HVA BøR GYMNASLæRERE VITE OM PRIMTALL?

Skövde

4. mai 2001

Innledning, referenser og matematikere.

Vi lever i en epoke da kunnskap er lavt vurdert. Vårt miljø invaderes av kunnskapskonsulenter og pedagoger. Kunnskapskonsulentene mener vi ikke behøver kunnskaper. Det rekker å vite hvor de finnes. Pedagogene mener at det ikke er kunnskapene som er viktige, men hvordan man formidler dem. Begge gruppene selger produkter de ikke eier, og som de knapt har sett.

Vi vet imidlertid at vi må beherske matematikk for å kunne lære utden, og at vi må forstå matematisk teori og tankegang for å han noen glede av matematikken. Det er derfor en fornøyelse å innlede disse matematikkdagene med et helt upedagogisk foredrag om primtall.

Det er mange grunner til at lærere på gymnaset bør kjenne til de viktigste resultatene om primtall.

* Stiduket at primtalle er et klassisk område av matematikken som er en del av vår kultur. metoder.
* Studiet av primtall er en førsteklasses illustrasjon av matematisk teori og tankegang.
* Teorien for primtall og problemer om primtall er inspirerende og er lett å forstå.
* Studiet av primtall er et levende område av matematikken med en mengde interessant problemer av alle vanskelighetsgrader.
* Primtallene forekommer i noen av de viktigste anvendelsene av matematikken, blandt annet i kodning og avkodning av nesten all elektronisk informasjon.

Jet håper materialet i denne forelesningen skal gi glede og matematisk selvsikkerhet, og at dere kan bruke det til å inspirere motiverte elever.

Materialet finnes på
`http://www.math.kth.se/~laksov/gymnaset`

Viggo Brun (1885-1978).
R.D. Carmichael
Eratosthenes fra Cyrene (276-∼194 f.Kr.)
Paul Erdös (1913-1996).
Euklid (∼ 300 f.Kr.)
Leonhard Euler (1707-1783).
Carl Friedrich Gauss (1777-1855).
Christian Goldbach (1690-1764)
Jacques Salomon Hadamard (1865-1963).
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-).

Referenser:

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.

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

Daniel Shanks, *Solved and unsolved problems in number theory. Third edition.* Chelsea Publishing Co., New York, 1985.

primtall

Eratosthenes sold

Eratosthenes sold.

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

En enkel metode for å finne alle primtall mindre eller lik et gitt tall n er Erathosthenes sold, som er oppkalt etter den greske matematikeren Eratosthenes. Skriv opp alle heltall fra 2 til n: $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, \ldots, n$. Det første tallet er primtallet 2. Stryk nå alle tallene større enn 2 som er delbare med 2. Vi får da $2, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20}, \ldots$. Det første tallet etter 2 som ikke er strøket er primtallet 3. Stryk nå alle tallene større enn 3 som er delbare med 3. Vi får $2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \ldots$. Det første tallet som ikke er strøket er primtallet 5. Vi stryker nå alle tallene større enn 5 som ikke er delbare med 5. Det første tallet etter $2, 3, 5$ som ikke er strøket er primtallet 7. fortsetter vi på denne måten blir de tallene som står igjen alle primtallene mindre eller lik n. Her ser vi resultatet av Eratosthenes sold når $n = 101$:

	2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	$\not{9}$	$\not{10}$
11	$\not{12}$	13	$\not{14}$	$\not{15}$	$\not{16}$	17	$\not{18}$	19	$\not{20}$
$\not{21}$	$\not{22}$	23	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	29	$\not{30}$
31	$\not{32}$	$\not{33}$	$\not{34}$	$\not{35}$	$\not{36}$	37	$\not{38}$	$\not{39}$	$\not{40}$
41	$\not{42}$	43	$\not{44}$	$\not{45}$	$\not{46}$	47	$\not{48}$	$\not{49}$	$\not{50}$
$\not{51}$	$\not{52}$	53	$\not{54}$	$\not{55}$	$\not{56}$	$\not{57}$	$\not{58}$	59	$\not{60}$
61	$\not{62}$	$\not{63}$	$\not{64}$	$\not{65}$	$\not{66}$	67	$\not{68}$	$\not{69}$	$\not{70}$
71	$\not{72}$	73	$\not{74}$	$\not{75}$	$\not{76}$	$\not{77}$	$\not{78}$	79	$\not{80}$
$\not{81}$	$\not{82}$	83	$\not{84}$	$\not{85}$	$\not{86}$	$\not{87}$	$\not{88}$	89	$\not{90}$
$\not{91}$	$\not{92}$	$\not{93}$	$\not{94}$	$\not{95}$	$\not{96}$	97	$\not{98}$	$\not{99}$	$\not{100}$
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

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

Oppgave: La elevene bruke Eratosthenes sold til å finne primtall. Hvor store primtall kan de finne med denne metoden? Kan de finne en bedre metode?

Eratosthenes sold sier lite om primtallene. For eksempel fremgår det ikke av metoden om det finnes uendelig mange primtall.

Euklids bevis

Euklids bevis for at det finnes uendelig mange primtall.

Vi skal nå presentere et bevis for at det finnes uendelig mange primtall som vi vet var kjent for den greske matematikeren Euklid.

Tallet 2 er et primtall. Vi danner tallet $2+1=3$. Vi vet at 3 er et primtall, men selv uten å vite dette kan vi si at 2 ikke kan dele $2+1$ fordi den da måtte dele 1. Nu danner vi tallet $2\cdot 3+1=7$. Vi vet at 7 er et primtall, men igjen kan vi uten å vite dette si at 2 og 3 ikke kan dele $2\cdot 3+1$ fordi de da måtte dele 1. Nu danner vi tallet $2\cdot 3\cdot 7+1=43$. Vi vet at 43 er et primtall, men uten å vite dette kan vi si at $2,3$ og 7 ikke kan dele $2\cdot 3\cdot 7+1$ fordi de da måtte dele 1. Nu danner vi tallet $2\cdot 3\cdot 7\cdot 43+1=1807$. Dette er ikke et primtall, men vi kan si at primtallene $2,3,7,43$ ikke kan dele $2\cdot 3\cdot 7\cdot 43+1$ fordi de da må dele 1. Vi har at $1807=13\cdot 139$ så det minste primtallet som deler 1807 er 13. Nu danner vi tallet $2\cdot 3\cdot 7\cdot 43\cdot 13+1=23479$. Uansett om dette er et primtall eller ikke vet vi at tallene $2,3,7,13,43$ ikke kan dele $2\cdot 3\cdot 7\cdot 13\cdot 43+1$. Derfor er det minste primtallet som deler 23479 forskjellig fra $2,3,7,13,43$. Vi kan fortsette denne prosessen og finner uendelig mange primtall.

Oppgave: La elevene bruke Euklids bevis for å finne primtall. Hvor store primtall kan de finne? Istedenfor å bruke det minste primtallet som deler hver nytt tall kan de bruke det største. Hvilke primtall finner de da?

Problem: Det er ikke kjent hvilke primtall vi får når vi bruker metoden ovenfor. Tar vi største primtall som deler hvert nytt tall vet vi ikke engang om primtallene vi får øker i størrelse. Vi kjenner til en rekke primtall som vi ikke kan få ved Euklids metode. Det er også ukjent om serien av tall $2\cdot 3\cdots p_n+1$, for $n=1,2,\ldots$ der n er det n'te primtallet inneholder uendelig mange primtall, eller om det inneholder uendelig mange sammensatte tall.

Mer formelt kan Euklids bevis formuleres:
Anta at det bare finnes et endelig antall primtall $p_1=2,p_2=3,\ldots,p_r$. Vi kan skrive $p_1p_2\cdots p_r+1$ som et produkt av primtall. Hvert av disse primtallene må være forskjellig fra $p_1,p_2,\ldots,p_r$ fordi de ellers måtte dele 1. Vi har derfor funnet minst et primtall som er forskjellig fra $p_1,p_2,\ldots,p_r$. Dette motsier antagelsen om at $p_1,p_2,\ldots,p_r$ er alle primtall. Det finnes derfor uendelig mange primtall.

Eulers bevis for at det finnes uendelig mange primtall.

Vi skal nu gi et annet bevis for at det finnes uendelig mange primtall som ble funnet av opplysningstidens store matematiker, Sveitseren Leonard Euler. Beviset kan synes mer komplisert, men

det er et av de mest betydningsfulle bevisene i matematikkens historie. Den antyder dype forbindelser mellom **tallteorien og anlysen**, og leder frem til analytisk tallteori og det mest selebre av alle formodninger i matematikken *Riemanns hypotese*. Vi skal antyde hvordan analysen kommer inn og vise hvordan vi kan bruke Eulers metode til å få en ide om hvor mange primtall som finnes.

Euler

Vi kjenner alle til at

$$\frac{1}{1-\frac{1}{7}} = 1 + \frac{1}{7} + \frac{1}{7^2} + \cdots$$

der uttrykket $1 + \frac{1}{7} + \frac{1}{7^2} + \cdots$ betyr at den voksende følgen av tall $1,\ 1+\frac{1}{7},\ 1+\frac{1}{7}+\frac{1}{7^2}, \ldots$ nærmer seg tallet $\frac{1}{1-\frac{1}{7}}$.

Oppgave: La elevene generalisere og vise hva det betyr at tallfølgen $1, 1+a, 1+a+a^2, \ldots$ nærmer seg tallet $1/(1-a)$ når $0 \leq a < 1$. Be elevene generalisere og presisere hva det vil si at en tallfølge $a_0, a_0+a_1, a_0+a_1+a_2, \ldots$ nærmer seg et tall A for vilkårlige tall $a_0, a_1, a_2, \ldots$.

Vi har at

$$\begin{aligned}\frac{1}{1-\frac{1}{5}} \cdot \frac{1}{1-\frac{1}{7}} &= (1 + \frac{1}{5} + \frac{1}{5^2} + \cdots)(1 + \frac{1}{7} + \frac{1}{7^2} + \cdots) \\ &= 1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{5^2} + \frac{1}{5\cdot 7} + \frac{1}{7^2} + \cdots\end{aligned}$$

der uttrykket $1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{5^2} + \frac{1}{5\cdot 7} + \frac{1}{7^2} + \cdots$ betyr at den voksende følgen av tall $1,\ \frac{1}{5}+\frac{1}{7},\ \frac{1}{5^2}+\frac{1}{5\cdot 7}+\frac{1}{7^2},\ \frac{1}{5^3}+\frac{1}{5^2\cdot 7}+\frac{1}{5\cdot 7^2}+\frac{1}{7^3}, \cdots$ nærmer seg tallet $\frac{1}{1-\frac{1}{5}} \cdot \frac{1}{1-\frac{1}{7}}$. Nevnerne $5, 7, 5^2, 5\cdot 7, 7^2, \ldots$ består av alle positive heltall som bare er delbare med primtallene 5 og 7.

Oppgave: La elevene vise at om $A = a_0 + a_1 + a_2 + \cdots$ og $B = b_0 + b_1 + b_2 + \cdots$ og $a_0, a_1, a_2, \ldots$ alle er positive, så vil $AB = c_0 + c_1 + c_2 + \cdots$ der $c_n = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n$.

Vi kan selvsagt generalisere det vi har gjort ovenfor til et endelig antall primtall $p_1, p_2, \ldots, p_r$ slik at

$$\begin{aligned}&\frac{1}{\left(1-\frac{1}{p_1}\right)} \cdot \frac{1}{\left(1-\frac{1}{p_2}\right)} \cdots \frac{1}{\left(1-\frac{1}{p_r}\right)} \\ &= \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right)\cdots \\ &\left(1 + \frac{1}{p_r} + \frac{1}{p_r^2} + \cdots\right) \\ &= 1 + \frac{1}{p_1} + \frac{1}{p_2} \cdots + \frac{1}{p_r} + \frac{1}{p_1^2} + \frac{1}{p_1 p_2} + \cdots + \frac{1}{p_r^2} + \cdots \qquad (*)\end{aligned}$$

der nevnerne $p_1, p_2, \ldots, p_r, p_1^2, p_1 \cdot p_2, \ldots, p_n^2, \ldots$ er alle positive heltall som bare er delbare med primtallene $p_1, p_2, \ldots, p_r$. Skulle derfor $p_1, p_2, \ldots, p_r$ være alle primtallene fille nevnerne være alle tall $2, 3, 4, 5, \ldots$. Vi ville da ha at produktet $\frac{1}{1-\frac{1}{p_1}} \cdot \frac{1}{1-\frac{1}{p_2}} \cdots \frac{1}{1-\frac{1}{p_r}}$ i $(*)$ er lik summen $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots$. Men den siste summen er den harmoniske rekken som divergerer. Den kan derfor ikke være lik det endelige produktet. Derfor kan $p_1, p_2, \ldots, p_r$ være alle primtall og vi har få et nytt bevis for at det finnes uendelig mange primtall.

Eulers bevis

Mer formelt kan vi formulere Eulers bevis for at det finnes uendelig mange primtall som:
Anta at det bare finnes et endelig antall primtall $p_1 = 2, p_2 = 3, \ldots, p_r$. Da vil termene $\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_r}, \frac{1}{p_1^2}, \frac{1}{p_1 p_2}, \ldots, \frac{1}{p_r^2}, \ldots$, som forekommer sist i $(*)$ være de inverse til alle tallene $2, 3, 4, \ldots$. Derfor vil tallet $\frac{1}{1-\frac{1}{p_1}} \cdot \frac{1}{1-\frac{1}{p_2}} \cdots \frac{1}{1-\frac{1}{p_r}}$ være summen av tallene $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$. Vi vet imidlertid at summene $1, 1+\frac{1}{2}, 1+\frac{1}{2}+\frac{1}{3}, \ldots$ går mot uendelig når vi tar med flere termer, med andre ord den *harmoniske serien* $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$ divergerer. Dette er umulig så antagelsen om at det bare finnes et endelig antall primtall er feil. Det finnes altså et uendelig antall primtall.

Oppgave: La elevene vise at $1, 1+\frac{1}{2}, 1+\frac{1}{2}+\frac{1}{3}, \ldots$ går mot uendelig ved å vise at $\frac{1}{2}+\frac{1}{3}+\frac{1}{4} \geq \frac{1}{2}+\frac{2}{4} = 1$, $\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{8} \geq 1+\frac{4}{8} \geq \frac{3}{4}, \ldots$.

Forbindelser med analysen.

Fra analysen vet vi at vi kan definere den naturlige logaritmen $\log(x)$ til et positivt tall x ved integralet

$$\log(x) = \int_1^x \frac{1}{t}\, dt.$$

For hver tall t slik at $i \leq t \leq i+1$ har vi at $\frac{1}{t} \leq \frac{1}{i}$, så $\int_i^{i+1} \frac{1}{t}\, dt \leq \frac{1}{i}\int_i^{i+1} dt = \frac{1}{i}$. Om $n \leq x < n+1$ har vi derfor at

$$\begin{aligned} \log(x) = \int_1^x \frac{1}{t}\, dt &= \int_1^2 \frac{1}{t}\, dt + \int_2^3 \frac{1}{t}\, dt + \cdots + \int_n^x \frac{1}{t}\, dt \\ &= 1 + \frac{1}{2} + \cdots + \frac{1}{n}. \end{aligned} \tag{1}$$

Det er klart at tallene $2, 3, \ldots, n$ befinner seg blandt de tallene som bare er delbare med de primtallene $p_1, p_2, \ldots, p_r$ som er mindre

eller lik n. Derfor har vi at om $n \leq x < n+1$ så vil

$$\log(x) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \frac{1}{1-\frac{1}{p_1}} \cdot \frac{1}{1-\frac{1}{p_2}} \cdots \frac{1}{1-\frac{1}{p_r}} = \prod_{p_i \leq x} \frac{1}{1-\frac{1}{p_i}}. \quad (2)$$

Oppgave: La elevene vise at $\log(xy) = \log(x) + \log(y)$ for $0 < x, y$ når de bruker definisjonen ovenfor, ved å bruke likheten $\int_1^{xy} \frac{1}{t}\,dt = \int_1^x \frac{1}{t}\,dt + \int_x^{xy} \frac{1}{t}\,dt$ og bruke variabelsubstitusjonen $t = xu$.

Av (1) og (2) får vi at

$$\log(x) \leq \prod_{p_i \leq x} \frac{1}{1-\frac{1}{p_i}}. \quad (3)$$

Fra analysen vet vi også at når $0 \leq x \leq \frac{1}{2}$ så vil

$$-\log(1-x) \leq 2x. \quad (4)$$

Oppgave: La eleven vise at når $0 \leq x \leq \frac{1}{2}$ så vil $-\log(1-x) \leq 2x$ ved å vise at funksjonen $2x + \log(1-x)$ er 0 for $x = 0$ og har positiv derviert for $0 \leq x < \frac{1}{2}$.

Setning: *For hvert positivt tall x vil summen av den inverse $\frac{1}{p_i}$ av alle primtall p_i mindre eller lik x være minst lik $\frac{1}{2}\log(\log(x))$. Det vil si:*

$$\frac{1}{2}\log(\log(x)) < 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p_r}$$

når $p_r \leq x < p_{r+1}$.

Bevis. Vi bruker (4) med $x = \frac{1}{p_i}$ og får at

$$\sum_{p_i \leq x} \frac{1}{p_i} = 2 \sum_{p_i \leq x} \frac{2}{p_i} \geq -2 \sum_{p_i \leq x} \log(1 - \frac{1}{p_i}).$$

Bruker vi nu (3) får vi også at

$$-\sum_{p_i \leq x} \log(1 - \frac{1}{p_i}) = \log(\prod_{p_i \leq x} \frac{1}{1-\frac{1}{p_i}}) \geq \log(\log(x)).$$

Derfor er $\sum_{p_i \leq x} \frac{1}{p_i} \geq 2\log(\log(x))$ som vi skulle vise.

Det følger av Setningen at summen tallfølgen $\frac{1}{2}, \frac{1}{2}+\frac{1}{3}, \frac{1}{2}+\frac{1}{3}+\frac{1}{5}, \ldots$ av summene av de inverse av primtallene vokser mot uendeligheten når vi tar med tilstrekkelig mange ledd. Vi sier at rekken

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\cdots$$

av de inverse til alle primtallene divergerer. Vi kan til og med si noe om hvor fort følgen av tall $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \ldots$ av de inverse av primtallene går mot uendelig. Dette gir en mer presis formulering av Eulers bevis for at det finnes uendelig mange primtall. Sammelikner vi med serien

Primtallsum

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots$$

som konvergerer, og den harmoniske serien $1+\frac{1}{2}+\frac{1}{3}+\cdots$ som divergerer kan vi litt løst si at det finnes flere primtall enn kvadrattall, og nesten like mange primtall som det finnes hele tall.

Oppgave: Vis at $1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots$ konvererer ved å bruke ulikhetene $1+\frac{1}{2^2}+\frac{1}{3^2} \leq 1+\frac{2}{2^2}=1+\frac{1}{2}, 1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\frac{1}{7^2}+\frac{1}{8^2} \leq 1+\frac{1}{2}+\frac{4}{4^2}=1+\frac{1}{2}+\frac{1}{2^2}, \ldots$.

Primtallstvillinger og Goldbachs hypotese:. Kikker vi på den lille tabellen over primtall mindre eller lik 101 så ser vi at det finnes forbausende mange par av primtall $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$ som ligger så nær hverandre som det er mulig for odde primtall, det vil si med avstanden 2.

Tvillinger

Formodning: Det finnes uendelig mange primtallstvillinger.

Den norske matematikeren Viggo Brun viste i 1946 at sekvensen $\frac{1}{3}+\frac{1}{5}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\cdots$ av de inverse av primtallstvillingene konvererer. Det vil si at selvom det finnes uendelig mange primtallstvillinger finnes det langt færre primtallstvillinger enn det finnes primtall. Brun brukte soldmetoder som senere har vist seg å være blandt de mest nyttige i tallteorien. Tallet som serien av de inverse av primtallstvillingene konvergerer mot er på formen $B = 1.90216054\cdots$, som kalles *Bruns konstant*

Oppgave: La elevene finne så mange primtallstvillinger som mulig, og test hvor nære de kan komme Bruns konstant.

Den formodningen som sannsynligvis er den mest kjente om primtall er *Goldbachs hypotese*. I et brev til Euler i 1742 skrev

Goldbach

Godlbach at han trodde at alle heltall minst lik 6 kan skrives som en sum av 3 primtall. Euler omformulerte dette som:
Goldbachs hypotese: Hvert like tall kan skrives som en sum av to primtall.

Eksempel: Vi har at $4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5 = 3 + 7, 12 = 5 + 7, 14 = 7 + 7 = 3 + 11, \ldots$.

Oppgave: Se hvor langt elevene kan verifisere Goldbachs hypotese.

Fermats Lille Sats.

En av de resultatene som forekommer oftest i anvendelser av matematikken er *Fermats Lille Sats*. Nesten all elektronisk informasjon som sendes over nettet og som ikke skal være alment tilgjengelig kodes og avkodes ved hjelp av dette resultatet. For eksempel er all kommunikasjon mellom en bankomat og banken kodet ved hjelp av Fermats Lille Sats. For å konstruere bra koder er det nødvendig å finne store primtall. Dette gjør man også ved hjelp av dette resultatet.

For å forstå og sette pris på Fermats Lille Sats er det bra å kjenne til modulregning. Modulregning brukes over alt i matematikken og bygger på begrepet *ekvivalens* som er fundamentalt i matematikken. Notasjonen ble innført av Carl Friedrich Gauss i hans fundamentale verk *Disquisitiones Arithmeticae* som ble publisert i 1801. Den kan virke ganske klumpete, men gir i virkeligheten essensen i modulregningen og er uhyre brukbart og elegant.

Modulregning

Fikser et tall n. Har vi to hele tall a og b betyr notasjonen

$$a \equiv b \pmod{n}$$

at tallet n deler differensen $a - b$. Vi sier at a er *kongruent med* b *modulo* n. For eksempel, om $n = 7$ har vi at $9 \equiv 2 \pmod 7, 32 \equiv 4 \pmod 7, 39 \equiv 11 \pmod 7$.

Oppgave: Vis at $\equiv$ er en ekvivalens i betydelsen at (i) (Refleksivitet) $a \equiv a \pmod n$. (ii) (Symmetri) Om $a \equiv b \pmod n$ så vil $b \equiv a \pmod n$. (iii) (Transitivitet) Om $a \equiv b \pmod n$ og $b \equiv c \pmod n$ så vil $a \equiv c \pmod n$.

Det fine med kongruenser er at vi kan regne med dem på en lignende måte som vi regner med vanlige tall. For eksempel har vi regnereglene:

$$\text{Om } a \equiv b \pmod n \text{ og } c \equiv d \pmod n \text{ så vil}$$
$$a + c \equiv b + d \pmod n \text{ og } ac \equiv bd \pmod n.$$

Oppgave: La elevene verifisere regnereglene ovenfor for modulregning.

Alle tall a er kongruente med et av tallene $0, 1, 2, \ldots, n-1$ modulo n fordi *ufullstendig divisjon* av a med n gir at $a = qn + r$ der q og r er hele tall og $0 \leq r < n - 1$. For eksempel om $n = 7$ så vil $37 = 5 \cdot 7 + 3$ så $37 \equiv 3 \pmod 7$ og $453 = 64 \cdot 7 + 5$ så $453 \equiv 5 \pmod 7$. Dette gjør at vi bare behøver å regne med tallene $0, 1, 2, \ldots, n-1$. Datamaskiner, som bare har et begrensent antall prosessorer og et begrenset minne, og derfor alltid regner d modulo et meget stort tall n. Vi illustrerer hvor hendig det er å kunne regne med tallene modulo n ved å avgjøre om tallet 5^{323} er delbart med 7. Tallet 5^{323} er altfor stort til å kunne regnes ut, og selvom vi kunne regne det ut skulle det ikke finnes plass nok i universet til å skrive det ned. Imidlertid er $5 \equiv -2 \pmod 7$, og derfor $5^3 \equiv -8 \equiv -1 \pmod 7$. Derfor får vi $5^{323} \equiv 5^{3 \cdot 107+2} \equiv (5^3)^{107} \cdot 5^2 \equiv (-1)^{107} \cdot 4 \equiv -4 =\equiv 3 \pmod 7$. Derfor ser vi at 5^{323} ikke er delbar med 7 uten å regne ut 5^{323} og bare ved å bruke tallene $0, 1, 2, 3, 4, 5, 6$ og renge modulo 7.

Fermats Lille

Fermats Lille Sats: La p være et primtall. Om a er et tall som ikke er delbart med p vil

$$a^{p-1} \equiv 1 \pmod p.$$

Bevis. Om i og j er blandt tallene $1, 2, \ldots, p-1$ og $ia \equiv ja \pmod p$ må $i = j$ fordi da vil p dele $ia - ja = (i - j)a$, og ettersom p ikke deler a ved antagelsen i satsen må p dele $i - j$. Men $0 \leq i - j < p$ om $i > j$ og $0 \leq j - i < p$ om $j > i$ så vi må ha at $i = j$ om p deler $i - j$. Ettersom $ia \equiv ja \pmod p$ medfører at $i = j$ om $0 < i, j < p$ så må tallene $a, 2a, \ldots, (p-1)a$ modulo p være like tallene $1, 2, \ldots, p-1$ i noen rekkefølge. Derfor vil $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod p$. Med andre ord vil p dele tallet $(2 \cdot 3 \cdots (p-1))(a^{p-1} - 1)$. Men p kan ikke dele $2 \cdot 3 \cdots (p-1)$ ettersom $2, 3, \ldots, p-1$ er mindre enn p. Derfor må p dele $a^{p-1} - 1$, det vil si $a^{p-1} \equiv 1 \pmod p$.

Eksempel: Om $p = 7$ har vi: $1^6 \equiv 1 \pmod 7, 2^6 \equiv (2^3)^2 \equiv 1^2 \equiv 1 \pmod 7, 3^6 \equiv (3^2)^3 \equiv 2^3 \equiv 1 \pmod 7, 4^6 \equiv (-3)^6 \equiv 3^6 \equiv 1 \pmod 7, 5^6 \equiv (-2)^6 \equiv 2^6 \equiv 1 \pmod 7, 6^6 \equiv (-1)^6 \equiv 1 \pmod 7$.

Vi behøver bare å kontrollere at Fermats Lille Sats holder for tallene $1, 2, \ldots, 6$ fordi alle andre tall a er kongruent med et av disse tallene modulo 7. På samme måte behøver vi bare å kontrollere Fermats Lille Sats for tallene $1, 2, \ldots, p-1$.

Oppgave: La elevene teste Fermats Lille Sats for endel av de primtallene de har funnet.

En interessant egenskap ved Fermats Lille Sats er at den *nesten* karakteriserer primtallene i den bemerkelsen at:
Om n er et positivt heltall og

$$a^{n-1} \equiv 1 \pmod{n}$$

for alle tall a som er primiske med n så er n *nesten alltid* et primtall. *Nesten alltid* betyr at det er meget få tall n som ikke er primtall og som har egenskapen at $a^{n-1} \equiv 1 \pmod{n}$ for alle tall a som er primiske med n. Unntakene kalles *Carmichael tall*. Det første Carmichael tallet er 561, og det er så få av dem at det ikke var før i 1974 at det ble vist at det finnes uendelig mange slike tall.

Carmichael tall

Oppgave: La elevene teste om $a^{n-1} \equiv 1 \pmod{n}$ for alle tall a som er primiske med n. Se om de kan finne noen Carmichael tall.

Ettersom det er lett å teste om $a^{n-1} \equiv 1 \pmod{n}$ for alle tall a som er primiske med n får vi en lett måte for å teste om et tall, med stor sannsynlighet, er et primtall.

Primtallsatsen.

En annen måte å måle antallet primtall på, enn ved å ta summen av de inverse av primtallene, er å betrakte antallet primtall $\pi(x)$ mindre eller lik et gitt tall x. Vi har $\pi(2) = 1, \pi(3) = 2, \pi(4) = 2, \pi(5) = 3, \pi(6) = 3, \pi(7) = 4, \pi(8) = 4, \pi(9) = 4, \pi(10) = 4, \pi(11) = 5, \ldots, \pi(101) = 26$. 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

$\pi(x)$

$$\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}.$$

Denne gjetningen kalles *primtallsatsen*.

Primtallsatsen

Ved å bruke L'Hospitals regel ser vi at $\mathrm{Li}(x) \sim \frac{x}{\log(x)}$ så vi kan uttrykke Gauss gjetning på den vanligere formen

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

Oppgave: L'Hospitals regel sier at om f og g er deriverbare funksjoner på et intervall (a, b) og $g'(x) \neq 0$, for alle $x \in (a, b)$,

der $-\infty \leq a < b \leq +\infty$, og om $\frac{f'(x)}{g'(x)} \to A$ og $g(x) \to +\infty$, når $x \to a$ så vil $\frac{f(x)}{g(x)} \to A$. La elevene bruke L'Hospitals regel med $f(x) = \mathrm{Li}(x)$ og $g(x) = \frac{x}{\log(x)}$, $a = 2$ og $b = +\infty$ for å vise at $\mathrm{Li}(x) \sim \frac{x}{\log(x)}$.

Oppgave: La elevene regne ut funksjonene $\pi(x)$ og $\frac{x}{\log(x)}$ for så store x som mulig. Stemmer funksjonene nonenlunde overens for store x?

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

Merk: Det er interessant at 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 $\pi(n) > \mathrm{Li}(n)$.

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.