HVOR MANGE PRIMTALL FINNES DET?

KTH

9. Februar 96

Resume, referenser og matematikere.

Resume

Til tross for at vi alle vet at det finnes uendelig mange primtall kan spørsmålet *hvor mange primtall finnes det* ha flere, helt presise, meninger. I dette foredraget skal vi diskutere noe måter antallet primtall kan måles på og vise hvordan disse er knyttet til noen av de mest interessante åpne problemene i matematikken.

Joseph Louis François Bertrand (1822-1900).
Viggo Brun (1885-1978).
Peter Gustav Lejeune-Dirichlet (1805-1859).
Paul Erdös (1913-).
Leonhard Euler (1707-1783).
Carl Friedrich Gauss (1777-1855).
Jacques Salomon Hadamard (1865-1963).
Helge von Koch (1870-1924).
Adrien-Marie Legendre (1752-1833).
John Edensor Littlewood (1885-1977).
Georg Friedrich Bernhard Riemann (1826-1866).
Charles-Jean de la Vallée Poussin (1866-1962).
Atle Selberg (1917-2007).
Pafnuti L. Tchebycheff (1821-1894).

Referenser:

Hans Riesel, *Prime numbers and computer methods for factorization (Second Edition)*, Birkhäuser 1994.

Victor Klee & Stan Wagon, *Old and new unsolved problems in plane geometry and number theory*, Math. Ass. of America, Dolciani Math. Expositions No. 11, 1991.

Paulo Ribenboim, *The little book of big primes*, Springer Verlag 1991.

Primtall.

primtall

Studiet av primtall er et av de mest fascinerende områdene i matematikken. Problemene tilhører de elste innenfor vitenskapene og noen av de mest kjente vitenskapsmennene på 17-, 18- og 1900 tallet har arbeidet med dem. Mange av problemene kan også formuleres så lekmenn kan forstå dem.

Et primtall er et heltall større eller lik 2 som ikke har andre positive heltall som divisorer enn seg selv og 1.

De kan finnes ved en *sold* metode:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101									

Vi finner 26 primtall mindre enn 102:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101.

Vi skal nummerere primtallene slik at

$$p_1 = 2, p_2 = 3, p_3 = 5, \ldots.$$

Det finnes uendelig mange primtall.

∞ primtall

Euklids bevis

Euclid: Anta at $p_1, p_2, \ldots, p_r$ er de n første primtallene. Vi kan skrive $P = p_1 p_2 \cdots p_r + 1$ som et produkt av primtall. La p være det minste av disse. Da kan ikke p være et av tallene $p_1, \ldots, p_n$, fordi den da vil dele $P - p_1 p_2 \cdots p_r = 1$, hvilket er umulig. Vi har fått et nytt primtall p. Slik kan vi fortsette å konstruere nye primtall.

Vi skal nu gi et annet bevis, som har hatt mye større betydning for matematikken.

Euler

Euler: Vi kjenner alle til følgende resultat om *geometriske serier.*

Lemma 1. *Serien* $\sum_{n=0}^{\infty} x^n$ *konvergerer mot* $\frac{1}{1-x}$ *om* $0 \leq x < 1$ *og divergerer om* $x \geq 1$.

Vi får at

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots,$$

for hvert primtall p. Om q er et annet primtall får vi

$$\begin{aligned}\frac{1}{\left(1-\frac{1}{p}\right)}\frac{1}{\left(1-\frac{1}{q}\right)} &= \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)\left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots\right) \\ &= 1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots.\end{aligned}$$

På høyre side har vi summen av inversene til alle positive heltall som kan skrives på formen $p^m q^n$. Merk at vi har brukt det velkjente resultatet:

Lemma 2. *La* $\sum_{n=0}^{\infty} a_n$ *og* $\sum_{n=0}^{\infty} b_n$ *være serier som konvergerer mot* A *henholdsvis* B*, og der* $\sum_{n=0}^{\infty} a_n$ *konvergerer absolutt. Da konvergerer serien* $\sum_{n=0}^{\infty} c_n$*, der* $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ *mot* AB.

Samme resonnement som ovenfor gir at

$$\text{(E)} \qquad \prod_{i=1}^{r} \frac{1}{1-\frac{1}{p_i}} = \sum_{n=p_1^{n_1}\cdots p_r^{n_r}} \frac{1}{n}.$$

Eulers bevis

Anta nu at det er et endelig antall primtall $p_1, p_2, \ldots, p_r$. Da vil høyre siden av (E) være lik den *harmoniske rekken* $1 + \frac{1}{2} + \frac{1}{3} + \cdots$. Denne sekvensen divergerer, så den kan ikke være lik tallet på venstre side. Vi får en motsigelse mot antagelsen at det bare finnes et endelig antall primtall.

Vi kan si noe mer om hvordan $\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)^{-1}$ vokser. La oss først, for et gitt tall x definere $[x]$ som heltallet bestemt ved $[x] \leq x < [x]+1$.

Lemma 3. *Vi har at*

$$\sum_{n=2}^{[x]} \frac{1}{n} < \log x < \sum_{n=1}^{[x]} \frac{1}{n}.$$

Bevis. Summen $\sum_{n=1}^{[x]} \frac{1}{n}$ er trappen over integralet $\int_1^{[x]+1} \frac{1}{t} dt$ så vi har ulikheter $\sum_{n=1}^{[x]} \frac{1}{n} > \int_1^{[x]+1} \frac{1}{t} dt = \log([x]+1) > \log x$.

På samme måte har vi at $\sum_{n=2}^{[x]} \frac{1}{n}$ er summen under integralet $\int_1^{[x]} \frac{1}{t} dt$, så vi har at $\sum_{n=2}^{[x]} \frac{1}{n} < \log[x] \leq \log x$.

Proposisjon 4. *For $x \geq 2$ har vi at*

$$\log x < \prod_{p_i \leq x} \frac{1}{1 - \frac{1}{p_i}}.$$

Bevis. Vi har sett i (E) ovenfor at $\prod_{p_i \leq x} \left(1 - \frac{1}{p_i}\right)^{-1} > \sum_{n=1}^{[x]} \frac{1}{n}$. Resultatet følger derfor av den høyre ulikheten i Lemma 3.

Eulers metode

Eulers bevis benytter en av matematikkhistoriens viktigste metoder. For å se dette behøver vi resultatet:

Lemma 5. *Anta at $a_1 \geq a_2 \geq \cdots \geq 0$. Da konvergerer serien $\sum_{n=1}^{\infty} a_n$, hvis og bare hvis sekvensen*

$$\sum_{k=0}^{\infty} 2^k a_{2^k} = a_1 + 2a_2 + 4a_4 + \cdots$$

konvergerer.

Setning 6 (Euler). *Serien $\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma}$ konvergerer om $\sigma > 1$ og divergerer om $\sigma \leq 1$.*

Bevis. Om $\sigma \leq 0$ går ikke hvert ledd mot null så sekvensen divergerer. Om $\sigma > 0$ følger det av Lemma 5 at serien $\sum_{n=1}^{\infty} a_n$ konvergerer hvis og bare hvis $\sum_{k=0}^{\infty} 2^k \frac{1}{2^{k\sigma}} = \sum_{k=0}^{\infty} 2^{(1-\sigma)k}$ konvergerer. Den siste serien konvergerer hvis og bare hvis $2^{1-\sigma} < 1$, det vil si, hvis og bare hvis $1 < \sigma$, på grunn av Lemma 1 om geometriske serier.

Samme resonnement som vi brukte for å vise (E) gir også at

$$(\mathrm{E}_\sigma) \qquad \prod_{i=1}^{r} \frac{1}{1 - \frac{1}{p_i^\sigma}} = \sum_{n = p_1^{n_1} \cdots p_r^{n_r}} \frac{1}{n^\sigma}.$$

Beviset til Euler kan da omformuleres som:

Om det finnes et endelig antall primtall $p_1, p_2, \ldots$ vil summen til høyre være over alle tall. Produktet til venstre vil derfor gå mot et reelt tall når σ går mot 1 ovenfra, mens høyre siden går mot uendelig ettersom den harmoniske serien $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ divergerer. Vi får igjen en motsigelse mot antagelsen at vi har et endelig antall primtall.

Av Setning 6 og formelen (E_σ) får vi at

$$\zeta(\sigma) = \prod_{i=1}^{\infty} \frac{1}{1 - \frac{1}{p_i^\sigma}}.$$

Vi har derfor et vakkert samband mellom primtall og analysen.

$\zeta(2k)$

Funksjonen $\zeta(\sigma) = 1 + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \cdots$ for reelle tall ble først studert av Euler. Han viste, blandt annet, at

$$\zeta(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!},$$

der $B_0, B_1, B_2, \ldots$ er Bernoullitallene, definert ved:

$$\frac{x}{e^x - 1} = \sum_{k=1}^{\infty} \frac{B_k}{k!}x^k,$$

eller ekvivalent ved at $B_0 = 1$ og at

$$\binom{k+1}{1}B_k + \binom{k+1}{2}B_{k-1} + \cdots + \binom{k+1}{k}B_1 + B_0 = 0,$$

for $k = 1, 2, \ldots$. (Vis denne ekvivalensen).

Vi får spesielt at $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $\ldots$ og at $\zeta(2) = \frac{\pi^2}{6}$. Verdiene for $\zeta(n)$ når n er odde kjenner vi ikke eksakt, bortsett fra at Apéry viste at $\zeta(3)$ er irrasjonalt. Apérys bevis kalles ofte *beviset som Euler overså.*

Antall primtall I.

 # primtall I

Vi har sett at serien $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ divergerer mens serien $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ konvergerer. Vi kan derfor påstå at det finnes *fler* tall i mengden $1, 2, 3, \ldots$, enn i $1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$.

Vi kan derfor spørre om det er mange tall i serien $p_1, p_2, \ldots$ av alle primtall i den bemerkelsen at $\frac{1}{p_1} + \frac{1}{p_2} + \cdots$ divergerer. For å svare på dette behøver vi resultatet:

Lemma 7. *For $0 \le x \le \frac{1}{2}$ har vi at*

$$-\log(1-x) \le 2x.$$

Bevis. Funksjonen $2x + \log(1-x)$ er null for $x = 0$ og har positiv derivert i intervallet $0 < x \le \frac{1}{2}$

Setning 8. *Vi har at*

$$\sum_{p_i \le x} \frac{1}{p_i} > \frac{1}{2}\log\log x.$$

Spesielt har vi at serien $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots$ *divergerer.*

Bevis. Vi har at

$$\sum_{p_i \le x} \frac{1}{p_i} = \frac{1}{2} \sum_{p_i \le x} \frac{2}{p_i} \ge -\frac{1}{2} \sum_{p_i \le x} \log\left(1 - \frac{1}{p_i}\right)$$
$$= -\frac{1}{2} \log\left(\prod_{p_i \le x} \left(1 - \frac{1}{p_i}\right)\right) = \frac{1}{2} \log\left(\prod_{p_i \le x} \frac{1}{1 - \frac{1}{p_i}}\right)$$

→ der vi har brukt Lemma 7 for ulikheten. Setningen følger nu av
→ ulikheten i Proposisjon 4.

Tvillinger

Primtallstvillinger Primtallstvillinger er primtall p slik at $p - 2$ eller $p + 2$ også er et primtall. Under 101 har vi 8 par av primtallstvillinger $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$, $(41, 43)$, $(59, 61)$, $(71, 73)$. Vi vet fremdeles ikke om det finnes uendelig mange slike par. Brun viste at $\sum_{p=\text{primtallstvilling}} \frac{1}{p}$ konvergerer. Han brukte soldmetoder som senere har vist seg å være blandt de mest nyttige i tallteorien. Vi skal illustrere en slik soldmetode i seksjonen om heuristiske bevis lenger bak.

Artim. ser.

Primtall i aritmetiske serier Dirichlet viste at det i hver aritmetisk serie

$$a + b, 2a + b, 3a + b, 4a + b, \ldots,$$

Drichlet-Euler

der a og b er innbyrdes primiske heltall, finnes et uendelig antall primtall. Han viste også at summen av de inverse av disse primtallene divergerer. Dirichlets bevis var et pionerarbeide når det gjaldt å bruke analytiske metoder til å bevise satser i tallteorien. Hans metode, som var inspirert av metoden til Euler, som vi har sett ovenfor, gikk ut på å vise at det finnes uendelig mange primtall i en aritmetisk sekvens hvis og bare hvis en analytisk funksjon på formen $L_\chi(\sigma) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^\sigma}$, der χ er en *karakter*, også kalt Dirichlet serier, ikke var null i punktet 1, og deretter bruke analytiske metoder til å vise at funksjonen ikke forsvant i punktet.

Antall primtall II.

 # primtall II

En annen måte å måle antallet primtall på er å betrakte antallet primtall $\pi(x)$ mindre eller lik et gitt tall x. Vi har $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, $\pi(5) = 3$, $\pi(6) = 3$, $\ldots$, $\pi(101) = 26$, $\ldots$.

Primtallsatsen

Gauss, 15 år gammel og inspirert av Legendre, gjettet på at $\pi(x)$ er omtrent lik $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$, når x er stor. For å uttrykke dette på en lett måte setter vi $f(x) \sim g(x)$ om $f(x)$ og $g(x)$ blir omtrent like store når x blir stor, med andre ord, om $g(x) \neq 0$ når x er stor og $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ Vi kan da uttrykke Gauss' gjetning som

$$\pi(x) \sim \mathrm{Li}(x).$$

Primtallsatsen

Denne gjetningen kalles *primtallsatsen*.

Lemma 9 (L'Hospitals regel). *Anta at f og g er differensiable funksjoner på et intervall (a,b) og $g'(x) \neq 0$, for alle $x \in (a,b)$, der $-\infty \leq a < b \leq +\infty$. Om $\frac{f'(x)}{g'(x)} \to A$ og $g(x) \to +\infty$, når $x \to a$ vil $\frac{f(x)}{g(x)} \to A$.*

Bruker vi L'Hospitals regel med $f(x) = \int_2^\infty \mathrm{Li}(x)$, $g(x) = \frac{x}{\log x}$, $a = 2$ og $b = +\infty$ får vi at primtallsatsen kan uttrykkes som:

$$\pi(x) \sim \frac{x}{\log x}.$$

$\mathrm{Li}(x) - \pi(x)$

For alle kjente verdier av x har vi at $\pi(x) < \mathrm{Li}(x)$, og det er sant for $x \leq 10^{20}$. Alle trodde dette altid holdt til Littlewood i 1914 viste at det finnes en uendelig sekvens av tall $x_1, x_2, \ldots$, slik at $x_j \to \infty$ og slik at $\mathrm{Li}(x_j) < \pi(x_j)$. At vi ennu ikke kjenner et eneste slikt tall viser at vi skal være forsiktige med å dra slutninger av eksperimenter, og at datamaskinene ofte ikke klarer av interessante problemer. Vi vet at mellom $6.62 \cdot 10^{370}$ og $6.69 \cdot 10^{370}$ finnes det minst 10^{180} heltall n slik at $\pi(n) > \mathrm{Li}(n)$.

Tchebycheff

De første alvorlige stegene mot å vise primtallsatsen ble tatt av Tchebycheff omkring 1850. Han viste at

$$\frac{7}{8}\frac{x}{\log x} < \pi(x) < \frac{9}{8}\frac{x}{\log x}.$$

Tchebycheff viste dessuten at

$$\frac{1}{3}\frac{n}{\log n} < \pi(2n) - \pi(n) < \frac{7}{5}\frac{n}{\log n},$$

Bertands post.

slik at $\pi(2n) - \pi(n) \geq 1$, for alle tall $n \geq 2$ Det vil si at mellom et tall og dets doble finnes det alltid minst et primtall. Dette kalles for *Bertrands postulat.*

Mange av Tchebycheffs beviser er basert på resultatet at

$$\sum_{p_i \leq x} \frac{\log p_i}{p_i} \sim x.$$

Vi skal bruke dette resultatet i et heuristisk bevis for primtallsatsen lenger bak. Ettersom det finnes ganske enkle beviser for dette, som dessuten bruker soldmetoder tar vi med et bevis i seksjonen om heuristiske bevis.

Bev. for primts.

Primtallsatsen ble vist i 1896 av Hadamard og de la Vallée Poussin, uavhengig av hverandre. Begge to brukte metoder fra funksjonsteorien. Enorme anstrengelser ble gjort for å vise satsen uten å bruke funksjonsteori, det vil si med *elementære metoder*. Hadamard sa at "den korteste veien mellom to satser om de reelle tallene gaar via de komplekse tallene". Primtallsatsen ble vist med elementære metoder av Selberg og Erdös i 1948.

Riemanns hypotese.

Riemanns hyp.

Det viktigste problemet i matematikken er å vise at det finnes en konstant C slik at

$$|\operatorname{Li}(x) - \pi(x)| < C\sqrt{x}\log x,$$

for store x.

Vi skal gi en annen og mye mer kjent formulering av Riemanns hypotese. Denne formuleringen handler om nullpunktene til funksjonen $\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}}$ kalt Riemanns zeta funksjon når σ er et komplekst tall. Som den står konvergerer den bare når realdelen av σ er større enn 1, men Riemann viste at den kan utvides til en funksjon på hele det komplekse planet bortsett fra 1. Euler betraktet funksjonen for reelle σ, men det var Riemann som innså hvilket potensial det lå i å betrakte zetafunksjonen som en kompleks funksjon, og som så de dype relasjonene som finnes mellom egenskapene til zetafunksjonen og distribusjonen av primtall.

$\zeta(\sigma)$ kompl.

kompl. anal.

Den andre formulering av Riemanns hypotese, som er Riemanns egen, og som vi nevnte ovenfor er:

Riemanns Hypotese: Alle de ikke reelle nullpunktene til $\zeta(\sigma)$ er på formen $\frac{1}{2} + ib$.

Det var von Koch som viste ekvivalensen av de to formuleringene. Vi skal gi en formulering av den siste versjonen som ikke nevner komplekse tall. For dette behøver vi et par resultater til:

Lemma. *Vi har at* $\zeta(\sigma) = \left(\frac{1}{1-2\cdot 2^{-\sigma}}\right) \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^{\sigma}}$, *for* $\sigma > 1$.

Bevis. Vi har at

$$\begin{aligned}
&\left(1+\frac{1}{2^\sigma}+\frac{1}{3^\sigma}+\cdots\right)\left(1-\frac{2}{2^\sigma}\right)\\
&=1+\frac{1}{2^\sigma}-1\cdot\frac{2}{2^\sigma}+\frac{1}{3^\sigma}+\frac{1}{4^\sigma}-\frac{1}{2^\sigma}\frac{2}{2^\sigma}+\cdots\\
&+\frac{1}{(2n-1)^\sigma}+\frac{1}{(2n)^\sigma}-\frac{1}{n^\sigma}\frac{2}{2^\sigma}+\cdots\\
&=1-\frac{1}{2^\sigma}+\frac{1}{3^\sigma}-\frac{1}{4^\sigma}+\cdots+\frac{1}{(2n-1)^\sigma}-\frac{1}{(2n)^\sigma}+\cdots.
\end{aligned}$$

Lemma. *Anta at* $|c_1|\geq|c_2|\geq|c_3|\geq\cdots$, *at* $c_{2m-1}\geq 0$, $c_{2m}\leq 0$, *for* $m=1,2,3,\ldots$, *og at* $\lim_{n\to\infty}c_n=0$. *Da vil* $\sum_{n=0}^{\infty}c_n$ *konvergere.*

Vi har derfor at $\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^\sigma}$ konvergerer for $\sigma>0$. Derfor kan vi definere zetafunksjonen for alle $\sigma>0$ og $\sigma\neq 1$ ved

$$\zeta(\sigma)=\frac{1}{1-2^{-\sigma+1}}\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^\sigma}. \tag{Z.}$$

Med samme metode kan vi definere zetafunksjonen for komplekse tall med positiv realverdi ved serien (Z). Dette kan lett sees ved å skrive $\sigma=a+bi$ og $n^\sigma=e^{\sigma\log n}$, og å bruke at $e^{it}=\cos t+i\sin t$. Bruker vi disse substitusjonene får vi også

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^\sigma}&=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{e^{(a+bi)\log n}}\\
&=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^a(\cos(b\log n)+i\sin(b\log n))}\\
&=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^a}\left(\cos(b\log n)-i\sin(b\log n)\right).
\end{aligned}$$

Vi kan nu formulere Riemanns Hypotese uten henvisning til komplekse tall som:

Riemanns hypotese i reell versjon: *Når* $0<a<1$ *er de eneste løsningene til likningene*

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^a}\cos(b\log n)=0$$

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^a}\sin(b\log n)=0$$

med $a = \frac{1}{2}$.

Heuristisk bevis av primtallsatsen.

Eratosth. sold

Eratosthenes sold: La $A(x,r)$ være antallet heltall mindre eller lik x som ikke er delbare med noen av de r første primtallene $p_1, p_2, \ldots, p_r$. Ettersom alle primtallene mindre eller lik x, som er forskjellige fra $p_1, p_2, \ldots, p_r$ bidrar til $A(x,r)$ har vi at

$$\pi(x) \leq r + A(x,r).$$

La $1 \leq i < j < \cdots < k \leq r$. Da vil antallet tall mindre eller lik x, som er delbare med $p_i p_j \cdots p_k$ være $\left[\frac{x}{p_i p_j \cdots p_k}\right]$. Vi får derfor at

$$\begin{aligned} A(x,r) = [x] &- \sum_{1 \leq i \leq r} \left[\frac{x}{p_i}\right] + \sum_{1 \leq i < j \leq r} \left[\frac{x}{p_i p_j}\right] \\ &- \sum_{1 \leq i < j < k \leq n} \left[\frac{x}{p_i p_j p_k}\right] + \cdots + (-1)^r \left[\frac{x}{p_1 p_2 \cdots p_r}\right]. \end{aligned}$$

Forskjellen mellom $A(x,r)$ og tallet

$$\begin{aligned} x - \sum_{1 \leq i \leq r} \frac{x}{p_i} + \sum_{1 \leq i < j \leq r} \frac{x}{p_i p_j} - \sum_{1 \leq i < j < k \leq n} \frac{x}{p_i p_j p_k} \\ + \cdots + (-1)^r \frac{x}{p_1 p_2 \cdots p_r} = x \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

er høyst lik

$$1 + \binom{r}{1} + \binom{r}{2} + \cdots + \binom{r}{r} = (1+1)^r = 2^r.$$

Vi har derfor at $A(x,r) \leq 2^r + x \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$, og derfor at

$$\pi(x) \leq r + 2^r + x \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \leq 2^{r+1} + x \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Sett $r = [\log x]$. Vi har at $\log\log x < \log(r+1) \leq \log p_r$. Videre

$\rightarrow$ har vi av Proposisjon 4 at $\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) < \frac{1}{\log p_r}$. Vi får at

$$\pi(x) \leq 2 \cdot 2^{\log x} + \frac{x}{\log p_r} < 2x^{\log 2} + \frac{x}{\log p_r} < 2x^{\log 2} + \frac{x}{\log\log x}.$$

Derfor har vi at

$$\frac{\pi(x)}{\frac{x}{\log\log x}} < 1 + 2\frac{\log\log x}{x^{1-\log 2}}.$$

Lemma 10. *For hvert positivt tall a vil kvotienten $\frac{\log x}{x^a}$ gå mot null når x blir stor.*

$\rightarrow$ Av soldet ovenfor og Lemma 10 får vi derfor at

Proposisjon 11. *For store x vil*

$$\pi(x) < 2\frac{x}{\log\log x}.$$

Merk at vi kunne ta hvilket som helst tall større enn 1 istedenfor
$\rightarrow$ 2 i Proposisjon 11.

Lemma 12. *For hvert heltall m lar vi $[m]_p$ være det minste positive tallet bestemt ved at $p^{[m]_p}$ deler m, men $p^{[m]_p+1}$ ikke deler m. Da har vi*

$$[n!]_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots .$$

Derfor vil

$$n! = \prod_{p_i \leq n} p_i^{\left(\left[\frac{n}{p_i}\right]+\left[\frac{n}{p_i^2}\right]+\cdots\right)}.$$

Bevis. Antallet tall blandt $2, 3, \ldots, n$ som er delbare med p^k, men ikke med p^{k+1} er $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$ og disse tallene teller med k i $[2]_p + \cdots + [n]_p$. Vi får derfor at

$$\begin{aligned}
[n!]_p &= [2]_p + \cdots + [n]_p \\
&= \left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) \\
&\quad + 3\left(\left[\frac{n}{p^3}\right] - \left[\frac{n}{p^4}\right]\right) + \cdots = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots .
\end{aligned}$$

Lemma 13. *Vi har at* $\log n! \sim n \log n$.

Bevis. Vi har at summen $\log n! = \log 2 + \log 3 + \cdots + \log n$ er trappen under integralet $\int_1^{n+1} \log t dt$. Vi får at $\log 2 + \log 3 + \cdots + \log n \leq \int_1^n \log t dt + \log(n+1) = n \log n + \log(n+1)$. På den andre siden har vi at $\log 2 + \log 3 + \cdots + \log n$ er trappen over $\int_1^n \log t dt$ så $n \log n \leq \log 2 + \log 3 + \cdots + \log n$. Vi har vist at

$$1 \leq \frac{\log n!}{n \log n} \leq 1 + \frac{\log(n+1)}{n \log n}.$$

Lemmaet følger nu av at $\frac{\log(n+1)}{n \log n} < \frac{2}{n}$.

Setning 14. *Vi har at*

$$\sum_{p_i \le x} \frac{\log p_i}{p_i} \sim \log x.$$

→ *Bevis.* Av Lemma 12 har vi at

$$\log n! = \sum_{p_i \le n} \left(\left[\frac{n}{p_i} \right] + \left[\frac{n}{p_i^2} \right] + \cdots \right) \log p_i .$$

Dette gir

$$\begin{aligned} \log n! &\le \sum_{p_i \le n} \frac{n}{p_i} \log p_i + \sum_{p_i \le n} \left(\frac{n}{p_i^2} + \frac{n}{p_i^3} + \cdots \right) \log p_i \\ &= \sum_{p_i \le n} \frac{n}{p_i} \log p_i + n \sum_{p_i \le n} \frac{\log p_i}{p_i(p_i - 1)}. \end{aligned}$$

→ Vi har at $\frac{1}{k-1} < \frac{3}{k}$ og av Lemma 10 vil vi ha $k \le 1/3k^{\frac{1}{2}}$ for store k. Derfor vil $\frac{\log k}{k(k-1)} < \frac{1}{k^{\frac{1}{2}}}$, for store k og sekvensen $\sum_{k=2}^{\infty} \frac{\log k}{k(k-1)}$ konvergerer. Derfor finnes det, for hvert $\varepsilon > 0$ et tall N slik at

$$\frac{\log n!}{n \log n} < \frac{\sum_{p_i \le n} \frac{\log p_i}{p_i}}{\log n} + \varepsilon,$$

for $n \ge N$.

Omvendt har vi at

$$\begin{aligned} \log n! &\ge \sum_{p_i \le n} \left[\frac{n}{p_i} \right] \log p_i \ge \sum_{p_i \le n} \left(\frac{n}{p_i} - 1 \right) \log p_i \\ &\ge \sum_{p_i \le n} \frac{n \log p_i}{p_i} - \pi(n) \log n. \end{aligned}$$

→ Av Proposisjon 4 har vi $\frac{\pi(n) \log n}{n \log n} < 2 \frac{n \log n}{(\log \log n)(n \log n)} = 2 \frac{1}{\log \log n}$. For hver $\varepsilon > 0$ kan vi derfor finne et N slik at

$$\frac{\log n!}{n \log n} > \frac{\sum_{p_i \le n} \frac{\log p_i}{p_i}}{\log n} - \varepsilon,$$

→ for $n \ge N$. Setningen følger nu av Lemma 13.

Heur. primt. I

Heuristisk bevis av primtallsatsen I. Anta at vi har en funksjon $W(x)$ som beskriver tettheten av primtallene. Det vil si at vi har omtrent $W(x_i)\Delta x_i$ primtall i et intervall Δx_i omkring x_i. Vi antar at denne funksjonen beskriver primtallene så bra at $\pi(x) \sim \int_{t=2}^{x} W(t)dt$ og at $\sum_{p_i \leq x} \frac{\log p_i}{p_i} \sim \int_{t=2}^{x} W(t)\frac{\log(t)}{t}dt$. Det følger av
→ Setning 14 at vi da har at

$$\log x \sim \int_{t=1}^{x} W(t)\frac{\log t}{t}dt.$$

Vi kan nu bestemme $W(x)$ eksplisitt. Setter vi

$$\log x = \int_{t=1}^{x} W(t)\frac{\log t}{t}dt$$

og deriverer får vi

$$\frac{1}{x} = W(x)\frac{\log x}{x},$$

det vil si $W(x) = \frac{1}{\log x}$. Derfor har vi

$$\pi(x) \sim \int_{2}^{x} W(t)dt = \int_{2}^{x} \frac{dt}{\log t},$$

som er primtallsatsen.

Heur. primt. II

Heuristisk bevis av primtallsatsen II. Vi skal gi et ennu mer tvilsomt argument for at primtallsatsen holder. La s_n være sannsynligheten for at tallet n er primtall. Denne sannsynligheten kan uttrykkes ved hjelp av sannsynligheten for at mindre tall er primtall ved å notere at et tall n er primtall om det ikke er delbart med noe mindre primtall, og at sannsynligheten for at n er delbar med *primtallet* m er produktet av sannsynligheten for at m er primtall og sannsynligheten for at tallet er delbart med m, det vil si $s_m\frac{1}{m}$. Sannsynligheten s_n for at n er et primtall er derfor lik produktet av sannsynlighetene for at det ikke er delbart med *primtallet* m for $m = 2, 3, \ldots, n-2$. Med andre ord, vi har at

$$s_n = \left(1 - \frac{s_2}{2}\right)\left(1 - \frac{s_3}{3}\right)\cdots\left(1 - \frac{s_{n-1}}{n-1}\right).$$

der $s_2 = 1$. Vi får derfor at

$$\frac{s_{n+1}}{s_n} = 1 - \frac{s_n}{n},$$

eller $\frac{1}{s_{n+1}} - \frac{1}{s_n} = \frac{1}{n}\frac{s_n}{s_{n+1}}$. Antar vi nu at kvotienten $\frac{s_{n+1}}{s_n}$ går mot 1 når n går mot uendelig får vi, for store n, omtrent

$$\frac{1}{s_{n+1}} - \frac{1}{s_n} = \frac{1}{n},$$

det vil si at

$$\frac{1}{s_n} - \frac{1}{s_2} = \frac{1}{2} + \cdots + \frac{1}{n},$$

→ med $s_2 = 1$. Det følger av Lemma 3 at vi har

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} \sim \log n.$$

Derfor får vi at

$$s_n \sim 1/\log n,$$

som vi ville vise.