

Gert Buschmann

Analytisk Talteori

Trykværket

Forord

Denne bog forudsætter en smule kendskab til kompleks funktionsteori, og dens emne er denne teoris anvendelse til at udlede Riemanns eksakte formel for antallet af primtal mindre end et givet tal og Hardy & Littlewoods tilnærmelsesformel for antallet af opspaltninger af et givet lige tal i summen af to primtal.

Bogen er en introduktion til denne teori, derfor er beviserne kun skitseagtige. Det primære er at vise, hvordan man kan lave de relevante computerprogrammer.

Programmerne nævnt i bogen kan hentes fra en internetadresse. Der er vedlagt en kompiler og alle de programmer som forfatteren har lavet til bogens udregninger og illustrationer.

Indhold

Opspaltning i primfaktorer

Möbius-inversion

Antallet af primtal mindre end et givet tal

Goldbachs formodning

Matematikkens grundlag

Komplekse funktioner

Euler-Maclaurins sumformel

Fourier-inversion

Mertens formodning

Udledning af Riemanns formel

Udledning af Hardy & Littlewoods formel

Vinogradovs teori

Litteratur og computerprogrammer

Opspaltning i primfaktorer

Ethvert naturligt tal kan skrives som et produkt af primtal, og hvis primtallene opskrives efter størrelse, er fremstillingen entydig. At et naturligt tal *kan* skrives som et produkt af primtal, følger af definitionen af et primtal. Men at denne opspaltning er entydig på nær faktorernes orden, er ikke indlysende: den gælder ikke i almindelighed for algebraiske tallegemer. De sædvanlige hele tal er de *hele tal* i det algebraiske tallegeme \mathbb{Q} = mængden af de rationale tal. I det algebraiske tallegeme $\mathbb{Q}(\sqrt{6})$ er de *hele tal* tallene af formen $m+n\sqrt{6}$, hvor m og n er sædvanlige hele tal, og her er for eksempel $6 = 2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}$, og 2, 3 og $\sqrt{6}$ er *primtal* i $\mathbb{Q}(\sqrt{6})$. For de sædvanlige hele tal kaldes entydigheden af primtalsfremstillingen for *aritmetikkens fundamentalsætning*. Den blev selvfølgelig erkendt og bevist af de gamle grækere. De formulerede dog tingene på en anden måde end vi gør, men sætningen følger af Theorem 14 i *Euklid* bog IX. I Euklid bliver det også bevist, at der er uendeligt mange primtal. Dette bevis lyder kort fortalt, at hvis der kun var endeligt mange primtal og man gangede dem allesammen med hinanden og adderede 1 til, så ville dette tal både være og ikke være et primtal.

Lad n være det tal som skal undersøges. Vi deler først n med 2, så mange gange det er muligt (hvis det er muligt), og derefter med 3, så mange gange det er muligt. Og dette fortsættes for de ulige tal 5, 7, 11, ..., men kun hvis et sådant tal d er et primtal, og d er et primtal, hvis ingen af de ulige tal fra 3 til \sqrt{d} går op i d , i så fald deles n med d , så mange gange det er muligt. I hvert tilfælde udskrives primtallet d efterfulgt af dette antal: d 's *multiplicitet* i n . Det tal der er tilbage, kaldes igen n , og proceduren gentages så længe det er muligt: er det sidste $n > 1$, er det et primtal, og det udskrives med multiplicitet 1. Programmet "PrimePart".

Möbius-inversion

En funktion som er defineret på mængden af de naturlige tal (og hvis værdier er hele eller reelle eller komplekse tal), kaldes en *talteoretisk funktion*. For eksempel funktionen $\rho(n)$ defineret ved $\rho(n) =$ summen af alle primfaktorerne i n (vi har $\sigma(117) = \sigma(3 \cdot 3 \cdot 13) = 3 + 3 + 13 = 19$) - for denne funktion gælder $\sigma(mn) = \sigma(m) + \sigma(n)$, den har altså logaritmeegenskaben (men er selvfølgelig ikke bijektiv).

I det følgende vil vi hyppigt møde *Möbius' funktion* $\mu(n)$. Den er defineret ved $\mu(n) = (-1)^f$, hvis n er produktet af netop r forskellige primtal og ellers 0 (vi har $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$). $\mu(n)$ opfylder $\mu(mn) = \mu(m)\mu(n)$, når m og n er indbyrdes primiske, i modsat fald er $\mu(mn) = 0$. $\mu(n)$ har den egenskab, at for ethvert naturligt tal n er summen af tallene $\mu(d)$ for *alle* divisorerne d i n lig 0, undtagen for $n = 1$, idet $\mu(1) = 1$. Og denne egenskab giver anledning til fænomenet *Möbius-inversion*: hvis $f(x)$ er en funktion defineret på mængden af de reelle eller komplekse tal, og vi definerer funktionen $F(x)$ ved

$$F(x) = \sum_{m=1}^{\infty} f(mx)/m$$

så kan vi udtrykke $f(x)$ ved $F(x)$ ved i denne formel at indføre $\mu(n)$

$$f(x) = \sum_{n=1}^{\infty} \mu(n)F(nx)/n$$

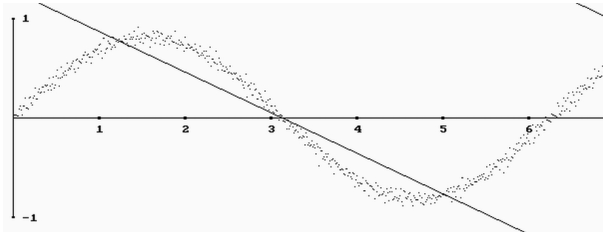
- forudsat naturligvis, at de to rækker konvergerer. Dette vises simpelthen ved at indsætte den første ligning i den anden og udnytte egenskaben ved $\mu(n)$.

Hvis for eksempel $f(x) = \sin x$ er $F(x)$ *savtakfunktionen* $S(x)$: $S((2n+1)\pi) = 0$ og $S(n2\pi) = \pm\pi/2$ og $S(x)$ lineært aftagende imellem disse punkter (det vises på side 51):

$$S(x) = \sum_{m=1}^{\infty} \sin(mx)/m$$

Så Möbius-inversion betyder, at vi kan udtrykke $\sin x$ som en uendelig sum af "savtakker", hvor takkerne bliver mindre og mindre og veksler fortegn:

$$\sin x = \sum_{n=1}^{\infty} \mu(n)S(nx)/n$$

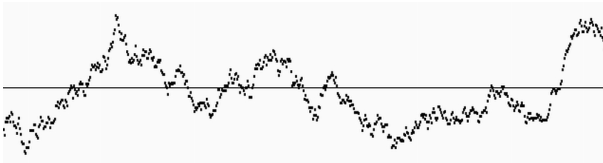


- i billedet er anvendt 100 savtakker.

$\mu(n)$ er kun forskellig fra 0, når n ikke indeholder nogen primfaktor mere end én gang (og sandsynligheden herfor er $6/\pi^2 = 0,6079\dots$, side 63), i så fald er $\mu(n)$ enten 1 eller -1, og vi formoder, at der er lige mange plusser og minusser, altså at summen

$$\sum_{n=1}^N \mu(n)$$

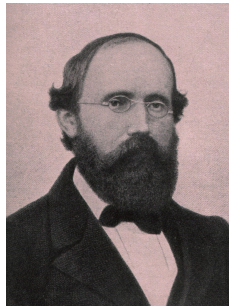
numerisk er lille i forhold til N . Grafen for disse tal *divideret med* \sqrt{N} , fra $N = 10.000$ til 20.000 , ser således ud:



Der synes ganske rigtigt at være lige mange plusser og minusser, siden kurven som helhed hverken stiger eller falder, men variationen i $\sum \mu(n)$ kan ikke siges at være jævn. Vi vender tilbage til denne sag.

Antallet af primtal mindre end et givet tal

I 1859 udkom en afhandling - på otte sider - om hvilken det er blevet sagt, at den rykkede udviklingen hundrede år frem inden for sit emne, talteorien. Det er *Bernhard Riemanns* "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse".



Udgangspunktet for Riemann var en vis tilnærmelsesformel, man kendte for antallet af primtal som er mindre end et givet tal N . Hvis vi betegner dette antal π_N , lyder denne tilnærmelsesformel (*primtalssætningen*)

$$\pi_N \approx \int_2^N dx / \log x$$

Den blev postuleret af den 15-årige *Gauss* i 1792. Gauss havde observeret, at sandsynligheden for at et tal n er et primtal, er omkring $1/\log n$, ergo må antallet af primtal mindre end N være omkring

$$\sum_{1 < n < N} 1/\log n$$

og Gauss mente, at integralet måtte være en bedre tilnærmelse til π_N . En grov tilnærmelse til integralet og summen er tallet $N/\log N$, idet det

gælder, at forholdet mellem $N/\log N$ og hver af disse konvergerer imod 1 for $N \rightarrow \infty$. Så hvis en af disse tre tilnærmelser er sand, altså hvis forholdet mellem denne og π_N konvergerer imod 1 for $N \rightarrow \infty$, så er de to andre tilnærmelser også sande. Den grove tilnærmelsesformel lyder altså (den kaldes også primtalsætningen)

$$\pi_N \approx N/\log N$$

At disse tilnærmelser *er* sande, blev bevist i 1896 af *Hadamard* og *La Vallée-Poussin* (uafhængigt af hinanden), altså 100 år efter Gauss og 40 år efter Riemann. Jamen hvad var da Riemanns fortjeneste? Den var, at han fandt *resten* af formlen for π_N . For det er jo nok sådan, at Gauss' integral er det første led i en række, hvis sum er en eksakt formel for π_N . Det er ikke givet, at en sådan formel eksisterer: den eksisterer ikke for funktionen v_N i næste kapitel. Og i de tilfælde hvor en sådan række eksisterer, er den ofte ikke særligt svær at manipulere sig frem til. Problemet er at *bevise*, at den række man har fundet, er den "sande" række, i den forstand at det første led er en god tilnærmelse, og at leddene har aftagende betydning, jo længere man kommer ud i rækken. Og dette beviste Riemann ikke: han beviste (som sagt) ikke, at hans formels vigtigste led, Gauss' integral, virkelig er en tilnærmelse til π_N , og han beviste heller ikke, at den vigtigste *del* af hans formel, som er en uendelig sum af integraler der minder om Gauss' integral, er en bedre tilnærmelse til π_N end Gauss' integral - for eksempel *under forudsætning af*, at Gauss' tilnærmelse er bevist at være sand. For dette sidste er nemlig usandt (side 17). Desuden var Riemanns bevis for selve formlen ikke komplet: der var nogle ting som Riemann ikke kunne bevise eller ikke fandt det umagen værd at bevise helt til bunds, de blev først bevist tre-fire årtier senere.

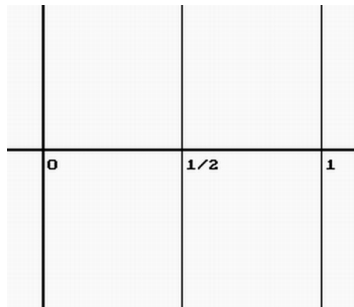
Og *Riemanns hypotese*, som fremsættes i denne afhandling, men som ikke har betydning for selve formlen, er gået hen og blevet matematikkens mest betydningsfulde uløste problem.

Riemann tager udgangspunkt i følgende formel af *Euler* (*Eulers produktfremstilling*)

$$\sum_{n=1}^{\infty} 1/n^z = \prod_{p \text{ primtal}} (1 - 1/p^z)^{-1}$$

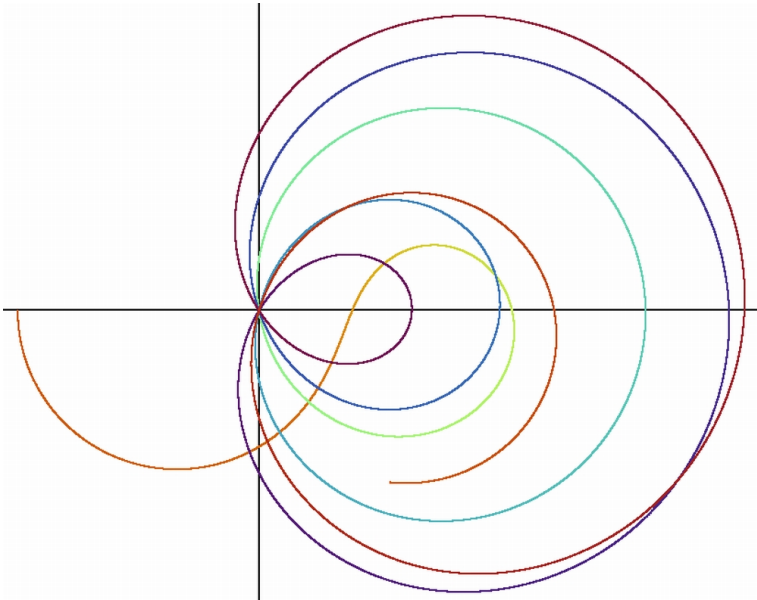
som gælder for ethvert komplekst tal z hvis reeddel er > 1 . Formlen bygger på den omtalte aritmetikkens fundamentalsætning, og den er ikke svær at eftervise. Den funktion af z som defineres ved den uendelige række eller det uendelige produkt, betegnede Riemann $\zeta(z)$, så den er blevet kaldt *Riemanns zetafunktion*. Den er umiddelbart kun defineret til højre for linjen $x = 1$ (hvor rækken og produktet er absolut konvergent), men Riemann udledte et integraludtryk for $\zeta(z)$ som viser, at $\zeta(z)$ kan udvides til en funktion der er holomorf (= kompleks differentiabel) i hele den komplekse plan, undtagen i punktet $z = 1$, idet $\zeta(z) \rightarrow \infty$ for $z \rightarrow 1$ (den *harmoniske række* $1 + 1/2 + 1/3 + 1/4 + \dots$ er divergent). En sådan holomorf udvidelse er *entydigt bestemt*. Det gælder nemlig (*Riemanns identitetssætning*): Hvis to holomorfe funktioner på et åbent område stemmer overéns langs et kurvestykke (det kan være vilkårligt lille), da er de identiske.

$\zeta(z)$ har uendeligt mange nulpunkter (altså punkter z hvor $\zeta(z) = 0$), nemlig, viste Riemann, dels alle de lige negative tal: $-2, -4, -6, \dots$, og dels uendeligt mange punkter i strimlen til højre for y -aksen og til venstre for linjen $x = 1$:



Riemann betragtede det som "sehr wahrscheinlich", at alle nulpunkterne i strimlen ligger på dens midterlinje $x = 1/2$ - dette er Riemanns hypotese. Da $\zeta(\bar{z}) = \overline{\zeta(z)}$ er nulpunkterne beliggende symmetrisk om x -aksen.

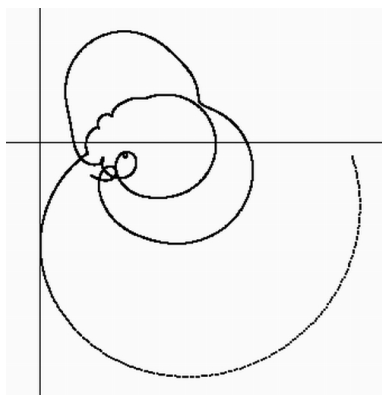
Når man bevæger sig op langs linjen igennem $x = \frac{1}{2}$ og tegner $\zeta(z)$, det vil sige tegner punkterne $\zeta(\frac{1}{2}+yi)$ for tallene $\frac{1}{2}+yi$ ($y \geq 0$), får man en kurve, som *hele tiden* vil gå igennem origo, mens de tilsvarende kurver for $x \neq \frac{1}{2}$ aldrig vil gå igennem origo.



Om denne kendsgerning skulle være sand, har ingen betydning for gyl-digheden af Riemanns formel, blot benyttes i udledningen en vurdering af antallet af nulpunkter i strimlen beliggende over x -aksen og under linjen y , og Riemann fandt at dette antal tilnærmelsesvist er $(y/2\pi)(\log(y/2\pi)-1)$ - det var en af de ukomplette påstande.

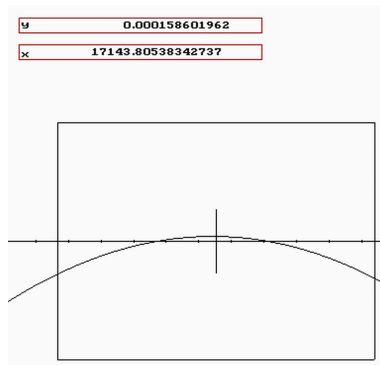
Kurven $y \rightarrow \zeta(x+yi)$ vil altså for $x \neq \frac{1}{2}$ aldrig gå igennem origo. For $x = 1$ var det i lang tid antaget, at kurven ligger til højre for y -aksen, men da ingen kunne bevise det, søgte man efter et modbevis. Matematikeren *J. van de Lune* skriver: "On January 22, 1979, for the first time I found a t such that $\text{Re } \zeta(1+it) < 0$: $\text{Re } \zeta(1+i * 38\ 468\ 816.1) \approx -.107$." Senere fandt van de Lune en noget mindre t -værdi: 682.112,92, og for denne er $\text{Re}(\zeta(1+ti)) \approx -0,003$. Hvis vi i programmet "ZetaFunc" sætter $x = 1$ og (start) $y = 682.112$, får vi denne kurve frem (vores program præciserer

-0.003 til -0,0027272...):



Hvis der skulle findes et nulpunkt for $\zeta(z)$, som ikke ligger på linjen $x = \frac{1}{2}$, vil der være et par af nulpunkter, som ligger symmetrisk om denne linje: hvis nulpunktet ρ ikke ligger på linjen $x = \frac{1}{2}$, altså hvis $\rho = (\frac{1}{2} + \varepsilon) + yi$, hvor $\varepsilon \neq 0$, da er punktet $\rho' = (\frac{1}{2} - \varepsilon) + yi$ også et nulpunkt (thi hvis ρ er et nulpunkt, vil såvel det konjugerede tal $\bar{\rho}$ som tallet $1 - \rho$ være et nulpunkt, det sidste som følge af funktionalligningen for $\zeta(z)$, side 74). Hvis et punkt er tilstrækkeligt nær ved et nulpunkt, kan vi finde dette nulpunkt ved Newton-iteration: $z \rightarrow z - \zeta(z)/\zeta'(z)$. Men hvis der nu fandtes to nulpunkter ρ og ρ' symmetrisk om linjen $x = \frac{1}{2}$, hvor ville da punktet ρ_0 midt imellem disse itereres hen ved $z \rightarrow z - \zeta(z)/\zeta'(z)$? Det ville vel tilhøre Julia-mængden for denne iteration og således forblive i denne mængde ved iterationen og derfor ikke iterere imod et nulpunkt. Punktet ville sikkert iterere imod ∞ , hvilket ville betyde at $\zeta'(\rho_0) = 0$. Og dette ville igen betyde, at kurven som vi bruger til at lokalisere nulpunkterne (side 77, programmet "ZeroFunc"), i dette punkt ville have en top som ligger under y-aksen, eller en dal som ligger over y-aksen. Det er faktisk dette fænomen, man har interesseret sig mest for i forsøget på at bevise Riemanns hypotese, idet man har forsøgt at bevise, at det ikke kan finde sted, altså at kurven ikke kan gå ned imod y-aksen og derefter op igen uden at have passeret y-aksen, og tilsvarende nedefra. Man har fundet flere steder, hvor det er lige ved at gå galt, og kurven opfører sig uroligt i disses omegn (som om den véd at den er på forbudte veje). Dette kaldes *Lehmers fænomen*. Prøv at se grafen fra $y = 17.140$ til 17.150 , det ser ud

som om den tangerer y-aksen, men hvis man zoomer ind, ser man at den opfører sig korrekt (afstanden mellem de to nulpunkter er 0,035):



Det viser sig, at Lehmers fænomen især optræder ved de y -værdier hvor $\text{Re}(\zeta(1+yi))$ er negativ.

Riemanns hypotese - eller rettere, den tilsvarende påstand for beslægtede funktioner (herom senere) - har overordentlig stor betydning: der er sætninger som strengt taget ikke er komplet bevist: det benyttes i deres bevis at Riemanns hypotese er sand. Og så er problemet jo i sig selv en mægtig udfordring: hvorfor modsætter denne *kendsgerning* sig så hårdnakket et bevis? Men måske *kan* Riemanns hypotese ikke bevises, for det er nemlig ikke givet, at en matematisk påstand som er sand, kan bevises - som vi skal se.

Vi vil senere udlede Riemanns formel, her skal vi blot se den og lave et program, som bygger på de vigtigste dele af den, og se, hvor nøjagtig en formel for π_N vi får. I Riemanns formel indgår en kompleks funktion som vi først må definere: $\text{Li}(z)$ - *integrallogaritmen*. Den er defineret ved

$$\text{Li}(z) = \int_{-\infty}^1 z^t dt/t$$

for $|z| \geq 1$, og

$$\text{Li}(z) = \int_1^{\infty} z^t dt/t$$

for $|z| \leq 1$ (for $z = 1$ er integralerne divergente). Når z ikke er et positivt reelt tal, er z^t ikke veldefineret, så umiddelbart er denne komplekse funktion meningsløs. Funktionen $\text{Li}(x^z)$, hvor x er et positivt reelt tal, er dog en veldefineret funktion af z , og det er kun funktioner af denne form vi vil benytte, og en sådan funktion er holomorf i hele den komplekse plan undtagen i punktet $z = 0$. I det første integral er integranden ikke defineret for $t = 0$ som tilhører integrationsintervallet $]-\infty, 1]$. For et sådant integral fra a til b , hvor der imellem a og b er en singularitet c for integranden, er værdien *defineret* som grænseværdien for $\varepsilon \rightarrow 0$ ($\varepsilon > 0$) af integralet fra a til $c - \varepsilon$ plus integralet fra $c + \varepsilon$ til b .

Nu kan vi opskrive Riemanns formel:

$$\pi_N = \sum_{m=1}^{\infty} \mu(m)/m J(N^{1/m}) - \delta$$

hvor

$$J(x) = \text{Li}(x) - \sum_{\rho} \text{Li}(x^{\rho}) + \sum_{k=1}^{\infty} \text{Li}(x^{-2k})$$

her løber ρ over nulpunkterne for Riemanns zetafunktion $\zeta(z)$ i strimlen $0 < \text{Re}(z) < 1$, og $-2k$ over de øvrige nulpunkter, som er alle de negative lige tal. Tallet δ er $1/2$ hvis N er et primtal og ellers 0.

Riemanns påstand, at der er uendeligt mange nulpunkter for $\zeta(z)$ som er uregelmæssigt fordelt, følger af denne formel. For da primtallene er uregelmæssigt fordelt, er venstresiden π_N en uregelmæssig funktion af N , derfor må højresiden også være en uregelmæssig funktion af N , og denne uregelmæssighed må primært komme fra tallene ρ , da der går information tabt ved Möbius' funktion $\mu(m)$. Hvis vi ser bort fra den del som skyldes de uregelmæssige nulpunkter, og også fra den som skyldes de regelmæssige nulpunkter $(-2k)$, idet denne del går imod 0 for $N \rightarrow \infty$ (samt fra tallet δ), så får vi en tilnærmelsesformel for π_N ved at erstatte $J(x)$ med $\text{Li}(x)$: Riemanns tilnærmelsesformel. I denne skal vi kun udregne $\text{Li}(x)$ for reelle $x > 1$, og for sådanne x gælder (ved at indføre substitutionen $t = \log u / \log x$):

$$\text{Li}(x) = \int_{-\infty}^1 x^t dt/t = \int_0^x du/\log u$$

Riemanns tilnærmelsesformel lyder altså

$$\pi_N \approx \sum_{m=1}^{\infty} \mu(m)/m \text{Li}(N^{1/m})$$

Det første led er $\text{Li}(N)$ - Gauss' tilnærmelsesformel - den formel som Riemann havde sat sig for at generalisere (forskellen mellem 0 og 2 i integrationen betyder kun en afvigelse på omkring 1). For et givet N aftager leddene i størrelse, fordi $N^{1/m}$ aftager, og fordi der divideres med m . Det andet led, $-\text{Li}(\sqrt{N})/2$, er et relativt stort *negativt* tal, og de følgende to led er også negative. Dette betyder, at Riemanns tilnærmelse til π_N er mindre end Gauss' tilnærmelse $\text{Li}(N)$ for alle N . Så hvis den uregelmæssige del af Riemanns eksakte formel for π_N er af forsvindende betydning, er $\pi_N < \text{Li}(N)$ for alle N . At denne ulighed gælder, var engang en kendsgerning som man forsøgte at bevise, da alle empiriske undersøgelser viste at $\pi_N < \text{Li}(N)$. Og dette viser alle empiriske undersøgelser fortsat. Men i 1914 beviste *Littlewood*, at der findes *uendeligt mange* N for hvilke $\pi_N > \text{Li}(N)$. Det mindste N som opfylder $\pi_N > \text{Li}(N)$, må være meget stort, og det er måske så stort, at det aldrig vil blive fundet, da det kan være af størrelsesorden 10^{300} , for man har bevist (i 1986), at der findes N -værdier af denne størrelsesorden (og endda en meget lang række af på hinanden følgende tal) som opfylder $\pi_N > \text{Li}(N)$. Men dette betyder, at for et sådant N hvor $\pi_N > \text{Li}(N)$, er Gauss' tilnærmelse $\text{Li}(N)$ til π_N *bedre* end Riemanns, som jo er mindre end $\text{Li}(N)$. Den uregelmæssige del af Riemanns eksakte formel for π_N har større betydning, end Riemann havde forestillet sig. Hvis ikke det var blevet bevist, at der findes N -værdier således at π_N er større end $\text{Li}(N)$, ville man stadig have troet, at π_N altid er mindre end $\text{Li}(N)$, og man ville fortsat have forsøgt at bevise det, og man ville have betragtet Riemanns tilnærmelsesformel som bedre end Gauss'.

Men der er altså noget som tyder på, at for alle de N -værdier, som menneskenes computere nogensinde vil kunne håndtere, er Riemanns tilnærmelsesformel for π_N bedre end Gauss'. For disse værdier svinger Riemanns tal omkring π_N , og dette er jo et tegn på en god tilnærmelse. I programmet "NumbPrimes" udregnes π_N ved optælling og ved forskellige tilnærmelser, nemlig:

1. Tallet $N/\log N$.
2. Gauss' tilnærmelse $\text{Li}(N)$ (udregnet ved Simpsons formel)
3. $\sum \mu(m)/m \text{Li}(N^{1/m})$ (sum fra $m = 1$ til 100)
4. En formel der omformer den uendelige sum hvori $\text{Li}(N^{1/m})$ indgår til en uendelig sum hvori tallene $\zeta(n)$ ($n = 2, 3, \dots$) indgår og som konvergerer ekstremt hurtigt - den er vist på side 78 og den skyldes den danske matematiker *J.P. Gram* (1850-1916).
5. Integralformlen på side 69.