**Opspaltning i primfaktorer**

Et program som kan undersøge om et tal er et primtal, eller finde hvilke primtal det er sammensat af, er det allerførste program enhver talentusiast laver. For den tid jo er forbi hvor man udgiver matematiske tabeller, fra nu af foregår alt ved lommeregneren og computeren.

Som bekendt kan ethvert naturligt tal på en *entydig* måde skrives som et produkt af primtal - entydig hvis primtallene opskrives efter størrelse. At ethvert naturligt tal *kan* skrives som et produkt af primtal, følger af definitionen på et primtal. Men at denne opspaltning er entydig på nær faktorernes orden er ikke indlysende, og den gælder i almindelighed ikke for generelle algebraiske tallegemer. De sædvanlige hele tal er de *hele tal* i det algebraiske tallegeme Q, mængden af de rationale tal. I det algebraiske tallegeme $Q(\sqrt{6})$ er de *hele tal* tallene af formen $m+n\sqrt{6}$, hvor m og n er sædvanlige hele tal, og her er f.eks. $6 = 2\cdot 3 = \sqrt{6}\cdot\sqrt{6}$, og 2, 3 og $\sqrt{6}$ er *primelementer* i $Q(\sqrt{6})$. Entydighedssætningen for de sædvanlige hele tal (dvs. for det algebraiske tallegeme Q) kaldes *aritmetikkens fundamentalsætning,* og den blev selvfølgelig erkendt og bevist af de gamle grækere. De formulerede dog tingene på en ganske anden måde end vi gør, men sætningen følger af Theorem 14 i *Euklid* bog IX. I Euklid bliver det også bevist at der er uendelig mange primtal. Dette bevis lyder (meget kort gengivet): hvis der kun var endelig mange primtal og man gangede dem allesammen med hinanden og adderede 1 til, så ville intet primtal gå op i dette tal, og et tal som intet primtal går op i er en umulighed.

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 succesivt for de ulige tal 5, 7, 9, ..., men kun hvis et sådant tal d er et primtal, og d er et primtal hvis ingen af de ulige tal fra 3 til (den hele del af) $\sqrt{d}$ 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 sålænge $d < \sqrt{n}$. En sådan opgave er altid en stor fornøjelse for en computer, dog er det største *hele* tal som computeren kan håndtere tallet $2^{31} - 1 = 2147483647$, men se bare hvor hurtigt den kan finde ud af at dette tal er et primtal. Det er jo trods alt "kun" de ulige tal op til $\sqrt{2147483647} \approx 46341$ som skal undersøges. Og da det største primtal mindre end dette tal er 46337, er dette primtal den største primfaktor som kan forekomme med multiplicitet større end 1. En sjov opgave er at indtaste en række cifre med et system i og se om der også er et smukt system i opspaltningen (hvordan opspalter f.eks. 1212121?).

**Möbius' funktion μ(n)**

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.* F.eks. funktionen σ(n) defineret ved σ(n) = summen af alle primfaktorerne i n (f.eks. σ(117) = σ(3·3·13) = 3+3+13 = 19) - for denne funktion gælder σ(mn) = σ(m) +σ(n), dvs. den er en logaritmefunktion på de naturlige tal.

I de følgende kapitler vil vi hyppigt møde *Möbius' funktion* μ(n). Den er defineret ved $\mu(n) = (-1)^r$ hvis n er produktet af *netop* r forskellige primtal, ellers 0 (dvs. hvis en primfaktor optræder mere end én gang) (f.eks. μ(4) = 0, μ(5) = -1, μ(6) = 1). μ(n) opfylder derfor μ(mn) = μ(m)μ(n) når m og n er indbyrdes primiske, i modsat fald er μ(mn) = 0. μ(n) har den særlige egenskab, at for ethvert naturligt tal n er summen af tallene μ(d) for *alle* divisorene d i n lig 0, undtagen for n = 1, idet μ(1) = 1. Og denne egenskab giver anledning til fænomenet *Möbius-inversion:* hvis f(x) er en funktion defineret på mængden af de naturlige eller hele eller reelle eller komplekse tal (og hvis værdier er 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 μ(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 den omtalte egenskab ved μ(n).

Hvis f.eks. f(x) = sin x er F(x) savtakfunktionen S(x) fra side 242, dvs. S(x) = 0 for x = nπ (n hel) og S(x) = ±1 for x = (n+½)π og S(x) er lineært aftagende imellem disse punkter:

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

(dette vises på side ...). 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:

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

Programmet "Möbius" (i Mappen "Möbius- og Fourier-inversion") viser hvordan en sinuskurve ser ud når den laves af et antal savtakker (f.eks. 5000) som skal indtastes.

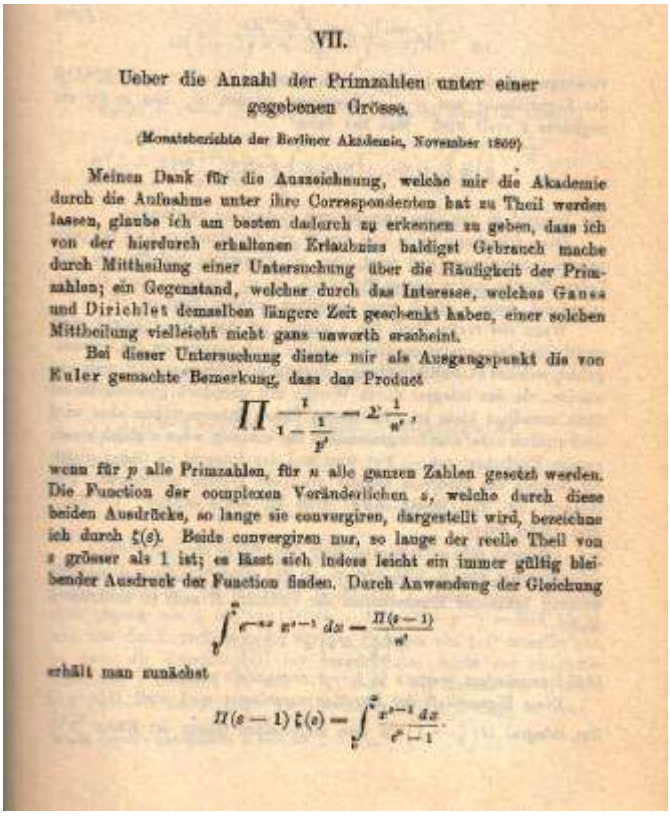
μ(n) er kun forskellig fra 0 når n ikke indeholder nogen primfaktor mere end én gang (og sandsynligheden herfor er $6/\pi^2 = 0.6079...$, se side ...), i så fald er μ(n) enten 1 eller -1, og vi formoder at der "set på lang afstand" er lige mange plusser og minusser, altså at summen

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

numerisk er lille i forhold til N. Programmet "Merten" (i mappen "Mertens formodning") tegner grafen for disse tal *divideret med* √N, op til et stort tal som skal indtaste (f.eks. 100000). Der synes ganske rigtigt at være lige mange plusser og minusser, siden kurven som helhed hverken stiger eller falder, men variationen i ∑ μ(n) kan ikke siges at være lille i forhold til N. Vi vender tilbage til denne sag.

**Antallet af primtal mindre end et givet tal**

I 1859 udkom en afhandling om hvilken det er blevet sagt, at den rykkede udviklingen hundrede år frem indenfor dens emne, talteorien. Og den er på kun 8 sider. Ja, det er Bernhard Riemanns afhandling "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse":



VII.

Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Monatsberichte der Berliner Akademie, November 1859)

Meinen Dank für die Auszeichnung, welche mir die Akademie durch die Aufnahme unter ihre Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erkennen zu geben, dass ich von der hierdurch erhaltenen Erlaubniss baldigst Gebrauch mache durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welcher durch das Interesse, welches Gauss und Dirichlet demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

$$\Pi \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für $p$ alle Primzahlen, für $n$ alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen $s$, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von $s$ grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx} x^{s-1}\, dx = \frac{\Pi(s-1)}{n^s}$$

erhält man zunächst

$$\Pi(s-1)\,\zeta(s) = \int_0^\infty \frac{x^{s-1}\, dx}{e^x - 1}.$$

Udgangspunktet for Riemann var vis en tilnærmelsesformel man kendte for antallet af primtal som er mindre end et givet tal N. Hvis vi betegner dette antal $\pi_N$, 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

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

Dette tal er en tilnærmelse til integralet, og Gauss mente at integralet måtte være en bedre tilnærmelse. En grov tilnærmelse til integralet og summen er tallet N/log N, idet det gælder at forholdet imellem N/log N og hver af disse konvergerer imod 1 for $N \to \infty$. Så hvis en af disse tre tilnærmelser er sand, dvs. hvis forholdet imellem denne og $\pi_N$ konvergerer imod 1 for $N \to \infty$, så er de to andre tilnærmelser også sande. Den grove tilnærmelsesformel lyder altså (den kaldes også primtalssætningen):

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

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 $\pi_N$. For det er jo nok sådan at Gauss' integral er det første led i en række af udtryk hvis betydning er aftagende og hvis sum er en eksakt formel for $\pi_N$. Det er ikke givet at en sådan formel, som vel at mærke er nogenlunde enkel og relevant, eksisterer: den eksisterer ikke for funktionen $\nu_N$ i næste kapitel. Og i de tilfælde hvor sådanne rækker eksisterer, er de ofte ikke særlig svære 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 til det ønskede og at leddene har aftagende betydning jo længere man kommer ud i rækken. Og dette var Riemann heller ikke i stand til at bevise: han beviste ikke at hans formels vigtigste led, Gauss' integral, virkelig er en tilnærmelse til $\pi_N$, 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 $\pi_N$ end Gauss' integral (f.eks. *under forudsætning af* at Gauss' tilnærmelse er bevist at være sand). For dette sidste er som allerede antydet usandt (side ...). Desuden var Riemanns bevis for selve formlen ikke komplet: der var nogle ting som Riemann ikke kunne eller ikke fandt det umagen værd at bevise helt til bunds, disse blev først bevist tre-fire årtier senere.

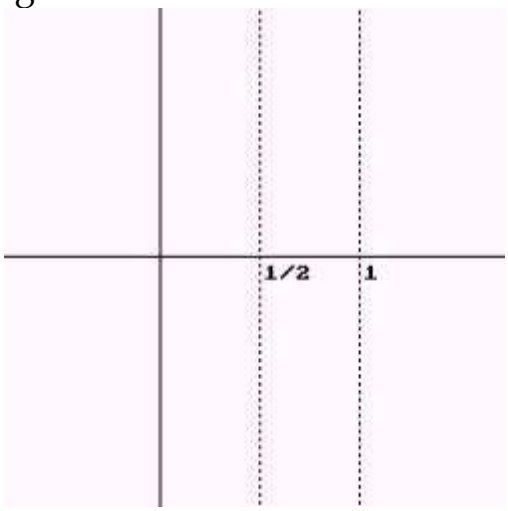
Og *Riemanns hypotese*, som fremsættes i denne afhandling men som ikke har betydning for selve formlen, er som sagt gået hen og blevet matematikkens mest betydningsfulde uløste problem.

Riemann tager, som det ses, udgangspunkt i følgende formel af *Euler* (1707-83) (*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 reeldel 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 zeta-*

*funktion.* Den er umiddelbart kun defineret til højre for linien x = 1 (hvor rækken og produktet er absolut konvergent), men Riemann udledte et integraludtryk for ζ(z) som viser at ζ(z) kan udvides til en funktion der er holomorf i hele den komplekse plan, undtagen i punktet z = 1, idet $\zeta(z) \to \infty$ for $z \to 1$ (den *harmoniske* række 1 + 1/2 + 1/3 + 1/4 + ... er divergent). En sådan holomorf udvidelse er *entydigt bestemt*. Det gælder nemlig, at hvis to holomorfe funktioner på et åbent område blot stemmer overéns langs et *vilkårligt lille* kurvestykke, da er de identiske (*Riemanns identitetssætning*). ζ(z) har uendelig mange nulpunkter (altså punkter z hvor ζ(z) = 0), nemlig, viste Riemann, dels alle de lige negative tal: -2, -4, -6, ..., og dels uendelig mange punkter i strimlen tilhøjre for y-aksen og tilvenstre for linie x = 1:




Riemann betragtede det som "sehr wahrscheinlich" at alle nulpunkterne i strimlen ligger på dens midterlinie x = ½ (da $\underline{\zeta(z)} = \zeta(\underline{z})$ er de beliggende symmetrisk om x-aksen), dette er Riemanns hypotese. Og nu hvor vi har lært om komplekse tal, kan vi forstå kurven og talen på side ...: kurven fremkommer når man bevæger sig op langs den stiplede linie igennem x = ½ og tegner ζ(z), dvs. tegner punkterne $\zeta(½+iy)$ for tallene $z = ½+iy$ ($y \geq 0$). Og Riemanns hypotese siger altså, at denne kurve *hele tiden* vil gå igennem origo, mens derimod de tilsvarende kurver for $x \neq ½$ *aldrig* vil gå igennem origo. Om dette skulle være sandt har ingen betydning for gyldigheden af Riemanns formel, blot benyttes i beviset at *antallet* af nulpunkter i strimlen beliggende over x-aksen og under linien $y = y_0$ tilnærmelsesvist er $(y_0/2\pi) \log(y_0/2\pi)$, og det-te var en af de ting Riemann ikke beviste, påstanden blev først bevist af von Mangoldt i 1905.

Riemanns hypotese har som sagt (side ...) vist sig at have overordentlig stor betydning: et utal af sætninger indenfor den moderne matematik er strengt taget ikke fuldtud beviste, idet det benyttes i deres bevis at Riemanns hypotese (eller en analog påstand) er sand. Og så er problemet jo i sig selv en mæg-

tig udfordring: hvorfor modsætter denne *kendsgerning* sig så hårdnakket et bevis? Men måske *kan* Riemanns hypotese slet ikke bevises, det er nemlig ikke givet at en matematisk påstand som er sand også kan bevises (denne sag vil blive uddybet i næste kapitel).

Jeg vil senere skitsere et bevis for 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 $\pi_N$ vi får. I Riemanns formel indgår en kompleks funktion som vi først må definere: Li(z) - *integrallogaritmen.* Den er defineret ved

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

hvis $|z| \geq 1$, og

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

hvis $|z| \leq 1$ (for $z = 1$ er integralerne divergente). Når z ikke er et positivt reelt tal, er $z^t$ ikke veldefineret (se side ...), så umiddelbart er denne komplekse funktion meningsløs. Funktionen $\mathrm{Li}(x^z)$, 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 $\varepsilon \to 0$ ($\varepsilon > 0$) af integralet fra a til $c-\varepsilon$ plus integralet fra $c+\varepsilon$ til b (se nærmere side ...).

Nu kan vi opskrive Riemanns formel:

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

hvor

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

idet ρ her løber over alle nulpunkterne for Riemanns zetafunktion ζ(z) i den omtalte strimmel 0 < Re(z) < 1, og -2k løber over de øvrige nulpunkter, som er alle de negative lige tal. Tallet ε er ½ hvis N er et primtal, ellers 0.

Riemanns påstand, at der er uendelig mange nulpunkter for ζ(z) i strimlen 0 < Re(z) < 1 og at disse er uregelmæssigt fordelt, følger direkte af denne formel. For da primtallene er uregelmæssigt fordelt, er venstresiden $\pi_N$ en uregelmæssig funktion af N, derfor må højresiden også være en uregelmæssig funktion af N, og denne uregelmæssighed kan kun komme fra tallene ρ. Hvis vi ser bort fra denne uregelmæssige del af formlen, og også fra den del som skyldes de regelmæssige nulpunkter (-2k), idet denne del nemlig går imod 0 for $N \to \infty$, så får vi en tilnærmelsesformel for $\pi_N$ ved at erstatte J(x) med Li (x): Riemanns tilnærmelsesformel. I denne skal vi kun udregne Li(x) for positive reelle x > 1, og for sådanne x gælder:

$$Li(x) = \int_{-\infty}^{1} x^t \, dt/t = \int_{0}^{x} du/\log u$$

(idet vi har indført substitutionen t = logu/logx). Og da vi også kan se bort fra tallet ε, lyder Riemanns tilnærmelsesformel for antallet af primtal mindre end N:

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

Det første led er Li(N), dvs. Gauss' tilnærmelsesformel, den formel som Riemann havde sat sig for at generalisere (forskellen imellem 0 og 2 i integrationen betyder kun en afvigelse på omkring 1), og for et givet N aftager leddene i størrelse, fordi $N^{1/m}$ aftager og fordi der divideres med m. Det andet led, -Li(√N)/2, er et relativt stort *negativt* tal - og de følgende to led er også negative - og dette betyder at Riemanns tilnærmelse til $\pi_N$ er mindre end Gauss' tilnærmelse Li(N) for alle N. Så hvis den uregelmæssige del af Riemanns eksak-

te formel for $\pi_N$ er af tilpas stærkt aftagende betydning, er $\pi_N < Li(N)$ for alle N. At denne ulighed gælder var engang en kendsgerning som man forsøgte at bevise, da alle empiriske undersøgelser viste at $\pi_N < Li(N)$. Og dette viser alle empiriske undersøgelser fortsat. Men i 1914 beviste Littlewood at der findes *uendelig mange* N for hvilke $\pi_N > Li(N)$. Det mindste N som opfylder $\pi_N > Li(N)$ må være meget stort, og det er måske så stort at det aldrig vil blive fundet, ja det er måske af størrelsesorden $10^{370}$, for man har bevist (i 1986) at der findes N-værdier af denne størrelsesorden (endda en meget lang række af på hinanden følgende tal) som opfylder $\pi_N > Li(N)$ (se side ...). Men dette betyder, at for et sådant N hvor $\pi_N > Li(N)$, er Gauss' tilnærmelse Li(N) til $\pi_N$ *bedre* end Riemanns tilnærmelse, som jo er mindre end Li(N). Den uregelmæssige del af Riemanns eksakte formel for $\pi_N$ har for meget store N-værdier større betydning end Riemann selv har forestillet sig. Hvis ikke det var blevet bevist at der findes N-værdier således at $\pi_N > Li(N)$, ville man stadig have troet at $\pi_N$ altid er mindre end Li(N) og man ville fortsat have forsøgt at bevise det, og man ville have betragtet Riemanns tilnærmelsesformel som bedre end Gauss'. Dette er et eksempel på hvor forsigtig man skal være med at opstille formodninger ud fra empiriske undersøgelser.

Men der er altså noget der tyder på, at for alle de N-værdier som menneskenes computere nogensinde vil kunne håndtere, er Riemanns tilnærmelsesformel for $\pi_N$ langt bedre end Gauss', og for disse værdier svinger Riemanns tal omkring $\pi_N$, og dette er jo tegn på en god tilnærmelse. Prøv programmet "Antallet af primtal" (i mappen "Riemann") hvor $\pi_N$ udregnes dels eksakt (ved optælling) og dels ved forskellige tilnærmelser. Nemlig:

1. $\sum_{m=1}^{100} \mu(m)/m \; Li(N^{1/m})$, hvor en tilnærmelse til integralet Li(x) udregnes (ved Simpsons formel, se side ...).

2. En formel der omformer den uendelige sum hvori $Li(N^{1/m})$ indgår til en uendelig sum hvori tallene $\zeta(n)$ (n = 2, 3, ...) indgår og som konvergerer ekstremt hurtigt (den er vist på side ... og den skyldes den danske matematiker J.P. Gram, 1850-1916).

3. Gauss' tilnærmelse Li(N).

4. Tallet N/log N.

Bemærk at Riemanns eksakte formel for $\pi_N$ har mening selv om N ikke er et helt tal, og da man jo ikke i praksis kan udregne alle dens uendelig mange led, men må nøjes med at medtage et vist antal, og da man i udregningen af disse må nøjes med tilnærmelser, får man på den måde en funktion af x som må smyge sig omkring trappefunktionen $\pi_x$. Dette fascinerende syn var Riemann ganske afskåret fra, for ham bestod formlens værdi alene i dens sandhed og skønhed. Til gengæld var enhver dygtig videnskabsmand og kunstner på hans tid skænket den glæde at vide, at hans skaberværker i al evighed ville gøre nytte og være værdsat - også - og især - hvis hans samtid ikke havde sans og forståelse for dem. Denne form for glæde er gået tabt, men til gengæld har vi fået et mægtigt vidunder, computeren, så således er der skabt retfærdighed i verden. I kapitlet "Udledning af Riemanns formel for $\pi_N$" skal vi se såvel den skønhed der foldede sig ud for øjnene af Riemann efterhånden som hans teori tog form, som den skønhed som *vi* har en særlig sans for: en kurve i et koordinatsystem der langsomt bliver til for øjnene af os og som stiger således som en salgskurve skal stige.

**Goldbachs formodning**

Da jeg talte med Riemann, nævnte han noget om at vi ikke kan bevise ting som ethvert barn på syv år kan forstå (side ...). Det var først senere jeg fæstnede mig ved denne udtalelse - under samtalen har jeg måske i forvirringen troet at jeg havde fortalt ham at man endnu ikke har bevist Goldbachs formodning. Men dette sagde jeg jo ikke noget om. Har Riemann selv arbejdet med dette problem? - løst det eller ment at han var tæt ved en løsning inden døden rev ham bort? Jeg tror det ikke, jeg tror ikke at man beskæftigede sig så meget med Goldbachs formodning på hans tid, men det var i hvert fald med direkte afsæt i den metode som han havde indført i studiet af primtallene - brugen af kompleks funktionsteori - at der et halvt århundrede senere kom gang i studiet af Goldbachs formodning. Derimod kan Riemann have haft den påstand i tankerne, at der er uendelig mange primtalstvillinger, dvs. par af på hinanden følgende ulige tal som begge er primtal. Denne påstand er også stadig ubevist, og den var et kendt problem på Riemanns tid, og måske har Riemann, nu hvor han var igang med primtallene, bevist den, men blot ikke offenliggjort beviset eller kigget det omhyggeligt efter i sømmene - for dengang var problemet jo ikke så svært som det er idag.

Riemanns hypotese er blevet udnævnt til matematikkens vigtigste uløste pro-

blem, fordi den (og især dens mange generaliseringer) dukker op et utal af steder, selv steder som tilsyneladende befinder sig langt fra talteorien. Men når vi ser kurven på side ..., kan vi godt forstå at et bevis for Riemanns hypotese kan være lidt problematisk. Dén ubeviste påstand som vi nu skal beskæftige os med - Goldbachs formodning - er derimod en virkelig gåde. Den er så elementær at ethvert barn på syv år kan forstå den, og den burde egentlig betragtes som matematikkens gåde nr. 1. Men dels har den ikke de samme vidtrækkende konsekvenser som Riemanns hypotese og dels kan den måske bevises ud fra Riemanns hypotese: de første betydningsfulde resultater man fandt som var beslægtede med Goldbachs formodning, byggede på Riemanns hypotese, det viste sig dog senere at de kan bevises uden Riemanns hypotese. Men fordi Goldbachs formodning er så elementær, er den det uløste matematiske problem som flest mennesker i nyere tid har kastet sig over - efter at de klassiske problemer såsom cirklens kvadratur og vinklens tredeling er blevet bevist at være uløselige. Derfor har det i nyere tid været Goldbachs formodning som har forvoldt megen menneskelig ulykke. Om denne mørke side af matematikken kan man læse i en roman hvor det netop er Goldbachs formodning der er synderen: Apostolos Doxiadis': "Onkel Petros og Goldbachs formodning" (Gyldendal, 2001). Denne roman har masser af dybde og spænding, og da forfatteren selv er matematiker får man en del at vide om matematikkens mennesker og dens forskellige discipliner og problemer. Men det er en udpræget *romantisk* roman: handlingen udspilles i de første tre fjerdedele af det 20. århundrede og dens mennesketyper og fagets position i den almindelige bevidsthed er en saga blot. Og det er ikke "virkeligheden" der skildres, men netop fortidens romantiske forestilling om matematikeren og hans fag - ikke mindst den magt som det var berygtet for at kunne få over den sjæl som var modtagelig og ikke tog sig iagt. Desuden betyder det at romanen overholder reglerne - hvilket kan skyldes forfatterens frygt for forlag og læsere - at de faglige muligheder som stoffet indbyder til ikke udnyttes. Ja selv Euklids ovenfor omtalte bevis for at der er uendelig mange primtal skønnes at overstige læserens fatteevne: af beviset hører man kun begyndelsen og slutningen, indmaden er erstattet af sætningen "Med en hurtig, energisk krattende blyant mod papiret og et par forklarende ord demonstrerede onkel Petros vor vise forfaders bevis for mig, og gav mig samtidig mit første eksempel på ægte matematik". Måske kan denne udeladelse dog også skyldes at dette stykke matematik ikke har format nok, men hvorfor viser forfatteren så ikke et andet stykke ægte matematik indenfor dette emne? - der er da masser at tage af, som vi nu skal se.

Således lyder den famøse påstand som ethvert barn kan forstå, men som det måske aldrig vil lykkes for mennesket at bevise:

*ethvert lige tal kan skrives som summen af to primtal*

Her har det første lige tal 2 en særstilling, idet vi godt nok har 2 = 1+1, men 1 regnes normalt ikke for et primtal. Men ellers har vi 4 = 2+2, 6 = 3+3, 8 = 3+5, 10 = 3+7 = 5+5, osv. Efter 12 kan opspaltningen altid ske på flere måder.

Goldbachs formodning har sit navn fra *Christian Goldbach* (1690-1764) som var professor i matematik ved det russiske kejserlige akademi og lærer for Peter den Store. I 1742 skrev han i et brev til Euler, at han formodede at "ethvert tal kan skrives som en sum af tre primtal". Euler svarede at dette er ensbetydende med at "ethvert lige tal kan skrives som en sum af to primtal", og det er denne måde at udtrykke påstanden på der senere har fået navnet Goldbachs formodning.

Eulers bevis for at de to påstande er ensbetydende forløber nogenlunde således: antag at "ethvert lige tal er summen af to primtal" og at vi har et tal n, så vil n være summen af tre primtal, for hvis n er lige, så er n-2 lige og derfor summen af to primtal, og hvis n er ulige, så er n-3 lige og derfor summen af to primtal, i begge tilfælde er n summen af tre primtal. Og omvendt: antag at "ethvert tal er summen af tre primtal" og at vi har et lige tal n, så vil n være summen af to primtal, for n+2 er summen af tre primtal, men da dette tal er lige må et af de tre primtal være tallet 2, ergo er n summen af to primtal.

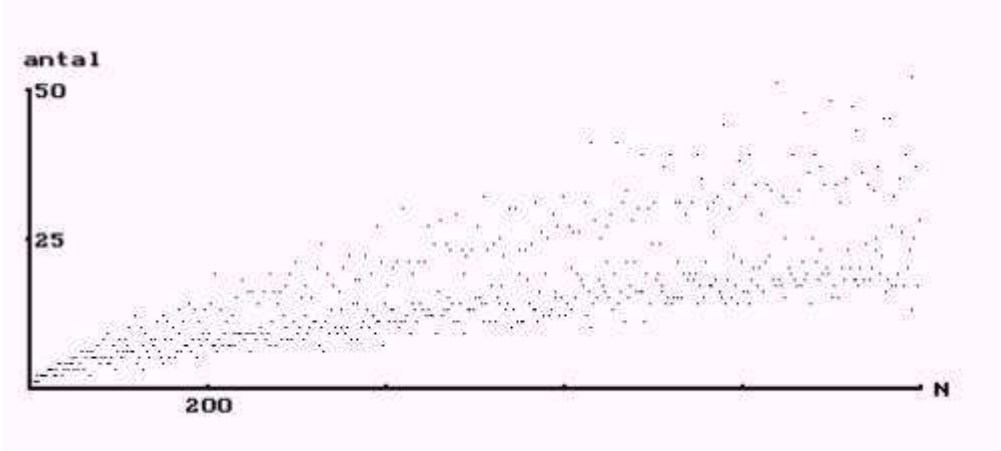
Men denne "kendsgerning" om tallene er måske ældgammel. Den er omtalt af *Descartes* (1596-1650), som skriver et sted at "ethvert lige tal er summen af et eller to eller tre primtal" (hvorfor dog ordet "lige"? - det kan tydeligvis udelades), og påstanden findes første gang på tryk i en bog fra 1770 af *Waring* om "algebraiske spekulationer". Men det var først i slutningen af 1800-tallet at man begyndte at beskæftige sig alvorligt med problemet. Foruden at man forsøgte at bevise påstanden, efterprøvede man den (den var i 1900 eftervist for tallene op til 10.000), og desuden forsøgte man at finde en tilnærmelsesformel for antallet af måder $\nu_N$ hvorpå et givet lige tal N kan skrives som summen af to primtal.

En sådan tilnærmelsesformel blev opstillet af *Sylvester* i 1871 og den lyder:

$\nu_N \approx$ 2 gange produktet af tallene (p-2)/(p-1) for de ulige primtal p < N som ikke går op i N gange $\pi_N$ (antallet af primtal mindre end N) divideret med logN.

Og havde Sylvester haft en computer, ville han straks have set at hans formel

er forkert, tallet bliver nemlig 1.123... gange for stort. Man skal dog op på meget store tal N førend denne tilnærmelsesformel er god: afvigelsen er af samme størrelsesorden som afvigelsen ved tilnærmelsen $\pi_N \approx N/\log N$. Og faktisk findes der ikke nogen formel for $\nu_N$ af samme slags som Riemanns eksakte formel for $\pi_N$. Det hænger sammen med at funktionen $\nu_N$ varierer stærkt:




Den korrekte formel for $\nu_N$ som svarer til Sylvesters formel, blev fundet omkring 1920 af *G.H. Hardy* og *J.E. Littlewood*, og den lyder:

$$\nu_N \approx 2\prod_{\substack{p \text{ ulige primtal}}}(1/(1-(p-1)^2)\prod_{\substack{p \text{ ulige primtal}\\ \text{som går op i N}}}((p-1)/(p-2))\, N/(\log N)^2$$

- og den kaldes stadig Sylvesters formel, fordi det væsentlige i Sylvesters formel trods alt er rigtigt. Det første produkt er uafhængigt af N og kan udregnes én gang for alle: $\prod(1/(1-(p-1)^2)$ (produkt over primtallene > 2) = 0.66016....

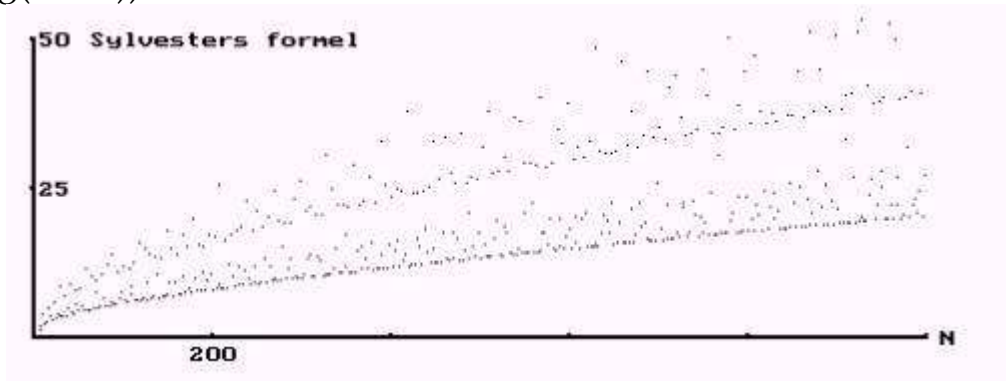
Man har senere vist at denne formel kan forbedres betydeligt, således at den får en nøjagtighed af samme grad som Gauss' formel

$$\pi_N \approx \mathrm{Li}(N) = \int_0^N dx/\log x,$$

nemlig ved at ændre lidt i Hardy & Littlewoods fremgangsmåde (vi kommer ind på dette i det sidste kapitel). Den forbedrede formel lyder:

$$\nu_N \approx 2\prod_{\text{p ulige primtal}}(1/(1-(p-1)^2)\prod_{\substack{\text{p ulige primtal}\\ \text{som går op i N}}}((p-1)/(p-2))\int_0^N dx/(\log(N-x)\log(N+x))$$

- og det er denne jeg har tastet ind i programmet "Goldbachs formodning", idet der som tilnærmelse til integralet blot benyttes summen af tallene 1/(log (N-m)log(N+m)) fra m = 0 til m = N-2.




Jeg vil skitsere Hardy & Littlewoods bevis i det sidste kapitel. På deres tid var der en livlig aktivitet igang for at bevise Goldbachs formodning. Den mest aktive var onkel Petros i Apostolos Doxiadis' roman. Men i næsten alle disse forsøg var den matematik man betjente sig af af elementær natur. Den mest benyttede metode var *sigtemetoden,* som tager udgangspunkt i *Eratosthenes'* (250 f. Kr.) metode til at opskrive alle primtallene imellem √n og n: først fjernes de tal der er delelige med 2, så fjernes de tal der er delelige med 3, osv., dette gøres for alle primtallene op til √n. En anden metode var *tæthedsmetoden.* Men alle sådanne elementære metoder blev forkastet (og ringeagtet) af Hardy & Littlewood. Disse mente at den metode som Riemann var slået ind på i sin udforskning af primtallene - den *analytiske metode* - var den eneste vej frem. Hardy & Littlewoods metode - *cirkelmetoden,* som den analytiske metode kaldes i dette konkrete tilfælde - så yderst lovende ud, og det er i hvert fald den mest elegante af alle de metoder man har forsøgt sig med, så cirkelmetoden vil have interesse uanset hvordan det går med Goldbachs formodning.

Men er skæbnens ironi at alle de bedste resultater man indtil nu er nået frem til, når det gælder spørgsmål der er beslægtet med Goldbachs formodning, netop er opnået ved de metoder som Hardy & Littlewood forkastede. Det allerbedste resultat bygger på sigtemetoden og skyldes *Chen Jing Run* som i 1966 beviste at:

*ethvert tilstrækkelig stort lige tal er summen af et primtal*

*og et tal som højst har to primfaktorer.*

Og ved hjælp af tæthedsmetoden beviste Schnirelmann i 1930 at:

*der findes et fast tal k således at ethvert tal*
*kan skrives som en sum af højst k primtal,*

og det blev umiddelbart efter vist at k kan vælges lig 67. Dette tal er i tidens løb blevet reduceret, det er vist nået ned til 19: det er altså bevist at ethvert tal kan skrives som summen af højst 19 primtal. Det er dog også blevet bevist, at ethvert *tilstrækkelig stort* tal kan skrives som summen af højst 6 primtal (Vaughan, 1977).

Men der er noget fordægt over disse resultater. Om så det var blevet bevist at *ethvert* tal kan skrives som summen af højst 6 primtal, så er dette resultat latterligt i forhold til Goldbachs formodning, der som sagt er ensbetydende med at ethvert tal kan skrives som summen af højst 3 primtal. Og hver gang der her tales om et *tilstrækkelig stort* tal, så viser det sig altid, når man forsøger at estimere det, at det tal man kommer frem til har en svimlende størrelse, f.eks. $10^{4000000}$. Dvs. for at kunne sige at sætningen er komplet bevist, skal den bevises med computer for de tal der er mindre end dette tal, og ingen computer kommer måske nogensinde til at kunne udføre en sådan optælling for tal der er større end $10^{40}$.

Dette er det absurde ved den del af talteorien der har med primtallene at gøre. Hardy & Littlewood kendte dog næppe til omfanget af denne absurditet: de havde satset på at bevise at ethvert tilstrækkelig stort lige tal kan skrives som summen af to primtal, det måtte være det væsentlige, og det var det der forekom dem muligt ved hjælp af deres cirkelmetode. Cirkelmetoden kunne klart bruges til at udlede Sylvesters tilnærmelsesformel, og den afvigelse der er imellem det antal denne giver og det sande antal, kunne man måske estimere godt nok til at bevise at den for voksende N bliver af forsvindende betydning. Og så måtte Goldbachs formodning betragtes som værende bevist. Men restleddet ville - og vil fortsat - ikke lade sig estimere. Der er noget der går galt fire steder. F.eks. skal man vise, at et tal som afhænger af N er af mindre størrelsesorden end $N^{\varepsilon}$, hvor $\varepsilon < ½$, men man kan kun vise at tallet er af mindre størrelsesorden end $N^{½}$. Det er således lige på grænsen at beviset svigter.

Hardy & Littlewood gjorde derefter det, at de generaliserede problemet, således at de for et givet naturligt tal $r \geq 2$, søgte efter en formel for antallet af

måder hvorpå et tal N kan skrives som summen af r primtal. Og det viste sig, at når r > 2 *kan* restleddet estimeres. Dog kun under forudsætning af at en "mild Riemann hypotese" gælder for de såkaldte Dirichlets L-funktioner (herom senere). Hardy & Littlewood beviste altså næsten at

*ethvert ulige tal kan skrives som summen af tre primtal.*

I 1937 lykkedes det for *Vinogradov* at bevise at den milde Riemann hypotese som Hardy & Littlewood måtte forudsætte, kan undværes. Vinogradov beviste altså at restleddet i Hardy & Littlewoods formel for antallet af måder hvorpå et ulige tal N kan skrives som summen af tre primtal, er af relativt forsvindende betydning. Men en nærmere undersøgelse af Vinogradovs restled viste, at N skal være større end det nævnte tal $10^{4000000}$ førend man kan være sikker på at restleddet ikke laver ulykker, og dette tal er stort set ikke forbedret siden.

Hvad kan der være galt siden Goldbachs formodning modsætter sig et bevis? Ja ifølge onkel Petros er det *Gödel* (1906-78) som er skyld i det altsammen. I 1933 hører onkel Petros - efter over ti års arbejde på at bevise Goldbachs formodning - tilfældigt om en afhandling fra 1931 af en ung mand ved navn Kurt Gödel, og som havde rystet hele den matematiske verden i sin grundvold. Hele verden undtagen onkel Petros, for han havde haft så travlt med Goldbachs formodning at han først hører om det to år senere. I afhandlingen "Über formal unentschiedbare Sätze der Principia Mathematica und verwandter Systeme I" konstruerer Gödel et matematisk udsagn som er *sandt,* men som *ikke* kan bevises. Og han beviser desuden at man ikke kan *bevise* at matematikken er modsigelsesfri. Mere præcist beviste Gödel at "i enhver matematisk teori, som omfatter aritmetikken, findes udsagn som hverken kan bevises eller modbevises" og at "i en teori, som omfatter aritmetikken, kan et bevis for at den er modsigelsesfri ikke formaliseres indenfor teorien selv". Dette sidste betyder, at vi *i teorien* en dag kan risikere at støde på et matematisk udsagn som både kan bevises at være sandt og falsk. Så formalismen (side ...) *kan* altså bryde sammen, og matematikerne således måske tvunget til at slå ind på intuitionismens vej. Ingen formalist tror selvfølgelig på at dette vil ske. Og skulle katastrofen ske, ville den menige matematiker næppe komme til at mærke noget til det: den præcise årsag ville blive fundet og et mere sikkert grundlag ville blive etableret, ikke mindst fordi den moderne matematiske logik er gennemsyret af intuitionistisk tænkning og terminologi.

Den sætning at der findes udsagn som ikke kan bevises, fik Gödel ideen til ved at studere *Richard*'s paradoks (1905):

Vi ordner alle sproglige udsagn, hvori der indgår netop ét (variabelt) naturligt tal n, på rad og række (efter et leksikografisk princip). Det k-te udsagn betegnes Ek(n). Vi betragter nu udsagnet "En(n) er falsk". Da dette er et sprogligt udsagn, hvori der indgår netop ét (variabelt) naturligt tal n, må det være blandt Ek-erne. Lad os antage at det har nummer q, så har vi:

Eq(n) = "En(n) er falsk".

Men heraf følger (for n=q) at hvis Eq(q) er sand er Eq(q) falsk, og omvendt.

Gödels resultat, som jo umiddelbart er nedslående, er - af populærjournalistikken - blevet udråbt til ikke bare at være matematikkens fallit, men selve den menneskelige tænknings fallit. Men i virkeligheden er der ikke noget særlig mærkeligt i Gödels sætninger. Thi at bevise noget indenfor matematikken betyder at udlede det ad strengt logisk vej *ud fra* noget andet, således at det i sidste ende er bevist ud fra nogle helt grundlæggende men ubeviste antagelser, de såkaldte *aksiomer.* Disse aksiomer og de grundlæggende logiske slutningsregler som man må benytte sig af, havde man på denne tid helt klart styr på. Dels havde man *Russell & Whiteheads* trebindsværk "Principia Mathematica" fra 1910-13, og dels havde man *Zermelo-Fraenkels* aksiomsystem udviklet i årene 1908-24. Ved hjælp af disse aksiomsystemer kan man bevise langt de fleste "almindelige" matematiske udsagn som er sande. Men det er klart, at da ethvert aksiomsystem vil være af *endelig* natur, er det kun *nogle* af alle de tænkelige matematiske udsagn man kan opskrive, som kan bevises eller modbevises ud fra det *givne* aksiomsystem. Og man kan vel også forestille sig, at selv om man har et nok så omfattende aksiomsystem, så vil der altid være udsagn som man kan *argumentere for* må betragtes som sande, men som ikke kan bevises ud fra dette aksiomsystem. Spørgsmålet er bare hvor eksotisk et sådant udsagn vil se ud. Udsagn af den type Gödel konstruerede, behøver ingen matematiker at bekymre sig om, men det *kan* være, at der er helt normale matematiske udsagn som *er* sande (og det *er* Goldbachs formodning), men som unddrager sig et bevis ud fra det aksiomsystem som matematikerne idag officielt betjener sig af (Zermelo-Fraenkels aksiomsystem).

I hvert fald var onkel Petros lammet efter at en ung student havde bedt ham være behjælpelig med at oversætte en opsigtsvækkende afhandling fra tysk. Oh skræk! Måske hører *Goldbachs formodning* blandt de sætninger som ikke kan bevises! Måske har alt hans arbejde været spildt! Jeg skal ikke røbe mere af handlingen i denne roman, den er glimrende og den ender overordentlig dramatisk.

Et andet elementært og uløst problem er som sagt spørgsmålet om hvorvidt der er uendelig mange *primtalstvillinger,* dvs. par af primtal hvis differens er

2. Dette problem er nært beslægtet med Goldbachs formodning: hvis det ene problem kan bevises, kan det andet også. Der *er* uendelig mange primtalstvillinger, det viser computerundersøgelser, og ved hjælp af cirkelmetoden kan man finde en tilnærmelsesformel for antallet mindre end et givet tal N. Den lyder:

*antallet af primtalstvillinger mindre end N er tilnærmelsesvist givet ved*

$$2\prod_{\text{p ulige primtal}}(1/(1-(p-1)^2)\int_0^N dx/(\log x)^2.$$

Produktet er det samme som før: 0.66016 (som tilnærmelse til integralet kan man blot bruge summen af tallene $1/(\log m)^2$ fra m = 2 til m = N). Af formlen følger at sandsynligheden for at tallene N og N+2 er primtalstvillinger er omkring $1.32/(\log N)^2$ (sandsynligheden for at N er et primtal er som sagt $1/\log N$). Rækken af de reciproke primtal

$$1/2 + 1/3 + 1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/23 + 1/29 + ...$$

er divergent (se side ...), men den tilsvarende række for primtalstvillinger

$$1/2 + 1/3 + 1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + ...$$

er konvergent: dens sum er 1.90216054... (Viggo Brun, 1919).

Ved hjælp af den samme metode som Riemann benyttede til at udlede sin formel for $\pi_N$, kan man udlede en formel for summen af logaritmerne til primtallene mindre end N:

$$\sum_{\text{p primtal}<N} \log p.$$

Den vigtigste del af denne formel er

$$\sum_{m=1}^{N} \mu(m)\, N^{1/m},$$

og den vigtigste del af denne sum er tallet N. Dette kan også formuleres således:

*produktet af primtallene op til N er tilnærmelsesvist tallet $e^N$.*

En tilnærmelsesformel som er meget mere nøjagtig end denne er følgende:

$$\sum_{p \text{ primtal og } p^r < N} \log p \approx N$$

(summen er her over alle primtals*potenserne* $p^r$ mindre end N, idet hverts bidrag dog kun er logaritmen af dens rod p).

Et resultat som ikke har noget med primtal at gøre, men som kan udledes ved samme metode, og som minder lidt om Goldbachs problem, lyder: hvis $\kappa_n$ er antallet af måder hvorpå n kan skrives som summen af to kvadrattal (f.eks. 50 = 1 + 49 = 25 + 25), gælder

$$1/N \sum_{n=1}^{N} \kappa_n \approx \pi/8.$$

Dvs. det gennemsnitlige antal måder hvorpå et tal kan skrives som en sum af to kvadrattal er $\pi/8 = 0.3927....$ Men dette kan vises helt elementært ud fra Pythagoras' sætning.