersom $N^{1/10}$ är den undre summationsgränsen. Den andra summan är $\mathcal{O}(N^{1/3})$. I den sista termen i (6.3) kan vi resonera på ett liknande sätt med p_2^2, men eftersom summan är dubbel måste vi även notera att $p_1 \geq N^{1/10}$. Den sista feltermen blir då $\mathcal{O}(N^{9/10})$.

Om vi även byter summationsordning och begränsar den tredje summan ovanifrån i den modifierade versionen av (6.2) får vi till slut, se appendix B.4.1, att

$$|\{p : p \leq N, p + h \in P_2\}| \geq S(\mathcal{L}, \mathfrak{P}_h, N^{1/10}) - \frac{1}{2} \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \in \mathfrak{P}_h}} S(\mathcal{L}_{p_1}, \mathfrak{P}_h, N^{1/10}) - \frac{1}{2} \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \in \mathfrak{P}_h}} \sum_{\substack{N^{1/3} \leq p_2 < (N/p_1)^{1/2} \\ p_2 \in \mathfrak{P}_h}} \left| \left\{ p_3 : p_3 \leq \frac{N}{p_1 p_2}, p_1 p_2 p_3 - h = p \right\} \right| + \mathcal{O}(N^{9/10}). \quad (6.4)$$

6.3 Begränsning av termerna

Vi begränsar nu termerna i högerledet i (6.4). Från avsnitt 4.4 och 4.5 vet vi att $\mathcal{L}$ uppfyller (Ω_1), $(\Omega_2(1, L))$ och $R(1, \alpha)$. Vi har $L = \mathcal{O}_h(1)$, $\alpha = 1/2$ och inget A_i beror på N. Eftersom vi fixerat

h tillåter vi implicerade konstanter att bero på h utan att markera det explicit. Vi poängterar att inga implicerade konstanter tillåts bero på N.

Vi följer [HR, avsnitt 11.2] och begränsar den första termen i (6.4) med Sats 5.2 och den andra med Sats 5.1 för tillräckligt stora N. Vi får för den första termen

$$S(\mathcal{L};\mathfrak{P}_h, N^{1/10}) \geq XW(N^{1/10})\left(f\left(\frac{5\log X}{\log N}\right) + \mathcal{O}\left(\frac{1}{(\log X)^{1/14}}\right)\right) \tag{6.5}$$

där $X = \mathrm{li}\ N$. Att begränsa den andra termen, det vill säga den första summan, är mer intrikat. Vi följer tillvägagångssättet i [HR, Sats 9.1] som inleds med att sätta $\xi^2 = X^{1/2}/(\log X)^{A_4}$. Varje enskild term begränsas med Sats 5.1 där ξ^2/p_1 används för det som kallas ξ^2 i satsen. Eftersom $p_1 \leq N^{1/3}$ är $\xi^2/p_1 \geq X^{1/6}/(\log X)^{A_4}$, vilket är större än $w := N^{1/10}$ för stora N så att Sats 5.1 kan tillämpas, med w i rollen som z och $\lambda = 2$. Vi får då om vi sätter $y = N^{1/3}$ att

$$\begin{aligned}\sum_{\substack{w\leq p_1<y\\ p_1\in\mathfrak{P}_h}} S(\mathcal{L}_{p_1};\mathfrak{P}_h, N^{1/10}) \leq &\sum_{\substack{w\leq p_1<y\\ p_1\in\mathfrak{P}_h}} \frac{\omega(p_1)}{p_1} XW(N^{1/10})\left(F\left(\frac{\log(\xi^2/p_1)}{\log w}\right) + \mathcal{O}\left(\frac{1}{(\log(\xi/\sqrt{p_1}))^{1/14}}\right)\right)\\ &+ \sum_{\substack{w\leq p_1<y\\ p_1\in\mathfrak{P}_h}} \sum_{\substack{n<\xi^2/p_1\\ n\mid P(w)}} 3^{\nu(n)}|R_{p_1 n}|,\end{aligned} \tag{6.6}$$

Eftersom $\xi^2 \approx X^{1/2}$ använder vi (5.4), samt definitionen av ξ för att skriva

$$F\left(\frac{\log(\xi^2/p_1)}{\log w}\right) = F\left(\frac{\log(X^{1/2}/p_1)}{\log w}\right) + \mathcal{O}\left(\frac{1}{(\log X)^{1/2}}\right) \tag{6.7}$$

för tillräckligt stora X, se [HR, s. 245] för detaljer. Notera att exponenten $1/2$ kan väljas godtyckligt nära 1, men $1/2$ är tillräckligt för våra ändamål. Vi noterar även

$$\log(\xi/\sqrt{p_1}) \gg \log X^{1/6} - \log\log X^{A_4} \gg \log X. \tag{6.8}$$

Vi använder (6.7) och (6.8) för att skriva de två första termerna i högerledet från (6.6) som

$$XW(N^{1/10})\Bigg(\sum_{\substack{w\leq p_1<y\\ p_1\in\mathfrak{P}_h}} \frac{\omega(p_1)}{p_1} F\left(\frac{\log(X^{1/2}/p_1)}{\log w}\right) + \mathcal{O}\Bigg(\frac{1}{(\log X)^{1/14}} \sum_{\substack{w\leq p_1<y\\ p_1\in\mathfrak{P}_h}} \frac{\omega(p_1)}{p_1}\Bigg)\Bigg). \tag{6.9}$$

Per definition av w och y gäller $(\log y)/(\log w) = 10/3$ så att Lemma A.9 medför att den andra termen i (6.9) är $\mathcal{O}((\log X)^{-1/14})$. För att uppskatta resttermen i (6.6) observerar vi att indexet $p_1 n$ inte upprepas, eftersom n delar $P(w)$ och $p_1 \geq w$ så att den största primtalsfaktorn i $p_1 n$ alltid är p_1. Dessutom gäller $p_1 n < \xi^2$, $(p_1 n, \overline{\mathfrak{P}_h}) = 1$, samt att $p_1 n$ är kvadratfri. Därmed kan resttermen begränsas av

$$\sum_{\substack{d<\xi^2\\ (\overline{\mathfrak{P}},d)=1}} \mu^2(d) 3^{\nu(d)} |R_d| = \mathcal{O}\left(\frac{X}{\log^2 X}\right),$$

där vi för att erhålla $\mathcal{O}$-termen använt villkoret $R(1,\alpha)$ samt definitionen av ξ^2. Eftersom vi betraktar ett linjärt problem ger (3.10), eller den explicita beräkningen av $W(N^{1/10})$ nedan, att resttermen kan absorberas i feltermen så att vänsterledet i (6.6) kan begränsas av

$$XW(N^{1/10})\Bigg(\sum_{\substack{w\leq p_1<y\\ p_1\in\mathfrak{P}_h}} \frac{\omega(p_1)}{p_1} F\left(\frac{(\log X^{1/2}/p_1)}{\log w}\right) + \mathcal{O}\left(\frac{1}{(\log X)^{1/14}}\right)\Bigg). \tag{6.10}$$

Det som krävs för att avsluta uppskattningen är att begränsa summan i (6.10). Man kan med hjälp av Lemma A.8, Lemma A.9 och partiell integrering, jämför [HR, s. 246], se att summan är

$$\int_3^{10} F\left(5 - \frac{10}{t}\right)\frac{dt}{t} + \mathcal{O}\left(\frac{1}{\log X}\right).$$

Vi har enligt Lemma A.6, $X = N/(\log N)(1 + \mathcal{O}(1/(\log N))$. Om vi använder det i (6.5) får vi en undre begränsning av de två första termerna i (6.4) enligt

$$XW(N^{1/10})\left(f(5) - \frac{1}{2}\int_3^{10} F\left(5 - \frac{10}{t}\right)\frac{dt}{t} + \mathcal{O}\left(\frac{1}{(\log X)^{1/14}}\right)\right), \tag{6.11}$$

där vi med hjälp av (5.4) och $X \leq N$, för tillräckligt stora N, har skrivit

$$f\left(\frac{5\log X}{\log N}\right) = f(5) + \mathcal{O}\left(\frac{1}{(\log N)^{1/2}}\right) = f(5) + \mathcal{O}\left(\frac{1}{(\log X)^{1/2}}\right).$$

Vi fortsätter att följa [HR, avsnitt 11.2]. Genom att använda (5.3) ger en omfattande integralberäkning, se [HR, s. 323], att uttrycket involverande f och F i (6.11) är strikt större än $2{,}64e^{\gamma}/20$. Dessutom ger en beräkning, se appendix B.4.2, att $W(N^{1/10})$ kan begränsas underifrån av

$$20e^{-\gamma}\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{2<p|h}\frac{p-1}{p-2}\frac{1}{\log N}\left(1 + \mathcal{O}\left(\frac{1}{\log N}\right)\right).$$

Om vi kombinerar våra resultat och använder Lemma A.6 kan vi till slut, genom att välja ett tillräckligt stort N och utnyttja att den undre begränsningen för integralen är strikt, skriva

$$|\{p + h : p \leq N, p + h \in P_2\}| > 2{,}64\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{2<p|h}\frac{p-1}{p-2}\frac{N}{\log^2 N} - \frac{1}{2}S_0, \tag{6.12}$$

där S_0 är den tredje termen i (6.4). Vi påpekar, likt [HR, s. 324], att vi har bevisat Chens sats så som vi formulerat den om vi för tillräckligt stora N lyckas visa

$$S_0 \leq 3{,}96\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{2<p|h}\frac{p-1}{p-2}\frac{N}{\log^2 N}. \tag{6.13}$$

För vidare räkningar låter vi $\mathcal{P}_N = \{p_1p_2 : N^{1/10} \leq p_1 < N^{1/3} \leq p_2 < (N/p_1)^{1/2}\}$ och

$$\mathcal{A}(p_1, p_2) = \left\{p_1p_2p - h : p \leq \frac{N}{p_1p_2}\right\}. \tag{6.14}$$

Med dessa får vi

$$S_0 = \sum_{\substack{p_1p_2\in\mathcal{P}_N\\(p_1p_2,h)=1}}\left|\left\{p : p \leq \frac{N}{p_1p_2}, p_1p_2p - h = p'\right\}\right|. \tag{6.15}$$

Varje term i summan räknar antalet primtal i $\mathcal{A}(p_1, p_2)$. Vi påminner om att $P(z)$ är produkten av alla primtal i $\mathfrak{P}_h$ mindre än z och observerar att högst z element är faktorer i $P(z)$. I annat fall uppfyller de $(p_1p_2p - h, P(z)) = 1$. Vi erhåller därför

$$\left|\left\{p : p \leq \frac{N}{p_1p_2}, p_1p_2p - h = p'\right\}\right| \leq z + \left|\left\{p : p \leq \frac{N}{p_1p_2}, (p_1p_2p - h, P(z)) = 1\right\}\right|.$$

Vi definierar nu $z^2 = N^{1/2-\varepsilon}$, där $0 < \varepsilon < 10^{-5}$. Insättning i (6.15) ger att

$$S_0 \leq \sum_{p_1p_2\in\mathcal{P}_N}\left|\left\{p : p \leq \frac{N}{p_1p_2}, (p_1p_2p - h, P(z)) = 1\right\}\right| + \mathcal{O}(N^{11/12}). \tag{6.16}$$

Feltermens form beror på att $z < N^{1/4}$ och att summan har mindre än $N^{2/3}$ termer. Vi ska nu skriva om uttrycket med hjälp av $\Lambda(n)$, se Definition A.1. Målet är att få ett uttryck som innehåller samma mängd som i (6.16). Vi skriver $p_1p_2 = r$ och låter $\varepsilon_0 = 1/\sqrt{\log N}$. Därefter betraktar vi summan

$$\sum_{\substack{n\leq N/r\\(rn-h,P(z))=1}}\Lambda(n). \tag{6.17}$$

Dess termer är alltid ickenegativa, och nollskilda endast då n är en primtalspotens p^m. Vi får en undre begränsning genom att bara betrakta primtal p och inga högre potenser. Vidare exkluderar vi de termer sådana att $p \leq (N/r)^{1-\varepsilon_0}$. Eftersom $(N/r)^{1-\varepsilon_0} < p$ är $(1-\varepsilon_0)\log(N/r) < \log p$ och vi får då en undre begränsning av (6.17) enligt

$$\begin{aligned}\sum_{\substack{(N/r)^{1-\varepsilon_0}<p\leq N/r\\(rp-h,P(z))=1}} \log p &\geq (1-\varepsilon_0)\log(N/r) \sum_{\substack{(N/r)^{1-\varepsilon_0}<p\leq N/r\\(rp-h,P(z))=1}} 1\\ &\geq (1-\varepsilon_0)\log(N/r)\left(\left|\left\{p : p < \frac{N}{r}, (rp-h, P(z)) = 1\right\}\right| - (N/r)^{1-\varepsilon_0}\right).\end{aligned}$$

Summan i (6.16) begränsas därför ovanifrån av

$$\begin{aligned}&\sum_{p_1p_2\in\mathcal{P}_N}\left(\frac{1}{(1-\varepsilon_0)\log(N/p_1p_2)}\sum_{\substack{n\leq N/p_1p_2\\(p_1p_2n-h,P(z))=1}}\Lambda(n) + \left(\frac{N}{p_1p_2}\right)^{1-\varepsilon_0}\right)\\ &\quad\leq (1+2\varepsilon_0)\sum_{p_1p_2\in\mathcal{P}_N}\sum_{\substack{p_1p_2n\leq N\\(p_1p_2n-h,P(z))=1}}\frac{\Lambda(n)}{\log(N/p_1p_2)} + \sum_{p_1p_2\in\mathcal{P}_N}\left(\frac{N}{p_1p_2}\right)^{1-\varepsilon_0}. \qquad (6.18)\end{aligned}$$

Om vi byter summationsordning i dubbelsumman i (6.18) får vi den nya summan

$$S_1 := \sum_{\substack{m\leq N\\(m-h,P(z))=1}}\sum_{\substack{p_1p_2n=m\\p_1p_2\in\mathcal{P}_N}}\frac{\Lambda(n)}{\log(N/p_1p_2)} = \sum_{\substack{m\leq N\\(m-h,P(z))=1}}\Lambda_0(m),$$

där $\Lambda_0(m)$ betecknar den inre summan som en funktion av m. Vi har också att

$$\sum_{p_1p_2\in\mathcal{P}_N}\left(\frac{N}{p_1p_2}\right)^{1-\varepsilon_0} = N^{1-\varepsilon_0}\sum_{p_1p_2\in\mathcal{P}_N}\frac{(p_1p_2)^{\varepsilon_0}}{p_1p_2} \leq N^{1-\varepsilon_0/3}\sum_{p_1p_2\in\mathcal{P}_N}\frac{1}{p_1p_2} = \mathcal{O}(N^{1-\varepsilon_0/3})$$

eftersom $p_1p_2 \leq N^{2/3}$ och den sista summan är begränsad av en konstant enligt upprepad användning av Lemma A.9. För tillräckligt stora N får vi därför att

$$S_0 \leq (1+2\varepsilon_0)S_1 + \mathcal{O}(N^{1-\varepsilon_0/3}). \qquad (6.19)$$

6.4 Selbergs såll och Dirichletkaraktärer

För att uppskatta S_1 introducerar vi så kallade Dirichletkaraktärer. En komplexvärd funktion χ definierad på heltalen kallas för en Dirichletkaraktär modulo ℓ om $\chi(n+\ell) = \chi(n)$ för alla n, $\chi(mm) = \chi(m)\chi(n)$ för alla heltal m, n, $\chi(1) = 1$, samt $\chi(n) = 0$ för $(n,\ell) > 1$. Talet ℓ kallas för χ:s period. Vi presenterar nedan några användbara egenskaper hos Dirichletkaraktärer.

Från definitionen följer $|\chi(n)| = 1$ för alla $(n,\ell) = 1$, samt att $\chi(n)$ i sådana fall är en enhetsrot. Dessutom ser vi att om χ är en Dirichletkaraktär är också $\bar{\chi}$ det och $\chi(n)\bar{\chi}(n) = 1$ för $(n,\ell) = 1$. Från multiplikativiteten följer, om $(n,\ell) = 1$, att $\bar{\chi}(n) = \chi(n^{-1})$, där n^{-1} är invers till n modulo ℓ. En speciell karaktär är huvudkaraktären χ_0 som är indikatorfunktion för tal n sådana att $(n,\ell) = 1$. Fler detaljer återfinns i appendix B.4.3 och en fullständig behandling ges i [D, kapitel 1 och 4].

Vi använder nu Selbergs såll i specialfallet $\xi = z$, $q = 1$ och följer [HR, avsnitt 11.3]. Eftersom S_1 är nära relaterad till $\mathcal{A} := \mathcal{A}(p_1,p_2)$ från (6.14) väljer vi de vikter λ_d vi skulle använt för att studera $\mathcal{A}$, med tillhörande $\mathfrak{P} := \mathfrak{P}_h$. Notera att $z \leq N^{1/4} \leq p_1 \leq p_2$ så att för $d \leq z$ har vi $(d, p_1p_2) = 1$. Därmed är $\mathcal{A}$ en av de följderna vi studerade i avsnitt 4.3. Vi väljer därför $\omega(d) = d/\phi(d)$ för $d \leq z$, $(d,h) = 1$, och $\omega(d) = 0$ om $(d,h) > 1$. Vi väljer nu λ_d enligt (4.11) och erhåller, jämför (4.1), att

$$S_1 \leq \sum_{m\leq N}\Lambda_0(m)\Bigg(\sum_{\substack{d|P(z)\\d|m-h}}\lambda_d\Bigg)^2 = \sum_{d_1,d_2|P(z)}\lambda_{d_1}\lambda_{d_2}\sum_{\substack{m\leq N\\m\equiv h \bmod D}}\Lambda_0(m), \qquad (6.20)$$

där vi i första olikheten använt att kvadrater är icke-negativa, samt att $\lambda_1 = 1$ så att om $(m - h, P(z)) = 1$ får summan precis ett tillskott $\Lambda_0(m)$. D har vi definierat som $[d_1, d_2]$.

Eftersom $\mathfrak{P} = \mathfrak{P}_h$ är $(D, h) = 1$ och h har en invers modulo D. Därmed är $h \equiv m \bmod D$ ekvivalent med $mh^{-1} \equiv 1 \bmod D$. Vi kan nu använda Lemma B.6, som beskriver resultatet av en summation över alla Dirichletkaraktärer modulo D, för att skriva om högerledet i (6.20) till

$$\sum_{d_1,d_2|P(z)} \frac{\lambda_{d_1}\lambda_{d_2}}{\phi(D)} \sum_{m\leq N} \Lambda_0(m) \sum_{\chi \bmod D} \overline{\chi}(h)\chi(m) = \sum_{d_1,d_2|P(z)} \frac{\lambda_{d_1}\lambda_{d_2}}{\phi(D)} \sum_{\chi \bmod D} \overline{\chi}(h) \sum_{m\leq N} \Lambda_0(m)\chi(m),$$

Vi kallar hädanefter den innersta summan $\psi_0(N, \chi)$. För huvudkaraktären χ_0 har vi speciellt

$$\psi(N, \chi_0) = \sum_{\substack{m\leq N \\ (m,D)=1}} \Lambda_0(m) = \sum_{m\leq N} \Lambda_0(m) - \sum_{\substack{m\leq N \\ (D,m)>1}} \Lambda_0(m). \tag{6.21}$$

Vi delar därför upp summan över Dirichletkaraktärerna ovan för att hantera $\chi = \chi_0$ separat. Vi tar sedan absolutbelopp av de två sista delsummorna som uppkommer. Vi flyttar in absolutbeloppet och erhåller totalt

$$\begin{aligned} S_1 \leq \sum_{d_1,d_2|P(z)} \frac{\lambda_{d_1}\lambda_{d_2}}{\phi(D)} \sum_{m\leq N} \Lambda_0(m) &+ \sum_{\substack{D<z^2 \\ D|P(z)}} \frac{\mu^2(D)3^{\nu(D)}}{\phi(D)} \sum_{\substack{m\leq N \\ (m,D)>1}} \Lambda_0(m) \\ &+ \sum_{\substack{D<z^2 \\ D|P(z)}} \frac{\mu^2(D)3^{\nu(D)}}{\phi(D)} \Bigg| \sum_{\substack{\chi\neq\chi_0 \\ \chi \bmod D}} \overline{\chi}(h)\psi_0(N,\chi)\Bigg|, \end{aligned} \tag{6.22}$$

där vi använt samma resonemang som i förenklingen av (4.12) för att erhålla de två sista summorna. Vi följer [HR, avsnitt 11.3] och kallar den andra summan ovan S_2 och den tredje S_3. Vi kan direkt beräkna den första summan genom att byta summationsordning och då erhålla Σ_1 från (4.8) som den inre summan. Med våra val av λ_d, och teorin från Selbergs såll i avsnitt 4.2, vet vi att Σ_1 är lika med sitt minimum $(G(z))^{-1}$, där G är definierad i termer av ω ovan enligt (4.10).

För att avsluta beviset av Chens sats återstår det att uppskatta klart summorna i (6.22). Att färdigställa uppskattningen av den första summan och uppskatta S_2 kan göras med relativt enkla metoder, åtminstone om vi tillåter oss att använda primtalssatsen med felterm. Det visar sig att den första summan kommer vara den dominerande termen. Vi har att $S_3 \ll N/(\log^{38} N)$ och den ger därför inget nämnvärt tillskott till S_1 i förhållande till högerledet i (6.13), men att visa det kräver ytterligare teori om Dirichletkaraktärer, samt teori om det stora sållet. Uppskattningen blir teknisk och knyter inte an till den sållteori vi tidigare presenterat. Vi utelämnar därför uppskattningen av S_3, men den intresserade läsaren hänvisas till [HR, avsnitt 11.4-11.6] för detaljerna. För våra ändamål räcker det med marginal att veta att $S_3 \ll N/\log^3 N$.

Uppskattningen av de två första summorna beskrivs i appendix B.4.5. Vi erhåller ekvationerna (B.29) och (B.32). Tillsammans med $S_3 \ll N/\log^3 N$ har vi

$$3{,}95 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{N}{\log^2 N} \left(1 + \mathcal{O}\left(\frac{1}{\log N}\right)\right) + \mathcal{O}(N^{9/10}\log^5 N) + \mathcal{O}\left(\frac{N}{\log^3 N}\right),$$

som en strikt övre begränsning för S_1. Vi påminner om att den första produkten är konvergent och att den andra är positiv, så att alla feltermer kan absorberas i den första. Vi har alltså

$$S_1 < 3{,}95 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{N}{\log^2 N} \left(1 + \mathcal{O}\left(\frac{1}{\log N}\right)\right).$$

Vi kan alltså välja N_0 tillräckligt stort så att vi för $N \geq N_0$ har

$$S_1 \leq 3{,}95 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{N}{\log^2 N}. \tag{6.23}$$

Vi noterar att eftersom $\varepsilon_0 = 1/\sqrt{\log N}$ är feltermen i (6.19) speciellt $\ll N/\log^3 N$. Från (6.23), våra anmärkningar i anslutning till (6.13) och kopplingen mellan S_0 och S_1 i (6.19), följer därför Sats 6.1 genom att välja N tillräckligt stort.

Referenser

[A] T. M. Apostol, *Introduction to Analytic Number Theory*, 1 uppl. New York, NY, USA: Springer, 1976.

[Bo] E. Bombieri, ”On the large sieve”, *Mathematika*, vol. **12**, no. 2, s. 201–225, 1965, doi: 10.1112/S0025579300005313.

[Br] V. Brun, ”Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare”, *Archiv for Math. og Naturvid.* B **34**, no 8, 1915.

[C] J. R. Chen, ”On the Representation of a Large Even Integer as the Sum of a Prime and the Product of at Most Two Primes”, *Sci. Sinica*, vol. **16**, no 2, s. 157-176, 1973.

[D] H. Davenport, *Multiplicative Number Theory*, 2 uppl. New York, NY, USA: Springer, 1980.

[HR] H. Halberstam och H. E. Richert, *Sieve Methods*, 1 uppl. London, Storbritannien: Academic Press, 1974.

[M] J. Maynard, ”Small gaps between primes” *Ann. Math.*, vol. **181**, no 3, s. 383–413, 2015, doi: 10.4007/annals.2015.181.1.7.

[P] D. H. J. Polymath, ”Variants of the Selberg sieve, and bounded intervals containing many primes”, *Res. Math. Sci.*, vol **1**, no 1, s. 1-83, 2014, doi: 10.1186/s40687-014-0012-7.

[R] K. H. Rosen, *Elementary number theory*, Pearson new international edition, 6 uppl. London, Storbritannien: Pearson Education, 2013.

[S] A. Selberg, ”On an elementary method in the theory of primes”, *Norske Vid. Selsk. Forh.* vol. **19**, no. 18, s. 64-67, 1947.

[W] J. W. Wrench, ”Evaluation of Artin’s Constant and the Twin-Prime Constant”, *Math. Comput.*, vol **15**, no 76, s. 396-398, 1961, doi: 10.2307/2003029.

[Z] Y. Zhang, ”Bounded gaps between primes”, *Ann. Math.*, vol. **179**, no 3, s. 1121-1174, 2014, doi: 10.4007/annals.2014.179.3.7.

A Uppskattningar och elementär talteori

Vi presenterar nedan grundläggande resultat från elementär talteori samt talteoretiska uppskattningar, ibland tillsammans med våra egna korta bevis. Om bevisen inte är våra, men så välkända att de anses vara standardbevis, markerar vi det. Alla satser bevisas inte, eftersom det skulle öka rapportens omfång alltför mycket. Om satsen är särskilt viktig, eller om beviset illustrerar en viktig teknik inkluderar vi dock bevis om möjligt. Många av resultaten från elementär talteori återfinns i exempelvis [R] och många av uppskattningarna återfinns i [A].

A.1 Elementära resultat

Vi inleder med ett viktigt lemma som ger en användbar form att skriva en indikatorfunktion på [R, Sats 7.15].

Lemma A.1. *Definiera Möbiusfunktionen enligt* (1.1) *för positiva heltal n. Då gäller*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{om } n = 1, \\ 0 & \text{annars.} \end{cases}$$

Vi visar nu en viktig koppling mellan Möbiusfunktionen och multiplikativa funktioner.

Lemma A.2. *Låt h vara en multiplikativ funktion. Då gäller att*

$$\prod_{p|P'} (1 - h(p)) = \sum_{d|P'} \mu(d)h(d),$$

där P' är en godtycklig kvadratfri produkt av primtal.

Bevis. Vi utför beviset med induktion på antalet faktorer i P'. För basfallet $P' = 1$ är satsen trivial eftersom multiplikativiteten hos h medför $h(1) = 1$ och vi vet att $\mu(1) = 1$. Vi visar nu induktionsfallet. Antag att satsen är bevisad för $\nu(P_1') \leq n$, med $n \geq 0$. Låt P' vara sådant att $v(P') = n + 1$. Ordna primtalen som delar P' i storleksordning enligt $2 \leq p_{n+1} < ... < p_1$ så att $P' = p_{n+1} \cdot ... \cdot p_1$. Vi har då genom att använda induktionsantagandet att

$$\begin{aligned}
&\prod_{p|P'} (1 - h(p)) = \left(\sum_{d|p_{n+1}\cdot...\cdot p_2} \mu(d)h(d) \right) (1 - h(p_1)) \\
&= \sum_{d|p_{n+1}\cdot...\cdot p_2} \mu(d)h(d) - \sum_{d|p_{n+1}\cdot...\cdot p_2} \mu(d)h(p_1 d) = \sum_{d|p_{n+1}\cdot...\cdot p_2} \mu(d)h(d) + \sum_{d|p_{n+1}\cdot...\cdot p_2} \mu(p_1 d)h(p_1 d) \\
&= \sum_{\substack{d|p_{n+1}\cdot...\cdot p_1 \\ (d,p_1)=1}} \mu(d)h(d) + \sum_{\substack{d|p_{n+1}\cdot...\cdot p_1 \\ (d,p_1)=p_1}} \mu(d)h(d) = \sum_{d|P'} \mu(d)h(d),
\end{aligned}$$

vilket var det som skulle visas. I andra likheten använde vi att h var multiplikativ och i den tredje att Möbiusfunktionen byter tecken om vi lägger till en primtalsfaktor som inte redan finns i argumentet. Lemmat följer nu ur induktionsprincipen. □

Notera att Lemma A.2 speciellt kan tillämpas på $P' = P(z)$. Man kan också lätt bevisa följande lemma med samma metod. Faktum är att Lemma A.2 är ett specialfall av Lemma A.3, men det är instruktivt i beviset ovan att tydligt se vilken roll Möbiusfunktionen har.

Lemma A.3. *Låt h vara en multiplikativ funktion. Då gäller att*

$$\prod_{p|P'} (1 + h(p)) = \sum_{d|P'} h(d),$$

där P' är en godtycklig kvadratfri produkt av primtal.

Kinesiska restsatsen är ett användbart verktyg i arbete med kongruenser och vi formulerar den därför här [R, Sats 4.13].

Sats A.4 (Kinesiska restsatsen)**.** *Låt* $n = \prod_{1\le i\le r} p_i^{k_i} \ge 2$*. Då har systemet av kongruenser*

$$\begin{cases} x \equiv a_1 \ mod\ p_1^{k_1} \\ \vdots \\ x \equiv a_r \ mod\ p_r^{k_r} \end{cases}$$

en unik lösning x_0 *modulo* n*.*

En annan användbar sats är Eulers sats som relaterar funktionen ϕ till kongruensräkning. Vi hämtar formuleringen från [R, Sats 6.14]

Sats A.5. *Om* $(a, n) = 1$ *gäller*

$$a^{\phi(n)} \equiv 1 \ mod\ n.$$

A.2 Uppskattningar

Vi inleder med att relatera funktionen $\operatorname{li} x$ till de elementära funktionerna. Beviset är ett standardbevis och formuleringen kan jämföras med [A, övning 4.19].

Lemma A.6. *För* $x \ge 2$ *gäller*

$$\operatorname{li} x = \frac{x}{\log x} + \mathcal{O}\left(\frac{x}{\log^2 x}\right).$$

Bevis. Partiell integrering ger

$$\operatorname{li} x = \int_2^x \frac{1}{\log t} dt = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{1}{\log^2 t} dt.$$

Vi noterar att satsen är trivial för begränsade x eftersom vi då helt enkelt kan öka värdet av den implicerade konstanten. Vi antar därför att x är så stort att $\sqrt{x} \ge 2$. Vi kan då uppskatta den sista integralen enligt

$$\int_2^x \frac{1}{\log^2 t} dt = \int_2^{\sqrt{x}} \frac{1}{\log^2 t} dt + \int_{\sqrt{x}}^x \frac{1}{\log^2 t} dt \le \frac{\sqrt{x} - 2}{\log^2 2} + \frac{2(x - \sqrt{x})}{\log^2 x},$$

varefter vårt resultat följer. □

Vi ger nu en uppskattning som är användbar när vi betraktar villkoret $(\Omega_2(\kappa))$ i det linjära fallet [HR, ekvation (5.1.1)].

Lemma A.7. *Det gäller att*

$$\sum_{w \le p \le z} \frac{\log p}{p} = \log \frac{z}{w} + O(1), \quad 2 \le w \le z.$$

Ur lemmat ovan följer andra uppskattningar, men för att kunna härleda de behöver vi ytterligare verktyg. Vi introducerar därför partiell summation, som kan användas för att beräkna summor vars termer är produkter. Det kräver dock att man har god kontroll över partialsummorna hos den ena faktorn. Vi anmärker att vi ofta kommer ha nytta av partiell summation även utanför detta avsnitt. Formuleringen och beviset nedan kan jämföras med [A, Sats 4.2].

Lemma A.8. *Låt* $\{a_n\}_{n=1}^{\infty}$ *vara en följd av reella eller komplexa tal och låt* $x < y$ *vara reella tal. Definiera* $A(t) = \sum_{n<t} a_n$*. Låt* f*, definierad på* $[x, y]$ *vara en reellvärd, eller komplexvärd funktion som är kontinuerligt deriverbar på* $[x, y]$*. Då gäller*

$$\sum_{x \le n < y} a_n f(n) = A(y)f(y) - A(x)f(x) - \int_x^y A(u)f'(u)du.$$

Bevis. Bevisidén är att utveckla integralen i högerledet med hjälp av observationen att A är konstant mellan heltal. Betrakta partitionen av $[x, y]$ enligt $x = k_1 < k_2 < ... < k_{N-1} < k_N = y$ där k_i är på varandra följande heltal för åtminstone $i \neq 0, N$. Då är integralen ovan

$$\sum_{i \leq N-1} \int_{k_i}^{k_{i+1}} A(u)f'(u)du = \sum_{i \leq N-1} A(k_{i+1}) \int_{k_i}^{k_{i+1}} f'(u)du = \sum_{i \leq N-1} A(k_{i+1})(f(k_{i+1}) - f(k_i)).$$

Summan ovan är nästan teleskoperande. Vi observerar att $A(k_{i+2}) - A(k_{i+1}) = a_{k_{i+1}}$ för $1 < i < N-1$ så att summan är

$$A(k_N)f(k_N) - A(k_2)f(k_1) - \sum_{x<n<y} a_n f(n) = A(y)f(y) - A(k_2)f(x) - \sum_{x<n<y} a_n f(n).$$

Om x inte är ett heltal är $A(k_2) = A(x)$ och det finns inget heltal $n = x$ i summan så att vi är klara. Om x däremot är ett heltal är $A(k_2) = a_{k_1} + A(x)$. Om vi lägger till den extra termen i summan får vi

$$A(y)f(y) - A(x)f(x) - \sum_{x \leq n < y} a_n f(n),$$

som önskat. □

Ett vanligt trick är att sätta $a_n = 0$ för små värden på n om de inte är av intresse. Speciellt är $A(x) = 0$ om $a_n = 0$ för $n < x$. Från Lemma A.7 och Lemma A.8 följer lemmat nedan [HR, ekvation (5.1.2)]. Beviset är ett standardbevis.

Lemma A.9. *Vi har*

$$\sum_{w \leq p < z} \frac{1}{p} = \log \frac{\log z}{\log w} + \mathcal{O}\left(\frac{1}{\log w}\right), \quad 2 \leq w \leq z.$$

Bevis. Vi kommer att betrakta summanden på formen

$$\frac{\log n}{n} \mathbf{1}_{\{\text{n är ett primtal}\}} \cdot \frac{1}{\log n},$$

där $\mathbf{1}$ är en indikatorfunktion. Vi kallar den första faktorn a_n, men definierar den som 0 om $n < w$. Lemma A.7 ger då $A(t) = \log(t/w) + \mathcal{O}(1)$ för $t \geq w$. En tillämpning av Lemma A.8 ger

$$\sum_{w \leq p < z} \frac{1}{p} = \frac{\log(z/w) + \mathcal{O}(1)}{\log z} + \int_w^z \frac{\log(t/w) + \mathcal{O}(1)}{t \log^2 t} dt = \log \frac{\log z}{\log w} + \mathcal{O}\left(\frac{1}{\log w}\right).$$

□

Vi kan erhålla en uppskattning av en produkt av typen $\prod_{k<p<z}(1 - k/p)$ genom att först ta logaritmen av produkten, Taylorutveckla, och sedan använda Lemma A.9.

Lemma A.10. *För alla positiva heltal k finns strikt positiva konstanter C_1 och C_2, beroende på k, sådana att*

$$\frac{C_1}{\log^k z} \leq \prod_{k<p<z} \left(1 - \frac{k}{p}\right) \leq \frac{C_2}{\log^k z}$$

för $z \geq 2$.

Ur Lemma A.10 med $k = 1$ följer direkt en övre begränsning av $\phi(d)$. Vi har nämligen följande resultat.

Lemma A.11. *För d ett positivt heltal har vi $\phi(d) \gg \frac{d}{\log d}$.*

Bevis. Från elementär talteori vet vi att ϕ är multiplikativ så att

$$\phi(d) = d \prod_{p|d} \left(1 - \frac{1}{p}\right) \geq d \prod_{p \leq d} \left(1 - \frac{1}{p}\right) \gg \frac{d}{\log d},$$

där sista steget är Lemma A.10. □

Ibland har vi nytta av en skarpare variant av Lemma A.10 med $k = 1$. Beviset kräver dock grundläggande teori om Riemanns zetafunktion och utelämnas därför. Formuleringen är [HR, ekvation (5.1.3)].

Lemma A.12. *Vi har för $z \geq 2$*

$$\prod_{p<z}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log z}\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right).$$

Det kommer ofta vara användbart att ha en begränsning av funktionen ν. Med en elementär olikhet får vi genast följande lemma.

Lemma A.13. *För heltal $n \geq 1$ gäller $\nu(n) \ll \log n$.*

Bevis. Notera först $\nu(1) = 0$ så att vi kan anta $n \geq 2$. Antag $\nu(n) = k$. Då har vi

$$n \geq \prod_{i\leq k} p_i$$

eftersom produkten är det minsta heltalet med $\nu(n) = k$. Om vi tar logaritmen av båda led erhåller vi

$$\log n \geq \sum_{i\leq k} \log p_i \geq (\log 2)k \gg k$$

så att $\nu(n) \ll \log n$. □

För att lyckas med de mer avancerade uppskattningarna som krävs i beviset av Chens sats behöver vi primtalssatsen med felterm. Primtalssatsen finns i många ekvivalenta varianter och det vi kommer ha nytta av är formen som ger en uppskattning för en summa över Mangoldtfunktionen $\Lambda(n)$. Vi ger därför först följande definition.

Definition A.1. Mangoldtfunktionen $\Lambda(n)$ definieras enligt

$$\Lambda(n) = \begin{cases} \log p & \text{om } n = p^m \text{ för några } p,\ m \geq 1, \\ 0 & \text{annars.} \end{cases}$$

Nu formulerar vi en version av primtalssatsen med felterm [D, s. 111].

Lemma A.14 (Primtalssatsen)**.** *Det existerar en absolut positiv konstant c så att*

$$\sum_{n\leq x} \Lambda(n) = x\left(1+\mathcal{O}\left(e^{-c(\log x)^{1/2}}\right)\right),$$

för $x \geq 2$.

Eftersom konstanten c är positiv gäller $e^{-c(\log x)^{1/2}} \ll e^{-\log\log x} = 1/\log x$ för $x \geq 2$. Därmed kan vi skriva resttermen ovan på en svagare, men mer lättanvänd, form enligt nedan.

Korollarium A.15. *För $x \geq 2$ har vi*

$$\sum_{n\leq x} \Lambda(n) = x\left(1+\mathcal{O}\left(\frac{1}{\log x}\right)\right),$$

B Bevis av satser

Vi ger nedan delar av, eller hela, bevis som utelämnats från huvudtexten. Läsaren bör läsa avsnitten nedan tillsammans med motsvarande avsnitt i huvuddelen av texten.

B.1 Eratosthenes-Legendres såll

Vi redogör för beviset av Eratosthenes-Legendres såll från [HR, s. 30-31].

Bevis av Sats 2.1. Beviset är kort och inleds med en beräkning. Vi utnyttjar i första steget likheten (A.1) så att den första inre summan nedan är indikatorfunktion för a med $(a, P(z)) = 1$. Enligt kraven på q från avsnitt 2.1 har vi $(q, P(z)) = 1$. Därmed gäller

$$S(\mathcal{A}_q; \mathfrak{P}, z) = \sum_{a \in \mathcal{A}_q} \sum_{\substack{d|a \\ d|P(z)}} \mu(d) = \sum_{d|P(z)} \mu(d) \sum_{\substack{a \in \mathcal{A} \\ a \equiv 0 \bmod qd}} 1 = \sum_{d|P(z)} \mu(d) |\mathcal{A}_{qd}|,$$

där den sista likheten är per definition. Notera att vi i den andra likheten bytt summationsordning. Eftersom $d \mid P(z)$ och $(q, P(z)) = 1$ har vi $(q, d) = 1$ så att $d \mid a$, $q \mid a$ är ekvivalent med att $a \equiv 0 \mod qd$ enligt kinesiska restsatsen. Från definition av R_{qd} följer ur ovan

$$S(\mathcal{A}_q; \mathfrak{P}, z) = \sum_{d|P(z)} \mu(d) \frac{\omega(qd)}{qd} X + \sum_{d|P(z)} \mu(d) R_{qd}. \tag{B.1}$$

Vi använder nu att både μ och ω är multiplikativa för att beräkna den första termen ovan, vilket illustrerar en viktig princip för att omvandla en summa till en produkt. Omskrivningen följer ur Lemma A.2 samt att $\omega(p) = 0$ om $p \notin \mathfrak{P}$. Vi har då

$$\sum_{d|P(z)} \mu(d) \frac{\omega(d)}{d} = \prod_{\substack{p<z \\ p \in \mathfrak{P}}} \left(1 - \frac{\omega(p)}{p}\right) = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right).$$

Satsens första del följer nu genom att tillämpa triangelolikheten på den andra summan.

För satsens andra del sätter vi $q = 1$. Eftersom både (R) och (Ω_0) är uppfyllda har vi $|R_p| \leq A_0$ så att $|R_d| \leq A_0^{\nu(d)}$. Vi uppskattar nu den andra summan i (B.1) genom att tillämpa triangelolikheten och $|\mu(d)| \leq 1$. En avslutande beräkning likt ovan ger

$$\sum_{d|P(z)} |R_d| \leq \sum_{d|P(z)} A_0^{\nu(d)} = \prod_{p|P(z)} (1 + A_0) \leq (1 + A_0)^{\pi(z)} \leq (1 + A_0)^z.$$

Likheten är Lemma A.3 tillämpad på funktionen $h(d) = A^{v(d)}$. Den sista olikheten är den triviala olikheten för $\pi(z)$. Satsens andra del följer. $\square$

B.2 Bevis av Sats 3.2

Vi ska här studera beviset av Sats 3.2 enligt de linjer som ges i [HR, s. 57-62]. Så när som på några få detaljer är det vår ambition att ge en fullständig framställning. Vi delar upp arbetet i flera delresultat, och låter det vara underförstått att villkoren $(\Omega_1), (\Omega_2(\kappa))$ och (R) alltid är uppfyllda. Eventuella andra förutsättningar anges explicit.

Om z är begränsad följer resultatet av en generaliserad version av Eratosthenes-Legendres såll [HR, s. 57]. Vi kommer därför framöver anta att z är så stort som räkningarna kräver.

Vår utgångspunkt är (3.8), som gäller för alla kombinatoriska såll. Vi måste därför säkerställa att de aktuella funktionerna χ_v genererar ett sådant.

Lemma B.1. *Funktionerna $\chi_v, v = 1, 2$ definierade enligt* (3.11) *genererar ett kombinatoriskt såll.*

Bevis. Att $\chi_v(d) \in \{0, 1\}$ är uppenbart. Vidare är $\chi_v(1) = 1$ eftersom $\nu((1, P_{z_n,z})) = \nu(1) = 0$, och $2b - v + 2n - 1 \geq 2n - 1 \geq 1$ för $n = 1, 2, ..., r$. Antag nu att $t|d$ och $\chi_v(d) = 1$. Då är $\nu((d, P_{z_n,z})) \leq 2b - v + 2n - 1, n = 1, 2, ..., r$. Eftersom $t|d$ är $\nu((t, P_{z_n,z})) \leq \nu((d, P_{z_n,z}))$ och därmed är $\chi_v(t) = 1$.

Antag slutligen att $\chi_v(t) = 1, \mu(t) = (-1)^v$, att $p < q(t)$, och att $pt|P(z)$. Vi måste visa att $\chi_v(pt) = 1$, med andra ord att $\nu((pt, P_{z_n,z})) \leq 2b - v + 2n - 1$, $n = 1, 2, ..., r$. Vi observerar att $z_m \leq p < z_{m-1}$ för något m. Därför är $\nu((pt, P_{z_n,z})) = \nu((t, P_{z_n,z})) \leq 2b - v + 2n - 1$ för alla $n < m$, eftersom $\chi_v(t) = 1$. Antag nu att

$$\nu((pt, P_{z_n,z})) \leq 2b - v + 2n - 1 \tag{B.2}$$

för $n = m$. I så fall är (B.2) också uppfylld för alla $n > m$. Det beror på att högerledet växer då n växer medan vänsterledet däremot förblir konstant. Vi är därför klara om vi kan visa (B.2) för $n = m$.

Vi vet att $\nu((pt, P_{z_m,z})) = \nu(pt)$ eftersom $pt \mid P(z)$ och $z_m \leq p$. Vidare är $\nu(t) = \nu((t, P_{z_m,z})) \leq 2b-v+2m-1$. Om vi kan visa att olikheten är strikt är vi klara, eftersom $\nu(pt) = \nu(t)+1$. Eftersom $\mu(t) = (-1)^{\nu(t)} = (-1)^v$ gäller det att:

- Om $v = 1$ är $\nu(t)$ udda och $2b - v + 2m - 1$ är jämnt.
- Om $v = 2$ är $\nu(t)$ jämnt och $2b - v + 2m - 1$ är udda.

Alltså är $\nu(t) \neq 2b - v + 2m - 1$, vilket avslutar beviset. □

Eftersom $\chi_v(d) \geq 0$ för alla $d|P(z)$ och $v = 1, 2$, får (3.8) formen

$$X \sum_{d|P(z)} \mu(d)\chi_2(d)\frac{\omega(d)}{d} - \sum_{d|P(z)} \chi_2(d)|R_d| \leq S(\mathcal{A}; \mathfrak{P}, z) \leq X \sum_{d|P(z)} \mu(d)\chi_1(d)\frac{\omega(d)}{d} + \sum_{d|P(z)} \chi_1(d)|R_d|. \tag{B.3}$$

Beviset utförs genom att uppskatta de olika summorna var för sig. Innan dess behöver vi följande uträkning [HR, s. 44].

Lemma B.2. *Låt p^+ beteckna det minsta primtalet större än p. Under villkoret (Ω_1) och för $v = 1, 2$, gäller det att*

$$\sum_{d|P(z)} \mu(d)\chi_v(d)\frac{\omega(d)}{d} = W(z)\left(1 + (-1)^{v-1}\sum_{p<z}\frac{\omega(p)}{p}\frac{W(p)}{W(z)}\sum_{t|P_{p^+,z}}\frac{\chi_v(t)(1-\chi_v(pt))}{t}\omega(t)\right).$$

Bevis. Vår utgångspunkt är

$$\sum_{p|d}\left(\chi_v((d, P_{p^+,z})) - \chi_v((d, P_{p,z}))\right) = 1 - \chi_v(d), \quad d \mid P(z).$$

För $d = 1$ är båda led lika med 0. För $d > 1$ skriver vi $d = p_1...p_r$ där $p_1 < ... < p_r$, eftersom d är kvadratfri. Vi får då

$$\begin{aligned}\sum_{p|d}(\chi_v((d, P_{p^+,z})) - \chi_v((d, P_{p,z}))) &= \sum_{i=1}^{r}(\chi_v((d, P_{p_i^+,z})) - \chi_v((d, P_{p_i,z}))) \\ &= \sum_{i=1}^{r-1}(\chi_v(p_{i+1}...p_r) - \chi_v(p_i...p_r)) + \chi_v(1) - \chi_v(p_r) = 1 - \chi_v(d).\end{aligned}$$

Vi löser ut $\chi_v(d)$ och får

$$\sum_{d|P(z)} \mu(d)\chi_v(d)\frac{\omega(d)}{d} = \sum_{d|P(z)} \mu(d)\frac{\omega(d)}{d} - \sum_{d|P(z)} \mu(d)\frac{\omega(d)}{d}\sum_{p|d}\left(\chi_v((d, P_{p^+,z})) - \chi_v((d, P_{p,z}))\right).$$

Den första summan är lika med $W(z)$ enligt Lemma A.2. I den andra summan skriver vi allt under båda summatecken och absorberar ett minustecken genom att ersätta $\mu(d)$ med $\mu(d/p)$. Vi erhåller då

$$W(z) + \sum_{d|P(z)}\sum_{p|d}\mu\left(\frac{d}{p}\right)\frac{\omega(d)}{d}\left(\chi_v((d, P_{p^+,z})) - \chi_v((d, P_{p,z}))\right). \tag{B.4}$$

Vi delar nu upp $d = \delta pt$ i tre faktorer, där p är ett primtal, δ innehåller alla primtalsfaktorer mindre än och t alla större än p (om inga sådana faktorer finns är δ respektive t lika med 1). De är parvis relativt prima och eftersom ω och μ är multiplikativa är dubbelsumman i (B.4) lika med

$$\sum_{\delta pt|P(z)} \sum_{\substack{\delta|P(p)\\ p|P(z)\\ t|P_{p^+,z}}} \mu(\delta t)\frac{\omega(\delta)}{\delta}\frac{\omega(p)}{p}\frac{\omega(t)}{t}\left(\chi_v(t)-\chi_v(pt)\right)$$

$$= \sum_{p|P(z)} \frac{\omega(p)}{p} \sum_{\delta|P(p)} \mu(\delta)\frac{\omega(\delta)}{\delta} \sum_{t|P_{p^+,z}} \mu(t)\frac{\omega(t)}{t}\left(\chi_v(t)-\chi_v(pt)\right). \quad \text{(B.5)}$$

Vidare har vi att om $pt|P(z)$ och p är mindre än den minsta primtalsfaktorn i t är

$$\chi_v(t)-\chi_v(pt) = (-1)^{v-1}\mu(t)\chi_v(t)(1-\chi_v(pt)). \quad \text{(B.6)}$$

För att verifiera det kontrollerar vi tre olika fall. Om $\chi_v(pt)=1$ har vi att $\chi_v(t)=1$ eftersom funktionerna χ_v genererar ett kombinatoriskt såll. I så fall är båda led lika med 0. Detsamma gäller om $\chi_v(pt)=0$ och $\chi_v(t)=0$. Om $\chi_v(pt)=0$ och $\chi_v(t)=1$ måste $\mu(t)=(-1)^{v-1}$, och (B.6) gäller även då.

Vi använder nu (B.6) i (B.5) och erhåller

$$(-1)^{v-1}\sum_{p|P(z)} \frac{\omega(p)}{p} \sum_{\delta|P(p)} \mu(\delta)\frac{\omega(\delta)}{\delta} \sum_{t|P_{p^+,z}} \mu^2(t)\frac{\omega(t)}{t}\left(\chi_v(t)(1-\chi_v(pt))\right) =$$

$$= (-1)^{v-1}\sum_{p|P(z)} \frac{\omega(p)}{p} W(p) \sum_{t|P_{p^+,z}} \frac{\omega(t)}{t}\left(\chi_v(t)(1-\chi_v(pt))\right).$$

Villkoret (Ω_1) tillåter oss att bryta ut $W(z)$, vilket avslutar beviset. □

Nästa steg i beviset av Sats 3.2 är att definiera talen z_n, $n=1,2,...,r$. Givet $\Lambda>0$, som kommer specificeras nedan, väljer vi r som det minsta naturliga talet så att $e^{-r\Lambda}\log z \le \log 2$. Det betyder att $\log 2 < e^{-(r-1)\Lambda}\log z$ samt att

$$e^{((r-1)\Lambda)/2} < \sqrt{\frac{\log z}{\log 2}}, \quad \text{(B.7)}$$

vilket är användbart nedan. Vi definierar z_n enligt

$$\begin{cases} \log z_n & = e^{-n\Lambda}\log z, \quad n = 1,2,...,r-1, \\ z_r & = 2. \end{cases} \quad \text{(B.8)}$$

Under dessa förutsättningar har vi följande egenskap hos $W(z)$ [HR, s. 59]. Vi påminner om att λ och c_1 introduceras i formuleringen av Sats 3.2.

Lemma B.3. *Med $z_n, n=1,2,...,r$ är definierade som i* (B.8) *gäller det att*

$$\frac{W(z_n)}{W(z)} \le e^{2(n\lambda+c)} \text{ för } n=1,2,...,r \text{ där } c=\frac{c_1}{\log z}.$$

Bevis. Under (Ω_1) och $(\Omega_2(\kappa))$ gäller olikheten

$$\frac{W(w)}{W(z)} \le \exp\left(\kappa\log\frac{\log z}{\log w}+\frac{A_2}{\log w}\left(1+A_1\kappa+\frac{A_1A_2}{\log 2}\right)\right), \quad 2\le w\le z.$$

Man kan visa olikheten med hjälp av partiell summation, men vi avstår från att göra det här utan hänvisar istället till [HR, s. 53-54]. Med definitionen av z_n och c_1 erhåller vi

$$\frac{W(z_n)}{W(z)} \le \exp\left(\kappa\log\frac{\log z}{\log z_n}+\frac{A_2}{\log z_n}\left(1+A_1\kappa+\frac{A_1A_2}{\log 2}\right)\right)$$

$$= \exp\left(\kappa\Lambda n+\frac{2c_1e^{n\Lambda}}{\log z}\right) = e^{2c}\exp\left(n\left(\kappa\Lambda+\frac{2c_1}{\log z}\frac{e^{n\Lambda}-1}{n}\right)\right) \quad \text{(B.9)}$$

då $n = 1, 2, ..., r-1$. Samma olikhet gäller för $n = r$, eftersom $\log z/\log 2 \le e^{r\Lambda}$.

Med elementära medel kan vi se att $(e^x - 1)/x$ är växande för $x > 0$. Med hjälp av definitionen för z_n får vi därför

$$\frac{e^{n\Lambda}-1}{n} \le \frac{e^{r\Lambda}-1}{r} \le \frac{e^{r\Lambda}\Lambda}{r\Lambda} \le \frac{\Lambda e^{\Lambda}\log z}{\log 2 \log(\log z/\log 2)}.$$

Insättning i (B.9) och utbrytning av $\kappa\Lambda$ i den inre parentesen ger

$$\frac{W(z_n)}{W(z)} \le e^{2c}\exp\left(n\Lambda\kappa\left(1 + \frac{2c_1 e^{\Lambda}}{\kappa\log 2}\frac{1}{\log(\log z/\log 2)}\right)\right).$$

Eftersom z är tillräckligt stort kan vi anta att

$$\frac{2c_1 e^{\Lambda}}{\kappa\log 2}\frac{1}{\log(\log z/\log 2)} \le \varepsilon,$$

där $\varepsilon = 1/(200e^{1/\kappa})$. För $\Lambda = 2\lambda/(\kappa(1+\varepsilon))$ får vi då att

$$\exp\left(n\Lambda\kappa\left(1 + \frac{2c_1 e^{\Lambda}}{\kappa\log 2}\frac{1}{\log(\log z/\log 2)}\right)\right) \le e^{2n\lambda},$$

så att

$$\frac{W(z_n)}{W(z)} \le e^{2(c+n\lambda)}. \tag{B.10}$$

□

Lemma B.4 och B.5 nedan är centrala, vilket vi förstår när vi jämför (3.8) med ekvationerna i Sats 3.2. De återfinns som [HR, ekvation (2.4.12) och (2.4.21)].

Lemma B.4. *För $v = 1, 2$, gäller det att*

$$\sum_{d|P(z)} \mu(d)\chi_v(d)\frac{\omega(d)}{d} = W(z)\left(1 + 2\theta\frac{\lambda^{2b-v+2}e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}}e^{(2b-v+4)c/\lambda}\right),$$

där $|\theta| \le 1$ och $c = c_1/\log z$.

Bevis. Enligt Lemma B.2 är

$$\frac{1}{W(z)}\sum_{d|P(z)} \mu(d)\chi_v(d)\frac{\omega(d)}{d} = 1 + (-1)^{v-1}\sum_{p<z}\frac{\omega(p)}{p}\frac{W(p)}{W(z)}\sum_{t|P_{p^+,z}}\frac{\chi_v(t)(1-\chi_v(pt))}{t}\omega(t).$$

Vi indexerar summan i högerledet utifrån talen z_n och erhåller

$$\sum_{n=1}^{r}\sum_{z_n \le p < z_{n-1}}\frac{\omega(p)}{p}\frac{W(p)}{W(z)}\sum_{t|P_{p^+,z}}\frac{\chi_v(t)(1-\chi_v(pt))}{t}\omega(t). \tag{B.11}$$

Om $z_n \le p$ är

$$W(p) = \prod_{p'<p}\left(1 - \frac{\omega(p')}{p'}\right) \le \prod_{p'<z_n}\left(1 - \frac{\omega(p')}{p'}\right) = W(z_n)$$

eftersom $W(p)$ innehåller minst lika många faktorer som $W(z_n)$ och varje faktor enligt (Ω_1) uppfyller

$$\frac{1}{A_1} \le \left(1 - \frac{\omega(p')}{p'}\right) \le 1.$$

En övre begränsning av (B.11) är därför

$$\sum_{n=1}^{r}\frac{W(z_n)}{W(z)}\sum_{z_n \le p < z_{n-1}}\frac{\omega(p)}{p}\sum_{t|P_{p^+,z}}\frac{\chi_v(t)(1-\chi_v(pt))}{t}\omega(t).$$

Den innersta summan innehåller termer som endast är nollskilda om $\chi_v(t) = 1$ och $\chi_v(pt) = 0$. Enligt definitionen av funktionerna χ_v måste i så fall $\nu(t) = 2b - v + 2n - 1$. Vi erhåller därför en övre begränsning i form av

$$\begin{aligned}
&\sum_{n=1}^{r} \frac{W(z_n)}{W(z)} \sum_{z_n \le p < z_{n-1}} \frac{\omega(p)}{p} \sum_{\substack{t | P_{p^+,z} \\ \nu(t)=2b-v+2n-1}} \frac{\omega(t)}{t} \\
&= \sum_{n=1}^{r} \frac{W(z_n)}{W(z)} \sum_{z_n \le p < z_{n-1}} \sum_{\substack{t | P_{p^+,z} \\ \nu(t)=2b-v+2n-1}} \frac{\omega(p)}{p} \frac{\omega(t)}{t} = \sum_{n=1}^{r} \frac{W(z_n)}{W(z)} \sum_{\substack{d | P_{z_n,z} \\ \nu(d)=2b-v+2n}} \frac{\omega(d)}{d}.
\end{aligned} \tag{B.12}$$

I sista steget gjorde vi omskrivningen $d = pt$. Eftersom $t | P_{p^+,z}$ gäller det att $(p, t) = 1$ och $\omega(p)\omega(t) = \omega(pt)$.

Vi betraktar den inre summan, och observerar att

$$\sum_{\substack{d | P_{z_n,z} \\ \nu(d)=2b-v+2n}} \frac{\omega(d)}{d} \le \frac{1}{(2b - v + 2n)!} \left(\sum_{z_n \le p < z} \frac{\omega(p)}{p} \right)^{2b-v+2n}. \tag{B.13}$$

Det beror på att vi i vänsterledet summerar vi över alla delare d med exakt $2b - v + 2n$ distinkta primtalsfaktorer i intervallet $[z_n, z)$. Alla dessa termer återfinns i högerledet, men på grund av den upprepade multiplikationen förekommer de $(2b - v + 2n)!$ gånger. Därför dividerar vi med den faktorn.

Med elementära medel kan vi se att

$$x \le \log \frac{1}{1 - x} \text{ då } 0 \le x < 1.$$

Det följer att

$$\sum_{z_n \le p < z} \frac{\omega(p)}{p} \le \sum_{z_n \le p < z} \log \frac{1}{1 - \omega(p)/p} = \log \Big(\prod_{z_n \le p < z} \frac{1}{1 - \omega(p)/p} \Big) = \log \frac{W(z_n)}{W(z)}. \tag{B.14}$$

Vi kan använda (B.14) för att fortsätta uppskatta (B.13) ovanifrån. Vi behöver också att

$$(2b - v + 2n)! = (2b - v + 2n)(2b - v + 2n - 1) \cdot ... \cdot (2n)! \ge (2n)^{2b-v}(2n)!.$$

Tillsammans med Lemma B.3, som säger att

$$\log \frac{W(z_n)}{W(z)} \le 2(n\lambda + c),$$

får vi att

$$\frac{1}{(2b - v + 2n)!} \left(\sum_{z_n \le p < z} \frac{\omega(p)}{p} \right)^{2b-v+2n} \le \frac{1}{(2n)!(2n)^{2b-v}} (2(c + n\lambda))^{2b-v+2n}. \tag{B.15}$$

Användning av Lemma B.3 och (B.15) ger oss en övre begränsning av högerledet i i (B.12) enligt

$$\sum_{n=1}^{r} e^{2(c+n\lambda)} \frac{(2(c + n\lambda))^{2b-v+2n}}{(2n)!(2n)^{2b-v}} \le e^{2c}(\lambda + c)^{2b-v} \sum_{n=1}^{r} \frac{(2ne^{-1})^{2n}}{(2n)!} \left(1 + \frac{c}{n\lambda}\right)^{2n} (\lambda e^{1+\lambda})^{2n},$$

där vi även använde att $\lambda + c/n \le \lambda + c$.

Vi betraktar nu de två första faktorerna i termerna i summan till höger. Vi vet att följden $(1 + c/n\lambda)^{2n}$, $n = 1, 2, ...$ är växande och uppåt begränsad av $e^{2c/\lambda}$. Följden $(2ne^{-1})^{2n}/(2n)!, n =$

$1, 2, \ldots$ är avtagande, vilket vi kan se om vi dividerar två termer med index n respektive $n+1$ med varandra. Följden är därför uppåt begränsad av $2e^{-2}$, vilket erhålls då $n = 1$. Vi får därmed

$$\begin{aligned}
e^{2c}(\lambda+c)^{2b-v}\sum_{n=1}^{r}\frac{(2ne^{-1})^{2n}}{(2n)!}\left(1+\frac{c}{n\lambda}\right)^{2n}(\lambda e^{1+\lambda})^{2n} &\leq 2e^{2c}(\lambda+c)^{2b-v}e^{2c/\lambda}e^{-2}\sum_{n=1}^{r}(\lambda e^{1+\lambda})^{2n} \\
\leq 2e^{2c}(\lambda+c)^{2b-v}e^{2c/\lambda}e^{-2}\sum_{n=1}^{\infty}(\lambda e^{1+\lambda})^{2n} &= 2\frac{\lambda^{2b-v+2}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{2c(1+1/\lambda)}(1+c/\lambda)^{2b-v} \\
&\leq 2\frac{\lambda^{2b-v+2}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{2c(1+1/\lambda)}e^{(2b-v)c/\lambda} \leq 2\frac{\lambda^{2b-v+2}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{(2b-v+4)c/\lambda}.
\end{aligned}$$

Den oändliga serien konvergerar eftersom $0 < \lambda e^{1+\lambda} < 1$. Ur samma olikhet följer även att $0 < \lambda < 1$, vilket vi använder i det allra sista steget.

Totalt får vi att

$$\frac{1}{W(z)}\sum_{d|P(z)}\mu(d)\chi_v(d)\frac{\omega(d)}{d} = \left(1+2\theta\frac{\lambda^{2b-v+2}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{(2b-v+4)c/\lambda}\right)$$

där $|\theta| \leq 1$ och $v = 1, 2$, vilket avslutar beviset. □

Anmärkning. Vi använder inte villkoret (R) i beviset, eftersom lemmat inte involverar resttermerna $|R_d|$.

Vi fortsätter nu med nästa viktiga beståndsdel till beviset av Sats 3.2.

Lemma B.5. *För $v = 1, 2$, gäller det att*

$$\sum_{d|P(z)}\chi_v(d)|R_d| = \mathcal{O}\left(z^{2b-v+1+2{,}01/(e^{2\lambda/\kappa}-1)}\right).$$

Bevis. Definitionen (3.11) säger att $\chi_v(d) = 1$ om och endast om d har som mest $2b - v + 2n - 1$ primtalsfaktorer i intervallet $[z_n, z)$ för alla $n = 1, 2, ..., r$ och $\chi_v(d) = 0$ annars. Eftersom $d|P(z)$ och ligger alla d:s primtalsfaktorer i $\mathfrak{P}$. Tillsammans med villkoret (R) får vi därför

$$\sum_{d|P(z)}\chi_v(d)|R_d| \leq \sum_{d|P(z)}\chi_v(d)\omega(d) \leq \left(1+\sum_{p<z}\omega(p)\right)^{2b-v+1}\prod_{n=1}^{r-1}\left(1+\sum_{p<z_n}\omega(p)\right)^2. \tag{B.16}$$

Några förklaringar är lämpliga. Den första olikheten följer direkt ur (R). För att visa den andra behöver vi motivera varför alla termer i det mittersta ledet förekommer i produkten i högerledet. För att se det börjar vi med att observera en undre begränsning av högerledet ges om vi multiplicerar ihop faktorerna och bortser från de termer som inte är kvadratfria. Kvar blir då termer på formen $\omega(d)$ där d är kvadratfri, eftersom ω är multiplikativ. Vi ska visa att alla termer i det mittersta ledet förekommer bland dessa.

Vi börjar med att observera att summan av exponenterna i högerledet är $2b-v+1+2(r-1) = 2b - v + 2r - 1$. Alla termer $\omega(d)$ i högerledet uppfyller därför att d som mest har $2b - v + 2r - 1$ primtalsfaktorer, vilket uppfyller kravet i Definition 3.11 för $n = r$. Vidare kan endast $2b - v + 1 + 2(r - 1) - 2 = 2b - v + 2(r - 1) - 1$ av primtalsfaktorerna ligga i intervallet $[z_{r-1}, z)$, eftersom alla faktorer i högerledet utom

$$\left(1+\sum_{p<z_{r-1}}\omega(p)\right)^2$$

inkluderar sådana primtal. Mer generellt kan som mest $2b-v+1+2(r-1-k) = 2b-v+2(r-k)-1$ primtalsfaktorer ligga i intervallet $[z_k, z)$ för $k = 1, 2, ..., r - 1$ eftersom alla faktorer utom

$$\prod_{n=k}^{r-1}\left(1+\sum_{p<z_n}\omega(p)\right)^2$$

innehåller sådana primtalsfaktorer. Det visar att termerna $\omega(d)$ i högerledet uppfyller kravet i Definition 3.11 för $r-k$ där $k=1,2,...,r-1$, det vill säga för $n=1,2,...,r-1$. Därmed förekommer alla termer i det mittersta ledet även i högerledet, och den andra olikheten i (B.16) gäller.

Vi använder nu olikheten i [HR, Lemma 2.4] och får

$$\begin{aligned}&\left(1+\sum_{p<z}\omega(p)\right)^{2b-v+1}\prod_{n=1}^{r-1}\left(1+\sum_{p<z_n}\omega(p)\right)^2\\&\qquad\leq(1+A(2\operatorname{li}z+3))^{2b-v+1}\prod_{n=1}^{r-1}(1+A(2\operatorname{li}z_n+3))^2,\quad A=\max(A_2,\kappa).\end{aligned}$$

Vi kan med elementära medel se att

$$\frac{z}{\log z}\geq 1,\quad z\geq 2.$$

Vidare har vi enligt Lemma A.6 att finns det någon konstant C_1 så att

$$\operatorname{li}z\leq\frac{C_1 z}{\log z},\quad z\geq 2.$$

Det följer att

$$1+A(2\operatorname{li}z_n+3)=1+3A+2A\operatorname{li}z\leq\frac{Cz}{\log z},\quad C=1+3A+2AC_1,\quad z\geq 2.$$

Tillsammans med definitionen av z_n erhåller vi då

$$\begin{aligned}&(1+A(2\operatorname{li}z+3))^{2b-v+1}\prod_{n=1}^{r-1}(1+A(2\operatorname{li}z_n+3))^2\\&\leq\left(\frac{Cz}{\log z}\right)^{2b-v+1}\prod_{n=1}^{r-1}\left(\frac{Cz_n}{\log z_n}\right)^2=\left(\frac{Cz}{\log z}\right)^{2b-v+1}\prod_{n=1}^{r-1}\left(\frac{Cz_ne^{n\Lambda}}{\log z}\right)^2\\&=\left(\frac{Cz}{\log z}\right)^{2b-v+1}\left(\frac{Ce^{r\Lambda/2}}{\log z}\right)^{2(r-1)}\prod_{n=1}^{r-1}z_n^2.\end{aligned}$$

Med egenskapen (B.7) får vi att

$$\frac{Ce^{r\Lambda/2}}{\log z}=\frac{Ce^{\Lambda/2}e^{(r-1)\Lambda/2}}{\log z}\leq\frac{Ce^{\Lambda/2}}{\log z}\sqrt{\frac{\log z}{\log 2}}<1,$$

eftersom z är tillräckligt stort. Produkten av z_n^2, $n=1,2,...,r-1$, uppskattar vi enligt

$$\prod_{n=1}^{r-1}z_n^2=\exp\left(\sum_{n=1}^{r-1}\log z_n^2\right)=\exp\left(2\log z\sum_{n=1}^{r-1}e^{-n\Lambda}\right)\leq\exp\left(2\log z\sum_{n=1}^{\infty}e^{-n\Lambda}\right)=z^{2/(e^\Lambda-1)}.$$

Från ovan följer att

$$\left(\frac{Cz}{\log z}\right)^{2b-v+1}\left(\frac{Ce^{r\Lambda/2}}{\log z}\right)^{r-1}\prod_{n=1}^{r-1}z_n^2\leq C^{2b-v+1}z^{2b-v+1}\cdot z^{2/(e^\Lambda-1)}=\mathcal{O}\left(z^{2b-v+1+2/(e^\Lambda-1)}\right),$$

vilket slutför beviset. □

Vi är nu redo för detta avsnitts huvudresultat.

Bevis av Sats 3.2. För begränsade z är beviset klart enligt anmärkningarna i avsnittets inledning. För tillräckligt stora z använder vi Lemma B.4 och B.5 på (B.3), varpå resultatet följer. □

B.3 Detaljer till Selbergs såll

Vi ger nedan de detaljer som krävs för en fullständig framställning av teorin i avsnitt 4.2. Vi uppskattar även $G(z)$ nedifrån i ett specialfall med koppling till primtalstvillingar.

B.3.1 Verifiering av detaljer från avsnitt 4.2

Vi inleder med att verifiera att $\lambda_1 = 1$ är ekvivalent med (4.9). Härledningen sker med hjälp av en variant av så kallad Möbiusinversion, som nämns i [HR, s. 121]. Vi har per definition av y_ℓ att

$$\sum_{\substack{\ell<\xi \\ \ell|P(z)}} \mu(\ell) y_\ell = \sum_{\substack{\ell<\xi \\ \ell|P(z)}} \mu(\ell) \sum_{\substack{d|P(z) \\ \ell|d<\xi}} \lambda_d \frac{\omega(d)}{d} = \sum_{\substack{d|P(z) \\ d<\xi}} \lambda_d \frac{\omega(d)}{d} \sum_{\ell|d} \mu(\ell) = \lambda_1,$$

där den sista likheten följer ur Lemma A.1. Detta visar (4.9).

Nu härleder vi värden på λ_d från våra val av y_ℓ från avsnitt 4.2. Vi antog vid optimeringen med avseende på y_ℓ att y_ℓ kunde väljas fritt, om de uppfyllde bivillkoret ovan. Vi motiverar nu detta. Antag att vi fritt har valt några tal y_ℓ. Först vill vi att

$$y_m = \sum_{\substack{d|P(z) \\ m|d<\xi}} \lambda_d \frac{\omega(d)}{d} = \sum_{\substack{d|P(z) \\ m|d<\xi}}{}' \lambda_d \frac{\omega(d)}{d}, \tag{B.17}$$

ska gälla för alla m eftersom det var så vi ursprungligen definierade y_m.

Vi fixerar ett k och multiplicerar (B.17) med $\mu(\ell)$ och summerar likheten över alla ℓ så att $m := k\ell \mid P(z)$, $k\ell < \xi$. Vi ser att för att (B.17) ska gälla är det då nödvändigt att

$$\sum_{\substack{k\ell|P(z) \\ k\ell<\xi}} \mu(\ell) y_{k\ell} = \sum_{\substack{k\ell|P(z) \\ k\ell<\xi}} \sum_{\substack{d|P(z) \\ k\ell|d<\xi}} \mu(\ell)\lambda_d \frac{\omega(d)}{d} = \sum_{\substack{d|P(z) \\ d<\xi}} \lambda_d \frac{\omega(d)}{d} \sum_{\ell|d/k} \mu(\ell) = \lambda_k \frac{\omega(k)}{k}.$$

Där vi återigen använt Lemma A.1 i sista likheten. Detta ger oss en unik kandidat till definitioner av λ_d för d sådana att $\omega(d) \neq 0$, vilka är de enda λ_d som påverkar teorin. Vi definierar därför

$$\lambda_d = \frac{d}{\omega(d)} \sum_{\substack{dm|P(z) \\ dm<\xi}} \mu(m) y_{dm} \tag{B.18}$$

för sådana d. Vi visar nu att definitionen medför att (B.17) är uppfylld. För ett fixt $\ell \mid P(z)$ har vi, givet (B.18), att

$$\begin{aligned}
\sum_{\substack{d|P(z) \\ \ell|d<\xi}} \lambda_d \frac{\omega(d)}{d} &= \sum_{\substack{d|P(z) \\ \ell|d<\xi}} \sum_{\substack{dm|P(z) \\ dm<\xi}} \mu(m) y_{dm} = \sum_{\substack{d|P(z) \\ \ell|d<\xi}} \sum_{\substack{k|P(z) \\ d|k<\xi}} \mu(k/d) y_k \\
&= \sum_{\substack{k|P(z) \\ k<\xi}} y_k \sum_{\substack{d|k \\ \ell|d}} \mu(k/d) = \sum_{\substack{k|P(z) \\ k<\xi}} y_k \sum_{d|k/\ell} \mu(d) = y_\ell,
\end{aligned}$$

återigen enligt Lemma A.1. Detta var precis det vi ville visa. Alltså ger varje val av y_ℓ upphov till väldefinierade λ_d som uppfyller (B.17).

Nu verifierar vi (4.11) för kvadratfria d sådana att $\omega(d) \neq 0$. Vi använder (B.18) och valet av y_ℓ från avsnitt 4.2 för att erhålla

$$\frac{\omega(d)}{d} \lambda_d = \sum_{\substack{d\ell|P(z) \\ d\ell<\xi}} \mu(\ell) y_{d\ell} = \sum_{\substack{d\ell|P(z) \\ d\ell<\xi}} \mu(\ell)\mu(d\ell) \frac{g(d\ell)}{G(\xi, z)} = \frac{\mu(d) g(d)}{G(\xi, z)} \sum_{\substack{d\ell|P(z) \\ \ell<\xi/d}} \mu^2(\ell) g(\ell),$$

där vi använt att g är multiplikativ och att $(d, \ell) = 1$ eftersom $P(z)$ är kvadratfri. Den sista summan är precis $G_d(\xi/d, z)$ från (4.10) eftersom $P(z)$ är kvadratfri. Tillsammans med definitionen (4.5) av g visar detta

$$\lambda_d = \frac{\mu(d)}{\prod_{p|d}(1 - \omega(p)/p)} \frac{G_d(\xi/d, z)}{G(\xi, z)},$$

vilket är (4.11).

Det återstår att visa $|\lambda_d| \leq 1$. Vi följer strategin i [HR, avsnitt 6.1] och visar olikheten

$$G(\xi, z) \geq \frac{G_d(\xi/d, z)}{\prod_{p|d}(1-\omega(p)/p)},$$

som tillsammans med $|\mu(d)| \leq 1$ implicerar att $|\lambda_d| \leq 1$. Vi inleder med att observera att för $d \mid P(z)$ har vi, genom att summera över alla delare till d,

$$\begin{aligned} G(\xi, z) &= \sum_{\ell|d} \sum_{\substack{m<\xi \\ m|P(z) \\ (m,d)=\ell}} \mu^2(m)g(m) = \sum_{\ell|d} \sum_{\substack{h<\xi/\ell \\ h|P(z) \\ (h,d)=1}} \mu^2(h\ell)g(h\ell) = \sum_{\ell|d} \mu^2(\ell)g(\ell)G_d(\xi/\ell, z) \\ &\geq \sum_{\ell|d} \mu^2(\ell)g(\ell)G_d(\xi/d, z) = G_d(\xi/d, z)\prod_{p|d}(1+g(p)), \end{aligned}$$

där olikheten följer av att G_d är växande i sitt första argument och sista likheten är Lemma A.3. Det följer direkt från definitionen (4.4) att den sista produkten är

$$\prod_{p|d} \frac{1}{(1-\omega(p)/p)},$$

precis som önskat. Nu följer $|\lambda_d| \leq 1$.

B.3.2 Uppskattning av $1/G(z)$

Vi ska här redovisa några av räkningarna som leder fram till (4.18). De följer [HR, s. 113-115].

För vårt val av ω har vi (4.17), vilket ger att

$$g(p) = \frac{\omega(p)}{p\left(1-\frac{\omega(p)}{p}\right)} = \frac{1}{(p-1)\left(1-\frac{1}{p-1}\right)} = \frac{1}{p-1}\left(1+\frac{1}{p-2}\right)$$

så länge $p \nmid h$, och $g(p) = 0$ om $p|h$. Eftersom g är multiplikativ, $g(p) = 1/(p-2)$ och $p-1 = \phi(p)$ får vi med Lemma A.3 att

$$g(d) = \prod_{p|d} \frac{1}{\phi(p)}(1+g(p)) = \frac{1}{\phi(d)} \sum_{\ell|d} g(\ell).$$

Detta gäller så länge $(d, h) = 1$.

Med definitionen av $G(z)$ och vårt val av ω får vi

$$G(z) = \sum_{\substack{d<z \\ (d,h)=1}} \mu^2(d)g(d) = \sum_{\substack{d<z \\ (d,h)=1}} \frac{\mu^2(d)}{\phi(d)} \sum_{\ell|d} g(\ell).$$

Genom att skriva $d = m\ell$ och byta summationsordning har vi även

$$\sum_{\substack{\ell<z \\ (\ell,h)=1}} \frac{\mu^2(\ell)g(\ell)}{\phi(\ell)} \sum_{\substack{m<z/\ell \\ (m,h)=1 \\ (m,\ell)=1}} \frac{\mu^2(m)}{\phi(m)}.$$

Man kan visa [HR, Lemma 3.1] att den inre summan kan uppskattas nedifrån av

$$\prod_{p|h\ell}\left(1-\frac{1}{p}\right)\log\frac{z}{\ell}$$

Logaritmen skriver vi om som $\log z - \log \ell$ och får två summor att hantera separat. Efter en del manipulationer, där vi bland annat utnyttjar att $g(p) = 1/(p-2)$ då $p \nmid h$, får vi att

$$G(z) \geq \prod_{p|h}\left(1-\frac{1}{p}\right)\prod_{p\nmid h}\left(1+\frac{1}{p(p-2)}\right)\left(\log z - \sum_{p}\frac{\log p}{(p-1)^2}\right). \tag{B.19}$$

Observera att den sista summan är konvergent. Om vi inverterar (B.19) följer (4.18) efter några elementära omskrivningar.

B.4 Detaljer till Chens sats

Vi ger här de detaljer som utelämnats från kapitel 6. Vi inleder med att motivera omskrivningen av summor från avsnitt 6.2. Därefter uppskattar vi produkten $W(N^{1/10})$ från avsnitt 6.3. Vi presenterar sedan grundläggande teori om Dirichletkaraktärer som vi har nytta av. Till slut formulerar vi ett lemma och begränsar två summor från avsnitt 6.4.

B.4.1 Omskrivning av summor

Vi undersöker detaljerna i hur omskrivningen av summorna i (6.2) leder fram till de i (6.4). Vi avlägsnar villkoren implicerade av $\sum'$, byter summationsgräns till $p \leq N$, och undersöker summorna termvis. Den första är lika med

$$\sum_{\substack{p \leq N \\ (p+h, P(N^{1/10}))=1}} 1 = \sum_{\substack{a \in \mathcal{L} \\ (a, P(N^{1/10}))=1}} 1 = S(\mathcal{L}; \mathfrak{P}_h, N^{1/10})$$

enligt definitionen av $S(\mathcal{A}; \mathfrak{P}, z)$. Den andra är lika med

$$\begin{aligned}\sum_{\substack{p \leq N \\ (p+h, P(N^{1/10}))=1}} \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 | p+h, p_1 \in \mathfrak{P}_h}} 1 &= \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \in \mathfrak{P}_h}} \sum_{\substack{p \leq N \\ (p+h, P(N^{1/10}))=1 \\ p_1 | p+h}} 1 \\ &= \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \in \mathfrak{P}_h}} \sum_{\substack{a \in \mathcal{L}_{p_1} \\ (a, P(N^{1/10}))=1}} 1 = \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \in \mathfrak{P}_h}} S(\mathcal{L}_{p_1}; \mathfrak{P}_h, N^{1/10}).\end{aligned}$$

Slutligen har vi

$$\begin{aligned}\sum_{\substack{p \leq N \\ (p+h, P(N^{1/10}))=1}} \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 | p+h, p_1 \in \mathfrak{P}_h}} \sum_{\substack{N^{1/3} \leq p_2 < (N/p_1)^{1/2} \\ p_2 | p+h, p_2 \in \mathfrak{P}_h \\ p+h = p_1 p_2 p_3}} 1 \\ = \sum_{\substack{N^{1/10} \leq p_1 < N^{1/3} \\ p_1 \in \mathfrak{P}_h}} \sum_{\substack{N^{1/3} \leq p_2 < (N/p_1)^{1/2} \\ p_2 \in \mathfrak{P}_h}} \sum_{\substack{p \leq N \\ (p+h, P(N^{1/10}))=1 \\ p+h = p_1 p_2 p_3}} 1\end{aligned}$$

och om vi utelämnar villkoret $(p+h, P(N^{1/10})) = 1$ får vi en övre begränsning av den inre summan enligt

$$\sum_{\substack{p \leq N \\ p+h = p_1 p_2 p_3}} 1 = \left| \left\{ p_3 : p_3 \leq \frac{N}{p_1 p_2}, p_1 p_2 p_3 - h = p \right\} \right| + \mathcal{O}_h(1).$$

Vi har bytt till en summation över p_3 istället för p. Den övre begränsningen ges egentligen av $(N+h)/(p_1 p_2)$ eftersom $p_1 p_2 p_3 - h = p \leq N$, men primtalen mellan $N/p_1 p_2$ och $(N+h)/p_1 p_2$ har vi samlat i $\mathcal{O}_h(1)$-termen.

B.4.2 Uppskattning av en produkt

Vi härleder här den undre begränsningen för $W(N^{1/10})$ från avsnitt 6.3. Vi kommer nedan skriva w för $N^{1/10}$. Uppskattningen inleds med observationen

$$\begin{aligned}&\prod_{p<w} \left(1 - \frac{\omega(p)}{p}\right) = \prod_{\substack{p \nmid h \\ p<w}} \left(1 - \frac{1}{p-1}\right) \\ &= \prod_{p \nmid h} \left(\frac{1 - 1/(p-1)}{1 - 1/p}\right) \prod_{p | h} \frac{p}{p-1} \prod_{\substack{p<w \\ p \nmid h}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \nmid h \\ p \geq w}} \left(\frac{1 - 1/p}{1 - 1/(p-1)}\right) \prod_{p | h} \left(1 - \frac{1}{p}\right).\end{aligned} \tag{B.20}$$

De tre sista produkterna kan skrivas som

$$\prod_{p<w}\left(1-\frac{1}{p}\right)\prod_{\substack{p\nmid h\\ p\geq w}}\left(1+\frac{1}{p(p-2)}\right)\prod_{\substack{p\mid h\\ p\geq w}}\left(1-\frac{1}{p}\right). \tag{B.21}$$

Vi ser omedelbart att den mittersta produkten är större än 1. Den sista produkten kan uppskattas till

$$\left(1+\mathcal{O}\left(\frac{1}{w}\right)\right),$$

genom att ta logaritmen och Taylorutveckla och sen använda

$$\sum_{\substack{p\mid h\\ p\geq w}}\frac{1}{p}\leq\frac{\nu(h)}{w}\ll\frac{1}{w}.$$

Notera att den implicerade konstanten beror på h. För att uppskatta den första produkten i (B.21) använder vi Lemma A.12. Totalt kan vi begränsa (B.20) underifrån med

$$W(N^{1/10})\geq\prod_{p\nmid h}\left(\frac{1-1/(p-1)}{1-1/p}\right)\prod_{p\mid h}\frac{p}{p-1}\frac{10e^{-\gamma}}{\log N}\left(1+\mathcal{O}\left(\frac{1}{\log N}\right)\right).$$

En omskrivning leder till produkten

$$20e^{-\gamma}\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{2<p\mid h}\frac{p-1}{p-2}\frac{1}{\log N}\left(1+\mathcal{O}\left(\frac{1}{\log N}\right)\right),$$

vilket var det vi ville hitta.

B.4.3 Dirichletkaraktärer

Vi redogör här för några egenskaper hos Dirichletkaraktärer χ modulo ℓ. Låt n vara sådant att $(n,\ell)=1$. Vi vet enligt Sats A.5 att $n^{\phi(\ell)}\equiv 1 \bmod \ell$. Därmed har vi på grund av periodiciteten och multiplikativiteten att $(\chi(n))^{\phi(\ell)}=\chi(n^{\phi(\ell)})=\chi(1)=1$ så att $\chi(n)$ är en enhetsrot.

En annan viktig egenskap hos Dirichletkaraktärer modulo ℓ är att det finns precis $\phi(\ell)$ stycken. Beviset är relativt tekniskt och utelämnas, men återfinns i till exempel [D, s. 27-28]. Det vi kommer ha störst användning av är följande resultat från [D, s. 30].

Lemma B.6. *Vi har*

$$\sum_{\chi}\chi(n)=\phi(\ell)\mathbf{1}_{\{n\equiv 1\ mod\ \ell\}},$$

där $\mathbf{1}$ *är indikatorfunktionen och summationen sker över alla Dirichletkaraktärer modulo* ℓ*.*

Lemmats användningsområde kommer vara att skriva om en indikatorfunktion som en summa av karaktärer. Det kan tyckas vara ett svårare uttryck att hantera, men det visar sig vara möjligt att uppskatta väl.

B.4.4 Begränsning av en summa

Vi presenterar här resultatet [HR, Lemma 11.1] som används i uppskattningen av S_0 i nästa avsnitt.

Lemma B.7. *För tillräckligt stora* N *gäller det att*

$$\sum_{p_1p_2\in\mathcal{P}_N}\frac{1}{p_1p_2\log(N/p_1p_2)}<\frac{0{,}493}{\log N}.$$

Bevis. Vi skriver om summan enligt

$$\sum_{N^{1/10}\le p_1<N^{1/3}} \frac{1}{p_1} \sum_{N^{1/3}\le p_2<(N/p_1)^{1/2}} \frac{1}{p_2} \frac{1}{\log{(N/p_1p_2)}} \tag{B.22}$$

och betraktar först den inre summan. Vi ska använda partiell summation i form av Lemma A.8 och låter därför $a_n = 1/n$ då n är ett primtal större än eller lika med $N^{1/3}$, och 0 annars. Då blir

$$A(t) = \sum_{N^{1/3}\le p<t} \frac{1}{p} = \log\left(\frac{\log t}{\log N^{1/3}}\right) + \mathcal{O}\left(\frac{1}{\log N}\right), \tag{B.23}$$

enligt Lemma A.9. Vi låter också $f(t) = 1/\log{(N/p_1t)}$ varpå den inre summan i (B.22) är lika med

$$A((N/p_1)^{1/2})f((N/p_1)^{1/2}) - A(N^{1/3})f(N^{1/3}) - \int_{N^{1/3}}^{(N/p_1)^{1/2}} A(t)f'(t)dt. \tag{B.24}$$

Vi noterar direkt att $A(N^{1/3})f(N^{1/3}) = 0$. Vi har också att

$$A((N/p_1)^{1/2})f((N/p_1)^{1/2}) = \log\left(\frac{\log{(N/p_1)^{1/2}}}{\log N^{1/3}}\right) f((N/p_1)^{1/2}) + \mathcal{O}\left(\frac{1}{\log^2 N}\right),$$

där den sista resttermen får sin form av att

$$f((N/p_1)^{1/2}) = \frac{1}{\log((N/p_1)^{1/2})} = \mathcal{O}\left(\frac{1}{\log N}\right).$$

Enligt (B.23) kan vi skriva om integralen i (B.24) enligt

$$\begin{aligned}
&\int_{N^{1/3}}^{(N/p_1)^{1/2}} \log\left(\frac{\log t}{\log N^{1/3}}\right) f'(t)dt + \mathcal{O}\left(\frac{1}{\log N}\right) \int_{N^{1/3}}^{(N/p_1)^{1/2}} f'(t)dt \\
&\qquad = \log\left(\frac{\log{(N/p_1)^{1/2}}}{\log N^{1/3}}\right) f((N/p_1)^{1/2}) - \int_{N^{1/3}}^{(N/p_1)^{1/2}} \frac{f(t)}{t\log t}dt + \mathcal{O}\left(\frac{1}{\log^2 N}\right),
\end{aligned}$$

där vi även använt partiell integration. I den sista resttermen använde vi att $f((N/p_1)^{1/2})$ och $f(N^{1/3})$ är av storlek $\mathcal{O}(1/(\log N))$ eftersom $N^{1/10} \le p_1 < N^{1/3}$. Vi får därför att uttrycket i (B.24) är lika med

$$\int_{N^{1/3}}^{(N/p_1)^{1/2}} \frac{f(t)}{t\log t}dt + \mathcal{O}\left(\frac{1}{\log^2 N}\right)$$

eftersom huvudtermen i $A((N/p_1)^{1/2})f((N/p_1)^{1/2})$ förekommer både där och med motsatt tecken i integralomskrivningen, och därför försvinner.

Sammanfattningsvis har vi att summan i (B.22) är lika med

$$\begin{aligned}
&\sum_{N^{1/10}\le p_1<N^{1/3}} \frac{1}{p_1}\left(\int_{N^{1/3}}^{(N/p_1)^{1/2}} \frac{f(t)}{t\log t}dt + \mathcal{O}\left(\frac{1}{\log^2 N}\right)\right) \\
&\qquad = \sum_{N^{1/10}\le p_1<N^{1/3}} \frac{1}{p_1} \int_{N^{1/3}}^{(N/p_1)^{1/2}} \frac{f(t)}{t\log t}dt + \mathcal{O}\left(\frac{1}{\log^2 N}\right) \sum_{N^{1/10}\le p_1<N^{1/3}} \frac{1}{p_1}.
\end{aligned} \tag{B.25}$$

Den sista summan i (B.25) uppskattar vi med Lemma A.9 enligt

$$\log\left(\frac{\log N^{1/3}}{\log N^{1/10}}\right) + \mathcal{O}\left(\frac{1}{\log N}\right) = \mathcal{O}(1),$$

så att den sista resttermen är på formen $\mathcal{O}(1/\log^2 N)$.

Det återstår att behandla den yttre summan i (B.25). För det använder vi återigen Lemma A.8. Den här gången låter vi $a_n = 1/n$ då n är ett primtal större än eller lika med $N^{1/10}$, och 0 annars. Då får $A(t)$ samma form som tidigare, med $N^{1/10}$ som undre summationsgräns istället för $N^{1/3}$. Vi sätter

$$g(t) = \int_{N^{1/3}}^{(N/t)^{1/2}} \frac{1}{u \log u \log (N/tu)} du$$

varpå summan i högerledet i (B.25) är lika med

$$A(N^{1/3})g(N^{1/3}) - A(N^{1/10})g(N^{1/10}) - \int_{N^{1/10}}^{N^{1/3}} A(t)g'(t)dt. \tag{B.26}$$

Det följer direkt ur definitionen att $g(N^{1/3}) = 0$, och som tidigare är $A(N^{1/10}) = 0$. Således försvinner de två första termerna. Med partiell integration får vi att integralen i (B.26) är lika med

$$\begin{aligned}
&\int_{N^{1/10}}^{N^{1/3}} \log\left(\frac{\log t}{\log N^{1/10}}\right) g'(t)dt + \mathcal{O}\left(\frac{1}{\log N}\right) \int_{N^{1/10}}^{N^{1/3}} g'(t)dt \\
&\qquad = - \int_{N^{1/10}}^{N^{1/3}} \frac{g(t)}{t \log t} dt + \mathcal{O}\left(\frac{1}{\log N}\right) g(N^{1/10})
\end{aligned}$$

och

$$g(N^{1/10}) = \int_{N^{1/3}}^{N^{9/20}} \frac{1}{u \log u} \frac{1}{\log (N^{9/10}/u)} du = \mathcal{O}\left(\frac{1}{\log N}\right),$$

eftersom $N^{1/3} \leq u \leq N^{9/20}$. Vi får därför att summan i (B.22) är lika med

$$\int_{N^{1/10}}^{N^{1/3}} \frac{1}{t \log t} \int_{N^{1/3}}^{(N/t)^{1/2}} \frac{1}{u \log u} \frac{1}{\log (N/tu)} dudt + \mathcal{O}\left(\frac{1}{\log^2 N}\right).$$

Med variabelbytet $t = N^x$, $u = N^y$ får vi

$$\int_{1/10}^{1/3} \frac{1}{x} \int_{1/3}^{(1-x)/2} \frac{1}{y(1-x-y)} dydx \frac{1}{\log N} + \mathcal{O}\left(\frac{1}{\log^2 N}\right).$$

Numerisk integration av dubbelintegralen ger den övre begränsningen 0,493, vilket slutför beviset. □

B.4.5 Avslutande uppskattningar

Vi genomför här uppskattningarna av de två första summorna i (6.22). Uppskattningen formuleras i termer av lemman i [HR, avsnitt 11.3] och hela denna del följer bevisen där, men med ytterligare detaljer tillagda. Av våra kommentarer i anslutning till introduktionen av ekvation (6.22) vet vi att den första summan är

$$\frac{1}{G(z)} \sum_{m \leq N} \Lambda_0(m). \tag{B.27}$$

Per definition är summan innehållande $\Lambda_0(m)$ lika med

$$\sum_{m \leq N} \sum_{\substack{p_1 p_2 n = m \\ p_1 p_2 \in \mathcal{P}_N}} \frac{\Lambda(n)}{\log(N/(p_1 p_2))},$$

där det kommer vara fördelaktigt att betrakta den inre summationen som en summation över $p_1 p_2$ och där vi tolkar n som $m/(p_1 p_2)$ så att vi efter byte av summationsordning kan betrakta summan över m som en summa över n. Bytet ger tillsammans med Korollarium A.15 och Lemma B.7 att

$$\begin{aligned}
&\sum_{p_1 p_2 \in \mathcal{P}_N} \frac{1}{\log(N/(p_1 p_2))} \sum_{n \leq N/(p_1 p_2)} \Lambda(n) \\
&= N \left(1 + \mathcal{O}\left(\frac{1}{\log N}\right)\right) \sum_{p_1 p_2 \in \mathcal{P}_N} \frac{1}{p_1 p_2 \log(N/(p_1 p_2))} \leq \frac{0{,}493 N}{\log N}
\end{aligned} \tag{B.28}$$

för tillräckligt stora N. Vi använder här i feltermen att $N^{1/3} \leq N/(p_1p_2) \leq N$. Vi använder nu uppskattningen av $G(z)$ från (4.18) och påminner oss om att z ungefär är lika med $N^{1/4}$. Med $\varepsilon < 10^{-5}$ kan uttrycket i (B.27) då begränsas strikt av

$$3{,}95 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|h} \frac{p-1}{p-2} \frac{N}{\log^2 N} \left(1 + \mathcal{O}\left(\frac{1}{\log N}\right)\right). \tag{B.29}$$

Efter att ha förenklat den första summan fokuserar vi nu på den andra summan S_2. Vi påminner om att

$$S_2 = \sum_{\substack{D<z^2 \\ D|P(z)}} \frac{\mu^2(D)3^{\nu(D)}}{\phi(D)} \sum_{\substack{m \leq N \\ (D,m)>1}} \Lambda_0(m). \tag{B.30}$$

Faktorn $\mu^2(D)$ är egentligen redundant eftersom $D \mid P(z)$, men det kommer vara användbart att behålla den. Vi undersöker nu den inre summan. Notera att $m = p_1p_2n$ som ovan. Vi har villkoret $(m, D) > 1$, vilket vi kan skriva som $(p_1p_2n, D) > 1$. Vi vet från definitionen att $p_2 \geq N^{1/3} > z$, så de möjliga fallen är $(p_1, D) > 1$ och $(n, D) > 1$. Vi byter summationsordning som i (B.28) och får

$$\begin{aligned} \sum_{\substack{m \leq N \\ (m,D)>1}} \Lambda_0(m) \leq & \sum_{p_1p_2 \in \mathcal{P}_N} \frac{1}{\log(N/(p_1p_2))} \sum_{\substack{n \leq N/(p_1p_2) \\ (n,D)>1}} \Lambda(n) \\ & + \sum_{\substack{p_1p_2 \in \mathcal{P}_N \\ p_1|D}} \frac{1}{\log(N/(p_1p_2))} \sum_{n \leq N/(p_1p_2)} \Lambda(n). \end{aligned} \tag{B.31}$$

För den första summan kan vi notera att vi enligt definitionen av Λ har

$$\sum_{\substack{n \leq x \\ (n,D)>1}} \Lambda(n) = \sum_{p|D} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \leq (\log x)\nu(D).$$

Om vi sätter $x = N/p_1p_2$ ser vi att hela första summan kan begränsas av

$$\nu(D)|\mathcal{P}_N| \leq \nu(D)N^{2/3}.$$

Vi byter nu summationsordning i andra summan i (B.31) och tar bort några av villkoren på p_1, p_2 för att få en begränsning av andra summan till

$$\sum_{n \leq N} \Lambda(n) \sum_{\substack{N^{1/10} \leq p_1 < N/n \\ p_1|D,\, p_1 \leq N^{1/3}}} \sum_{\substack{p_2 \leq N/(p_1n) \\ p_2 \leq (N/p_1)^{1/2}}} \frac{1}{\log(N/(p_1p_2))}.$$

Den innersta summanden är begränsad av $1/\log N^{1/3} \ll 1/\log N$ så att hela innersta summan är $\ll N/(p_1 n \log N)$. Därmed är summan

$$\ll \frac{N}{\log N} \sum_{n \leq N} \frac{\Lambda(n)}{n} \sum_{\substack{N^{1/10} \leq p_1 \\ p_1|D}} \frac{1}{p_1} \leq \frac{N^{9/10}\nu(D)}{\log N} \sum_{n \leq N} \frac{\Lambda(n)}{n} \ll N^{9/10}\nu(D),$$

där vi i sista steget använt Korollarium A.15 tillsammans med partiell summation i form av Lemma A.8. Totalt är alltså summan i vänsterledet av (B.31) $\ll \nu(D)N^{9/10}$.

Insättning i (B.30) ger tillsammans med Lemma A.11 och Lemma A.13

$$S_2 \ll N^{9/10} \sum_{\substack{D<z^2 \\ D|P(z)}} \frac{\mu^2(D)3^{\nu(D)}\nu(D)}{\phi(D)} \ll N^{9/10} \sum_{D<z^2} \frac{\mu^2(D)3^{\nu(D)} \log^2 D}{D}.$$

Eftersom $\log z^2 \leq \log N$ kan vi begränsa uttrycket ovan med

$$N^{9/10} \log^2 N \sum_{D<z^2} \frac{\mu^2(D) 3^{\nu(D)}}{D}.$$

Den sista uppskattningen sker nu med samma metod som i beviset av [HR, Lemma 3.4]. Antalet sätt att skriva det kvadratfria talet D som en produkt av tre heltal är precis $3^{\nu(D)}$ enligt elementär kombinatorik. Därmed har vi

$$\sum_{D<z^2} \frac{\mu^2(D) 3^{\nu(D)}}{D} = \sum_{d_1 d_2 d_3 < z^2} \frac{\mu^2(d_1 d_2 d_3)}{d_1 d_2 d_3} \leq \left(\sum_{n<z^2} \frac{1}{n} \right)^3,$$

eftersom den sista summan innehåller alla produkter av tal mindre än z^2. En integraljämförelse visar att den sista summan är $\ll \log^3 z^2 \ll \log^3 N$. Totalt har vi alltså

$$S_2 \ll N^{9/10} \log^5 N. \tag{B.32}$$