Tallene

Halvor Aarnes, UiO, 2014. S.E.& O.

Innhold

Tallene 1
Rasjonale tall 3
Regneeksempler 3
Irrasjonale tall 5
Algebra, algebraiske- og transendentale tall 6
Mengdelære og kardinaltall 8
Brøk og brøkregning 10
Primtall 12
Riemanns zetafunksjon 18
Modulær matematikk - klokkearitmetikk 21
Kryptografering og store primtall 23
Dirichlets etafunksjon 24
Eulers phi-funksjon 25
Möbius-funksjon 29
Skrift og kryptografi 30
Slumptallsgeneratorer 35
Taxi-tall 36
Komplekse tall 37
Binære tall 51
Klassetall 55
Hyperkomplekse tall og kvaternioner 56
Mengdelære 59
Regneeksempler 60
Astronomi 60
Elektrisitet 64
Gravitasjon og akselleras jon 68
Hydrostatisk trykk 72
Radioaktivitet 72
Lyd og decibelskala 73

Richters skala 76

Tallene er abstrakte enheter og kan brukes til å beskrive mengder: 2 appelsiner, 2 bananer, 1½ brød.Tallene kan brukes til å telle eller å måle. Men tallene brukes også i andre sammenhenger som en kode i telefonnummer, bilnummer personnummer, serienummer, sikkerhetskoder, ISBN-nummer, produktnummer, bankkontonummer osv.Tallene bruker vil til å måle, telle, beregne og numrere. De **naturlige tallene** er telletallene 1,2,3,….
Aritmetikk – tall-lære, er læren om tallene og deres egenskaper.
Alle reelle tall har en plass på **tall-linjen**. Et tall er et punkt på **tall-linjen**. I hver sin ende av tall-linjen ligger henholdsvis pluss uendelig (+∞) og minus uendelig (-∞), men uendelig er ikke et eksakt tall.
Georg Cantor som innførte mengdelæren kunne vise at **uendelig** (∞) ikke er noen fast størrelse, det er forskjellige former for uendelig. Det betyr at uendelig ikke betyr det samme i alle sammenhenger, og alle uendelige mengder har nødvendigvis ikke samme antall elementer. Mengden av de reelle tallene er mer uendelig enn de naturlige tallene, det vil si det er flere reelle tall enn naturlige tall.Et liggende 8-tall, ∞, er symbolet for **uendelig**. Tallene eksisterer i en idéverden, men eksisterer tallene uten at vi tenker på dem ? Hva er sammenhengen mellom tallene og den virkelige verden ?

De **reelle tallene** ($\mathbb{R}$) inneholder undermengdene: de **naturlige tallene** (telletallene, heltallene, $\mathbb{Z}$) og **rasjonale tall** ($\mathbb{Q}$), brøkene m/n, er en kvotient med to helltall, teller m og nevner n, men hvor n er forskjellig fra null ($n \neq 0$). Hvis n = 1 omfatter de rasjonale tallene heltallene. Mellom de hele tallene ligger de rasjonale tallene.
De reelle tallene er en undergruppe av de komplekse tallene ($\mathbb{C}$), a + bi, hvor i er en imaginær enhet slik at $i^2 = -1$.

$$\mathbb{C} \subset \mathbb{R} \subset \mathbb{Q} \subset \mathbb{Z}$$

Rasjonale tall

Rasjonale tall ($\mathbb{Q}$) som uttrykker fraksjon eller forholdstall kan skrives som en **brøk** *a/b* eller *–a/b* , hvor *a* og *b* er naturlige tall, eller *a*=0, *a* er **teller** og *b* er **nevner** i brøken, men b må være forskjellig fra null. Hvis b=1, så ser man at de rasjonale tallene omfatter de naturlige tallene ($\mathbb{Z}$). Hvis vi har to rasjonale tall like ved siden av hverandre kan det finnes et uendelig antall rasjonale tall mellom dem. Rasjonale tall kan uttrykkes som både brøk og **desimaltall**, 4 = 4.00000, 3/4 = 0.750000, 1/3 = 0.33333...
Hinduene brukte 0 og tok i bruk de **negative tallene** for å kunne uttrykke debet og kredit. Tidligere trodde man ikke at det fantes tall som var mindre enn null og bruk av disse tallene ble overført til Europa med renessansen.

Hvis vi har et rettvinklet trekant hvor lengden av de to hosliggende sidene er lik 1 så blir lengden av hypotenusen *c* ifølge Pythagoras setning lik kvadratratoen av 2 ($\sqrt{2}$) fordi
$c^2 = 1^2 + 1^2$. Kvadratroten til 2 kan ikke uttrykkes som en brøk mellom to heltall og kalles et **irrasjonalt tall**. Kvadratroten av 3 ($\sqrt{3}$) er et annet eksempel på et irrasjonalt tall.

Regneeksempler

1.
Legenden og myten om sjakkbrettets oppfinnelse og betalingen som oppfinneren skulle ha var 1 riskorn på første rute, 2 riskorn på andre rute, 4 riskorn på tredje rute osv. Antall ris korn på rute *n* blir lik 2^{n-1}.
Sjakkbrettet har 8·8 = 64 ruter, og summen av antall korn blir :

$$18\,446\,744\,073\,709\,551\,615 \approx 1.844674 \cdot 10^{19}$$

$$2^{63} = 9\,223\,372\,036\,854\,775\,808 \approx 9.223372 \cdot 10^{18}$$

Prinsippet viser geometrisk vekst, og så mange hvetekorn var det umulig å oppdrive.

$$\sum_{n=0}^{63} 2^{63} = 2^0 + 2^1 + 2^2 + \ 2^3 + \cdots + 2^{63}$$

Det blir store tall på den første halvdelen av sjakkbrettet, men det er på den andre halvdelen av brettet hvor antallet stiger dramatisk og viser effekten av eksponentiell vekst. Hvis man antar massen til riskorn er 25 mg så vil bare antallet riskorn på siste ruten tilsvare 230584300921 tonn med ris. Sammenlign med verdensproduksjonen.

2.

1 mol karbon har masse 12 g og tilsvarer **Avogadros tall** med atomer er lik $6.0221409 \cdot 10^{23}$ atomer. Avogadros tall tilsvarer **1 mol** partikler. Hva blir massen til et karbonatom ?

$$\frac{12}{6.0221409 \cdot 10^{23}} = 1.992647 \cdot 10^{-23}\ g$$

3.

Lysfarten er 300000 km s^{-1}. Hvor langt går lyset i løpet av et år ?
Antall sekunder per år:

$$60 \cdot 60 \cdot 24 \cdot 365 = 31536000\ s$$

Dvs. $9.4608 \cdot 10^{12}$ km/år

4.

Landjorda er ca. $1.49 \cdot 10^8$ km^2. I 2011 vil Jordens befolkning være ca. 7 milliarder. Hvor mange mennesker blir dette per km^2 ?

$$\frac{7 \cdot 10^9}{1.49 \cdot 10^8} \approx 47$$

Dvs. ca. 47 mennesker per kvadratkilometer.
I Nederland bor det 501 mennesker per km^2, og i Singapore 7736.

5.

Vann (H_2O) har molekylvekt 18. Ett mol vann tilsvarer 18 g. Hva er massen til et vannmolekyl ?

$$\frac{18}{6.0221409 \cdot 10^{23}} = 2.98897 \cdot 10^{-23}\ g$$

Irrasjonale tall

Tallet pi (π) er lik forholdstallet mellom omkrets og diameter i en sirkel og er et irrasjonalt tall, i tillegg er π et transcendalt tall.
For tallene kvadratroten av 2, pi (π), konstanten i det gyldne snitt, tau (τ), og det naturlige tallet e er det ikke noe mønster i tallene, *ad infinitum*

$$\sqrt{2} = 2^{\frac{1}{2}} = 1.414213562373095\ ...$$
$$\pi = 3.1415926535\ ...$$
$$\tau = \frac{1+\sqrt{5}}{2} = 1.6180339887\ ...$$
$$e = 2.718282818284590\ ...$$

Dette er eksempler på **irrasjonale tall**,som ikke kan skrives som brøk av to heltall. Når irrasjonale skrives som desimaltall er det et uendelig antall desimaler som ikke har noe periodisk mønster.
Hvis vi har et rettvinklet trekant hvor lengden av de to hosliggende sidene er lik 1 så blir lengden av hypotenusen *c* ifølge Pythagoras setning lik kvadratroten av 2 ($\sqrt{2}$) fordi $c^2 = 1^2 + 1^2$. Kvadratroten av 3 ($\sqrt{3}$) er et annet eksempel på et irrasjonalt tall. Kvadratroten av 2 er **irrasjonalt**, men ikke transcendentalt fordi det er en løsning av ligningen

$$x^2 - 2 = 0$$

Det betyr at kvadratroten til 2 kan ikke uttrykkes som en brøk.

Kvadratroten til 2 er lik lengden til hypotenusen i en rettvinklet trekant med sidelengde av hosliggende katater lik 1. Også lik lengden av diagonalen i et kvadrat med sidelengde lik 1. Eksempler på noen approksimasjoner for verdien til kvadratroten av 2:

$$\frac{99}{70} = 1.414286..$$

$$\frac{577}{408} = 1.414216..$$

$$\frac{665857}{470832} = 1.414214..$$

Kvadratroten til 3 er irrasjonalt også kalt Theodorus konstant, og er lik lengden mellom parallelle sider i en likesidet sekskant med lengde 1.

$$\sqrt{3} = 1.732051$$

Kvadratroten av 5 er også irrasjonalt, og inngår i konstanten i det gyldne snitt.
Ethvert positivt tall har to kvadratrøtter, en positiv og en negativ.
Det naturlige tallet *e* er lik grunntallet i naturlige logaritmer. Euler viste at både e og e^2 er irrasjonale tall.

Algebra, algebraiske- og transendentale tall

Innen algebra benyttes bokstaver. Ofte brukes de greske bokstavene:

Stor	Liten	Navn	Stor	Liten	Navn
A	α	Alfa	N	ν	Nu
B	β	Beta	Ξ	ξ	Xi
Γ	γ	Gamma	O	ο	Omikron
Δ	δ	Delta	Π	π	Pi
E	ε	Epsilon	P	ρ	Rho
Z	ζ	Zeta	Σ	σ	Sigma
H	η	Eta	T	τ	Tau
Θ	θ	Theta	Y	υ	Upsilon
I	ι	Iota	Φ	φ	Phi
K	κ	Kappa	X	χ	Chi
Λ	λ	Lambda	Ψ	ψ	Psi
M	μ	Mu	Ω	ω	Omega

Algebra på 1800-tallet besto i å løse ligninger. En algoritme er en trinn for trinn prosedyre med matematiske instruksjoner som fører fra startbetingelser til en slutt.
Algebraiske tall fås ved løsning av polynomet:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_o = 0$$

hvor $a_n,\ldots,a_0$ er heltall. Algebraiske tall er reelle tall som tilfredsstiller polynomligningen med rasjonale koeffisienter

Ifølge **fundamentalteoremet i algebra vil e**thvert polynom med reelle koeffisienter ha reelle eller komplekse røtter. Dette ble bevist av Carl Friedrich Gauss i *Disquisitiones aritmeticae*. (Undersøkelser av aritmetikk, 1801)

Johann Heinrich Lambert (1728-1778)hadde en konjektur (formodning) om at π og e er transendentale tall. Cherles Hermite (1822-1901) viste at e er transendeltalt og at π er transendeltalt ble vist av Lindemann.

Reelle tall som ikke er algebraiske kalles **transendentale tall**. Alle transendentale tall er irrasjonale, men ikke omvendt. Det finnes en uendelig mengde transcendentale tall. Eksempler på transendentale tall er pi (π) og det naturlige tallet *e*.

Det naturlige tallet e:

$$e = \sum_{n=1}^{\infty} \frac{1}{n!} = 2.7182818284 \ldots.$$

$$\frac{\pi}{4} = \operatorname{atan}(1) = \sum_{n=0}^{\infty} \frac{(-1)^n}{2 \cdot n + 1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = 0.7853982 \ldots$$

som også blir kalt Leibniz rekke.

$$\ln 2 = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ 0.6931472 \ldots$$

At π er et transcendentalt tall (har ikke rot i noen algebraisk ligning med rasjonale koeffisienter) betyr at **sirkelens kvadratur** er umulig. Det vil si at det er umulig å konstruere med passer og lineal et kvadrat som har samme flateinnhold som en sirkel.
Hvis vi lar radius r i sirkelen være lik 1 betyr dette (arealet av en sirkel er πr^2.

$$x^2 - \pi = 0 \qquad \rightarrow x = \sqrt{\pi}$$

Det samme gjelder de klassiske geometriske problemstillingene **vinkelens tredeling** og **kubens fordobling**, som også er umulige. Kubens fordobling vil si å finne sidekanten x i en kube som har dobbelt så stort volum som den første. Hvis vi lar sidekanten i den første kuben være lik 1 betyr dette å finne x i ligningen:

$$x^3 - 2 \cdot 1^3 = 0 \qquad \rightarrow \quad x = \sqrt[3]{2}$$

Mange har studert rekkefølgen av tallene i π, for å se om det finnes noe mønster i tallrekken, hvilket man ikke finner, det er en fullstendig tilfeldig sekvens. Tallene 0-9 forekommer med samme sannsynlighet 1/10. Det vil si at tar man hundre tall i pi bør ca. ti av dem være 6.
Den russiske matematikeren Aleksandr Gelfond (1906-1968) kunne vise at a^b er transcendentalt når a er algebraisk (a ≠ 0 & 1) og b er algebraisk og irrasjonalt. Det betyr at

$$2^{\sqrt{2}}$$

er transcendentalt (Gelfond-Schneiders konstant, eller Hilberts tall), 2.6651441426….

Gelfonds konstant 23.140692… er også transcendentalt:

$$e^{\pi} = \left(e^{i\pi}\right)^{-i} = (-1)^{-i}$$

Mengdelære og kardinaltall

Mengdelære er studie av en samling objekter med samme egenskaper. Begrepet mengde (menge) var tidligere blitt brukt brukt av Barnard Bolzano (1781-1848), gjenoppdaget av Cantor. Bolzano arbeidet med både logikk og mengdelære, og hans *Paradoxien des Enendlichen* (Paradokser i uendelighet) ble utgitt posthumt i 1851. cantor fant at det er ikke nødvendig å telle uendelige mengder med like mange elementer. Det holder med en regel om en **entydig avbilding**, for hvert element i den ene mengden er det tilordnet ett og bare ett i den andre mengden og vice versa. Hvis det finnes en entydig avbildning mellom to mengder så kalles de likemektige.Det finnes både tellbare og ikke-tellbare mengder.

De relle tallene er ikke-tellbare. To mengder har like mange elementer (er likemektige) hvis det finnes en **entydig avbildning** av den ene mengden over i den andre. Det er like mange partall og oddetall. Allerede Galieli Galilei viste at fra de naturlige tallene kan det lages en entydig avbildning som inneholder kvadrattallene.De naturlige tallene og kvadrattallene er **likemektige**. De naturlige tallene og kubikktallene er likemektige, for hvert telletall finnes det et kubikktall 1,8,27,64 Mengden av de reelle tallene er mer uendelig enn de naturlige tallene, det vil si det er flere reelle tall enn naturlige tall. Cantor viste dette ved at hvis det til ethvert naturlig tall korresponderte et reelt tall i et 1:1 forhold så vil det være plass til flere tall mellom de reelle tallene.

Transfinite kardinaltall er et begrep som ble innført av Cantor for å kunne beskrive uendelige mengder. **Kardinaltall** er lik antall elementer som inngår i mengden.
Antall elementer i en mengde, for eksempel mengden A, er lik **kardinaltallet** og utrykkes som alef A (א (A)), hvor alef א er den første bokstaven i det hebraiske alfabetet. Hvis mengden A er uendelig er א(A) et transfinit tall. $\aleph_0$, alef null, hvor alef er den første bokstaven i det hebraiske alfabet er et transfinit kardinaltall som angir en tellbar mengde. Mengden av de naturlige telletallene 1,2,3,…, er en **tellbar mengde**, og er således et transfinit kardinaltall. Ofte lar man 0 være med i de naturlige tallene (telletallene). De relle tallene og de irrasjonale tallene ikke tellbare mengder, mens de rasjonale tall (brøker, hvor teller og nevner er heltell, integer, …-3,-2,-1,0,1,2,3,…) er en tellbar mengde. Antall elementer i en mengde A blir $\aleph(A)$, og hvis mengden A er uendelig blir $\aleph(A)$ uendelig. Hvis to mengder A og B er likemektige blir $\aleph(A) = \aleph(B)$. Mengden som bare inneholder tallet 0 blir lik 1. $\aleph(\{0\}) = 1$.

Kontinuitetsproblemet sto på Hilberts liste fra den internasjonale matematikkkonferansen i Paris i år 1900.
Hilberts hotell:Et hotell har et uendelig antall rom, og det bor gjester på alle rommene. Om kvelden kommer et et par som vil ha rom. Dette ordnes ved at alle flyttes til neste rom slik at rom 1 blir ledig.Flere bl.a. Poincaré var skeptisk til Cantors mengdelære. Cantor var en av de mange som led av melankoli og følelsesmessige problemer og døde på et mentalsykehus.

Bertrand Russels paradoks: Mengden av alle mengder som ikke er et element i seg selv. Dette er en umulighet, på lignende vis som frisøren som klipper alle som ikke klipper seg selv, men hvem klipper frisøren ?

Absoluttverdien til et tall *x* er gitt ved |x|:

$$|x| = \begin{cases} x & hvis\ x \geq 0 \\ -x & hvis\ x < 0 \end{cases}$$

De vertikale linjene kalles **absoluttverdistolper**.

$$|-6| = 6$$

Vi har **signum-funksjonen** *sgn(x)* (l. *signum*-tegn)som viser om x er positiv eller negativ, men sgn(0) har ingen definisjon.

$$sgn(x) = \frac{x}{|x|} = \begin{cases} 1 & hvis\ x > 0 \\ -1 & hvis\ x < 0 \\ udefinert & hvis\ x = 0 \end{cases}$$

Mengdelæren er en del av matematikken. Mengder pleier å angis med store bokstaver og elementene i mengden er atskilt med komma inne i en klammeparentes. For eksempel mengden av ”øyne” eller prikker på en spillterning S={1,2,3,4,5,6}

Brøk og brøkregning

En **brøk** består av en **teller** over **brøkstreken** og en **nevner** under brøkstreken. En brøkstrek er det samme som et deletegn. Hvis telleren er større enn nevneren er brøken større enn 1 og kalles en **uekte brøk**.
Å **utvide brøken** vil si å multiplisere teller og nevner med samme tall.
Forkorte en brøk vil si når teller og nevner er faktorisert kan et likt tall i teller og nevner erstattes med tallet 1.
Hvis teller og nevner er like store blir brøken lik tallet 1.
Et **blandet tall** er sammensatt av et heltall og en brøk, 2½. En uekte brøk kan presenteres som et blandet tall. En brøk som har 0 (null) i teller

blir lik 0. Null i nevneren gir uendelig Et heltall *n* kan omgjøres til en brøk: 3= 3/1

En forutsetning for å addere (legge sammen) og subtrahere (trekke fra) brøker er at brøkene må ha **fellesnevner**. Fellenevner finnes ved å faktorisere alle nevnerne og finne en fellenevner kalt **minste felles multiplum**. Deretter utvides brøkene slik at de får fellesnevner og deretter kan de adderes eller subtraheres.

Å **faktorisere** et tall vil si å skrive et tall som produkt av to eller flere tall. Dette benyttes bl.a. ved forkorting av brøker. Tallet 15 kan faktoriseres som 3·5. Hvis alle faktorene er primtall kalles det **primtallfaktorisering**.

To brøker kan multipliseres med hverandre ved å gange (multiplisere) teller med teller og nevner med nevner. Vi kan multiplisere et heltall med en brøk ved å multiplisere heltallet med telleren og beholde nevneren. Når vi skal dividere (dele) to brøker med hverandre så snur vi den siste brøken (divisor) og multipliserer brøkene med hverandre.

En **potens** består av et **grunntall** og en **eksponent**. Vi får følgende lover for eksponenter og som tilfredsstiller eksponentialfunksjoner for a større enn null (a > 0):

$a^x \cdot a^y = a^{x+y}$	$0^x = 0$	$a^0 = 1$	$1^x = 1$
$(a \cdot c)^x = a^x \cdot c^x$	$a^{\frac{1}{x}} = \sqrt[x]{a}$	$a^{\frac{1}{2}} = \sqrt{a}$	$(a^x)^y = a^{x \cdot y}$
$\frac{1}{a^y} = a^{-y}$	$\frac{a^x}{a^y} = a^{x-y}$	$\left(\frac{a}{c}\right)^x = \frac{a^x}{c^x}$	$(a^x)^{\frac{1}{x}} = a$

Tabell over noen potenser hvor *x* og *y* er eksponenter, *a* er grunntall og *c* er en konstant. Potenser som flyttes fra teller til nevner, eller omvendt, skifter fortegn på eksponenten.

$$2^3 2^5 = 2^8 \qquad \frac{2^5}{2^3} = 2^{5-3} = 2^2 \qquad \left(\frac{3}{2}\right)^4 = \frac{3^4}{2^4} \qquad (2^2)^{-4} = 2^{-8}$$

Kvadratrot til et tall *x* er et tall *n* som ganget med seg selv gir x.

$$\sqrt{x} = \sqrt[2]{x} = \sqrt{n^2} = n$$

$\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$	$\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$	$a^{\frac{x}{y}} = \sqrt[y]{a^x} = \left(\sqrt[y]{x}\right)^x$

Kjenner vi arealet til et kvadrat kan vi finne siden i kvadratet ved å ta kvadratroten av arealet.

Primtall

Primtallene er tall som bare er delelig med seg selv og 1, og primtall kan ikke skrives som et produkt av to mindre tall. Primtallene er grunnsteinene i tallrekken. Multiplikasjon av primtall gir alle tall.
Primtallene som er mindre enn 50 er
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.
Bortsett fra det første tallet 2 som er partall er resten av primtallene oddetall. Den minste avstanden mellom to primtall er mellom 2 og 3.
1 defineres ikke som primtall, selv om det egentlig passer med definisjonen for et primtall. Hadde 1 vært definert som et primtall kunne vi ikke foretatt en entydig faktorisering av tall. Ethvert tall >1 er enten primtall eller ikke primtall. Sammensatte tall som 10, 15, og 18 kan faktoriseres som et produkt av mindre hele primtall. Ethvert sammensatt tall kan skrives som et produkt av primtall. 6 = 2·3, 18 = 2·9 = 2·3·3
Tall som ikke kan faktoriseres kalles primtall. Et naturlig tall >1 er et primtall hvis det ikke kan uttrykkes som et produkt av to mindre tall. Primtallene er byggesteiner for alle de naturlige tallene. Hvorfor er noen tall primtall, og andre ikke ?
Alle de naturlige tallene 1, 2, 3, osv. kan lages ved 1+1+1+1 osv. og neste tall er 1 større enn det foregående. Hvis vi har tallet 12 vet vi at 12=4·3 og 3 og 4 kalles **faktorer** av 12. Den unike mengden i produktet kalles primfaktor.
Tall som ikke kan faktoriseres kalles primtall. Et naturlig tall >1 er et primtall hvis det ikke kan uttrykkes som et produkt av to mindre tall. Primtall er bare delelig på seg selv og 1. Ethvert naturlig tall >1 er et primtall eller kan uttrykkes som et produkt av primtall. Primtallene er byggesteiner for alle de naturlige tallene. Alle de naturlige tallene 1, 2, 3, osv. kan lages ved 1+1+1+1 osv. og neste talle er 1 større enn det foregående. Hvis vi har tallet 12 vet vi at 12 = 4·3 og 3 og 4 kalles **faktorer** av 12. Vi har generelt for et tall *m* at *m* = *n*·*k* , hvor tallene *n* og

k (kvotient) er faktorene til m. Går ikke divisjonen opp blir det en rest som er mindre eller lik tallet vi deler på. For eksempel 16:5= 3 og en rest r=1.

Fundamentalteoremet i aritmetikk sier at ethvert positivt heltall n kan uttrykkes som et produkt av en unik samling av primtall p_1,p_2,p_3,… hvor a, b, c,… angir hvor mange ganger primtallet forekommer.

$$n = p_1^a \cdot p_2^b \cdot p_3^c \cdot \ldots$$

Delingsalgoritmen: Hvis *m* og *n* er naturlige tall så finnes det en unik *k* og *r* slik at:

$$m = n \cdot k + r \quad hvor \quad 0 \leq r \leq n - 1$$

De 200 første primtallene

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59
61 67 71 73 79 83 89 97 101 103 107 109 113 127 131
133 137 139 149 151 157 163 167 173 179 181 191 193 197
199 211 223 227 229 233 239 241 251 257 259 263 269 271
277 281 283 293 301 307 311 313 317 331 337 347 349 353
359 367 373 379 383 389 397 401 409 419 421 431 433 439
443 449 457 461 463 467 479 487 491 499 503 509 511 521
523 541 547 553 557 559 563 569 571 577 587 593 599 601
607 613 617 619 631 641 643 647 653 659 661 673 677 683
691 701 709 719 727 733 739 743 751 757 761 769 773 787
793 797 809 811 817 821 823 827 829 839 853 857 859 863
871 877 881 883 887 889 907 911 919 929 937 941 947 953
967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039
1049 1051 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123
1129

Gauss og Legendre fant at andelen av primtall blant de naturlige tallene fulgte forholdet *1/ln(n)*.
Jo større primtallene blir, desto sjeldnere forekommer de.

N	Antall primtall fra 1 opp til *N*
10	4
100	25

1000 (10^3)	168
10000 (10^4)	1229
10000 (10^5)	9592
1000000 (10^6)	75498
10000000 (10^7)	664579
100000000 (10^8)	5761455
1000000000 (10^9)	50847534
10000000000 (10^{10})	455052511
10^{11}	4118054813
10^{12}	37607912018
10^{13}	346065536839
10^{14}	3204941750802
10^{15}	29844570422669
10^{16}	279238341033925

Blant de første tallene forekommer primtallene oftere enn lenger ut i tallrekken. Hvordan er fordelingen av primtall utover i tallrekken ?
Gauss konjektur (formodning) gir en gjetning om antall primtall i form av et logaritmisk integral, og gjetningen blir mer og mer riktig ettersom *N* øker. Carl Gauss og den franske astronomen og matematikeren Adrien Marie Legendre (1752-1833) fant at andelen av primtall blant de naturlige tallene fulgte tilnærmet forholdet *n/ln(n)*. Primtallsteoremet ble bevist i 1896 av Jacques Hadamard og Charles-Jean de la Vallée Poussin.

Primtallesteoremet: Når n går mot uendelig ($n \to \infty$) blir antall primtall ≤ *n* lik

$$\frac{n}{\ln n}$$

Antall primtall *N* er ca. lik arealet under kurven *y=1/ln(x)* mellom *x*=2 og *x*=*N*, det logaritmiske integralet til *N*.
Antall primtall *N* kan bestemmes mer nøyaktig enn formelen ovenfor, og er ca. lik arealet under kurven *y=1/ln(x)* mellom *x*=2 og *x*=*N*, det **logaritmiske integralet** til *N*.

$$\int_2^n \frac{1}{lnx}\,dx$$

Tvillingprimtall (primtallstvillinger) er primtall med to påhverandre følgende primtall av oddetalltypen 3 og 5; 5 og 7; 11 og 13 osv. Finnes det uendelig mange slike par ? Den norske matematikeren Viggo Brun (1885-1978) arbeidet med denne problemstillingen. Antall primtallspar er proporsjonal med $x/(lnx)^2$ og for store x er antall primtallspar $<100x/(lnx)^2$. Hvis man tar den resiproke av primtalltvillinger og summerer dem får man en rekke som konvergerer mot **Bruns sum** 1.90216….

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\left(\frac{1}{41}+\frac{1}{43}\right)+\left(\frac{1}{59}+\frac{1}{61}\right)\ldots$$

De neste primtallsparene er 71-73, 101-103, 107-109, 137-139, 149-151, 179-181, 191-193 og 197-199. For x opp til 10^3 finnes 35 primtallspar, opp til 10^4 finnes 205 og opp til 10^5 finnes 1224 osv.

Gauss kunne vise den **kvadratiske resiprositetsloven**:

$$x^2 \; mod \; p = q$$

hvor både p og q er primtall.

Den franske presten Marin Mersenne (1588-1648) viste at 2^n-1 er primtall (**Mersenne primtall**), men gjelder ikke alle (kjenner til 32 unntak). 2^3-1=7 Man vet ikke om det finnes et uendelig antall Mersenneprimtall.
31, 331, 3331, 33331 osv. er primtall, men når man kommer til 333333331 så er ikke dette et primtall: 17·19607843 = 333333331
Goldbachs formodning (Christian Goldbach 1690-1764), i et brev til Euler i 1742, skrev at ethvert liketall større enn 2 kan skrives som summen av to primtall: 4=2+2; 6=3+3. For noen er det flere muligheter: 24=5+19=7+17=11+13.
Alle hele tall >5 kan skrives som summen av tre primtall.

Følgende formel gjelder for mange tilfeller, men ikke alle:
Hvis p_1, p_2 osv. er primtall så vil $p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$ være et primtall:
(2·3·5)+1= 31

Ethvert positivt tall >1 kan skrives som et produkt av to eller flere primtall. Den ungarske matematikeren Paul Erdös viste at det kan alltid finnes et

primtall mellom ethvert heltall *n* og *2n*, for eksempel mellom 2 og 4, 8 og 16 osv.
Primtall i *4n+1* familien er: 5,13,17,29,37,41,53,61,73,89,97
Primtall i *4n-1* familien er: 3,7,11,19,23,31,43,47,59,67,71,79,83
Alle tall av typen

$$2^{2^n}$$

er primtall (Fermats konjektur(formodning)).
Fermats lille sats (1640):
Hvis *p* er et primtall og *a* er et heltall så er a^p-*a* delelig med *p*.

Stanislaw M. Ulam (1909-1984) fant et spiralmønster i primtallene, Ulam spiral.
Astronomen, matematikeren og lederen av biblioteket i Alexandria Eratosthenes (276-195 f.kr.), også kjent for beregning av omkretsen av jorda, laget **Eratosthenes sil** som sier hvis n er et sammensatt tall så vil minst en av primfaktorene til n være mindre eller lik kvadratroten til n. denne silen er best egnet hvis det bare er to primfaktorer.
Matematikeren Edward Waring utviklet et teorem for å finne hva som er primtall, kalt **Wilsons teorem** (oppkalt etter hans venn matematikeren John Wilson 1741-1793):
p et primtall hvis og bare hvis (p-1)!+1 er delelig på *p*.
(p-1)! vil så å multiplisere alle tallene fra 1 til p-1
Eksempel p=7 gir (7—1)!=6!=6·5·4·3·2·1=720. Legg til 1 og vi ser at tallet er delelig på 7, altså er 7 et primtall.
Den franske matematikeren Joseph Bertrand (1822-1900) kunne i *Cacul de probabilités* (1845) finne en konjektur:
for n≥ 2 så finnes det minst ett primtall mellom *n* og *2n*.
Dette ble seinere bevist av den russiske matematikeren Pafnuti Lvovich Tchebychef (1821-1894).

For neste primtall p_{n+1} så vil dette alltid bli mindre enn 2 ganger det forrige primtallet p_n:

$$p_{n+1} < 2 \cdot p_n$$

Vi har også at summerer du to påfølgende primtall p_{n+1} og p_n så vil summen av dem p_{n+2} være større enn det neste primtallet:

$$p_n + p_{n+1} > p_{n+2}$$

Produktet at to primtall pm·pn vil alltid være større enn summen av dem:

$$p_m \cdot p_n > p_{m+n}$$

Euler oppdaget at funksjonen:

$$f(x) = x^2 + x + 41$$

genererer primtall for x=[0,39].

41 43 47 53 61 71 83 97 113 131 151 173 197 223 251
281 313 347 383 421 461 503 547 593 641 691 743 797 853
911 971 1033 1097 1163 1231 1301 1373 1447 1523 1601

Andre funksjoner som gir mange primtall er $f(x)=2x^2-199$; f(x)=6x+5 ; og f(x)=30x – 13.

Det er lett etter mange tester for å finne ut om et tall er et primtall eller ikke. Ender tallet >2 på 0,2,4,6 eller 8 er det ikke et primtall.
Med avanserte datamaskiner letes det etter de største primtallene.
Faktorisering av store primtall danner basis for kryptografi.

Det finnes uendelig mange primtall. Ifølge **Eulers formel** er:

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod \frac{1}{1 - \frac{1}{p}}$$

hvor *p* er primtall.
Ethvert positivt tall kan uttrykkes som et unikt produkt av primtall.
Leopold Kronecker (1823-1891) kunne videreutvikle denne for s > 1:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \frac{1}{1 - \frac{1}{p^s}}$$

Heltallsverdiene *s* kan uttrykkes som *zeta s* (ζ(s)) i **Eulers zetafunksjon** hvor det er en sammenheng rekken av alle de positive tallene og produktet av alle primtallene !

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = \left(\frac{1}{1-2^s}\right)\left(\frac{1}{1-3^s}\right)\left(\frac{1}{1-5^s}\right)\ldots$$

For s≤ 1 gir dette en uendelig sum som har et uendelig svar, men for s>1 har summen en endelig verdi.

Euler fant at for den konvergente ueneelig rekken $\zeta(2) = \pi^2/6$ og nok en gang dukker pi opp på et underlig sted.

$$\zeta(2) = \sum_{n=0}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$$

for $\zeta(4)=\pi^4/90$ blir det en konvergent uendelig rekke:

$$\zeta(4) = \sum_{n=0}^{\infty} \frac{1}{n^4} = 1 + \frac{1}{16} + \frac{1}{81} + \frac{1}{256} + \cdots = \frac{\pi^4}{90}$$

Riemanns zetafunksjon

Riemanns zetafunksjon har sitt utgangspunkt i Eulers formel (Eulers zetafunksjon), og uttrykker summen av inverse potenser av positive tall. Riemann utvider den til å omfatte de komplekse tallene. Riemanns zetafunksjon treffer man på i de underligste sammenhenger innen naturvitenskap. Bernhard Riemann studerte forskjellen mellom reelle og komplekse funksjoner. Hvis vi har to komplekse tall *z=x+iy* og *w=u+iv* så vil grensen for *dw/dz* være den deriverte akkurat som for de reelle tallene.

Heltallsverdiene *s* kan uttrykkes som *zeta s* (ζ(s)):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

Vi definerer Riemanns zeta-funksjon som:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Laurent-rekke utvidelse av zeta-funksjonen er:

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \gamma_n (s-1)^n$$

hvor **Stieltjes konstant** γ_n er lik:

$$\gamma_n = \lim_{m\to\infty} \left(\left(\sum_{k=1}^{m} \frac{(ln(k))^n}{k} \right) - \frac{(ln(m))^{n+1}}{n+1} \right)$$

En **Laurent-rekke** er en potensrekke for en kompleks funksjon f(z) og som inneholder med negative ledd.
Vi kan finne verdien for Stieltjes konstant ved forskjellige verdier av n. Hvis n=0 blir Stieltjes konstant lik Euler-Mascheroni-konstanten (gammakonstanten).

Euler fant at for $\zeta(2) = \pi^2/6$ og for $\zeta(4)=\pi^4/90$:

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$$

ζ(3)=1.202… (Apérys konstant.
Verdien av zetafunksjonen for reelle tall for s fra 0 til 4

s	ζ (s)
0	ζ (0) = -0.50000…
1	ζ (1) = ∞ (uendelig)
2	ζ (2) = 1.644934…
3	ζ (3) = 1.202057…
4	ζ (4) = 1.082323…

Det viser seg at Riemanns zetafunksjon er koblet til fordelingen av primtall (*Über de Anzahl der Primzahlen unter einer gegebener Grösse* (1859)). Primtallsteoremet kan utledes fra nullene i zetafunksjon hvor nullene i kompleksplanet ligger symmetrisk på en linje.
Riemann uttrykte ζ(s) i form av integraler, og viste at det gjaldt for hele kompleksplanet. Ifølge Riemann har alle komplekse null av ζ(s) en reell del lik ½.
Hvis *s* er et komplekst tall *s=a+bi*

så vil alle løsninger av ligningen nedenfor bli et komplekst tall hvor a=1/2

$$1-\frac{1}{2^s}+\frac{1}{3^s}-\frac{1}{4^s}+\frac{1}{5^s}-\cdots=0$$

Det vil si at alle løsningene blir liggende på en rett linje i kompleksplanet med a=1/2, avgrenset av [0,1] på den relle aksen, og altså parallell med den imaginære aksen. Noen av de første ikke-trivielle løsningene er 0.5+14.135i; 0.5+21.022i; 0.5+25.011; og 0.5+30.425i

Hva nå hvis vi setter s=-1 ?

$$\zeta(-1)=\sum_{n=0}^{\infty}\frac{1}{n^{-1}}=\frac{1}{1^{-1}}+\frac{1}{2^{-1}}+\frac{1}{3^{-1}}+\frac{1}{4^{-1}}+\cdots=1+2+3+\cdots=\infty$$

Vi får da en divergent rekke hvor summen blir stadig større etter hvert som *n* øker.
Riemann utvidet funksjonen til:

$$\zeta(s)=\frac{\prod(-s)}{2\pi i}\int_C\frac{(-x)^s}{e^x-1}\frac{dx}{x}$$

Den **funksjonelle ligning** av Riemanns zetafunksjon gjør det mulig å regne ut zetafunksjonen for s=-1:

$$\zeta(s)=2^s\pi^{s-1}sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s)$$

Hvis vi regner ut for ζ(-1):

$$\zeta(-1)=2^{-1}\pi^{-2}sin\left(\frac{-\pi}{2}\right)\Gamma(2)\zeta(2)\qquad\zeta(2)=\frac{\pi^2}{6}$$

Vi har nå vist at:

$$1+2+3+4+5+\cdots=-\frac{1}{12}=-0.0833333\ldots$$

Et helt ulogisk regnestykke, hva er det som skjer ?
Vi kan se at zeta-funksjonen blir lik 0 for flere negative verdier, for negative liketall:ζ(-2)=0, ζ(-4)=0,ζ(-6)=0 osv.
Disse kalles trivielle null.
Riemannfunksjonen *R(n)* gir et mye bedre estimat av antall primtall i tallrekken, enn det Euler, Legendre og Gauss hadde klart, som viste at et estimat antall primtall fulgte funksjonen:

$$antall\ primtall \approx \frac{n}{\ln(n)}$$

og fra Riemannfunksjonen et bedre estimat:

$$antall\ primtall = R(n) - \sum_{\rho}^{\infty} R(n^{\rho})$$

hvor rho (ρ) er ikke trivielle 0 på linjen $0.5+x_i$.

Andricias konjektur (Dorin Andricia) tar for seg avstanden mellom primtall, og viser at denne differansen er mindre enn 1

$$A = \sqrt{p_{n+1}} - \sqrt{p_n} < 1$$

hvor p_n er det n-te primtall. Den høyste verdien for A er ved n = 4, og lik 0.67087…

Den minste avstanden for de 100000 første primtallene er 0.0009579968 og dette skjer for primtall nr. 99998

Goldbachs binære konjektur (Christian Goldbach 1690-1764): ethvert liketall større enn 4 (>4) kan uttrykkes som en sum av to primtall: 4 = 2+2; 6 = 3 +3; 8=3+5, 10=3+7 og 5+5, 12=5+7, 14=3+11 og 7+7…
For noen av partallene er det flere måter å uttrykke summen. For 34 er det fire måter: 17+17, 11+23, 3+31, 5+29. Dette tallet, C(34)=4, kalles Goldbachs tall.
Goldbachs ternære konjektur: Ethvert oddetall >7 kan uttrykkes som en sum av tre primtall.

Modulær matematikk - klokkearitmetikk

Modulær matematikk kalles også klokkearitmetikk. En 12-timers klokke, deler døgnet inn i to 12-timers perioder og er et eksempel på aritmetikk modulo 12. Klokken er en ring med heltall, og 12 er kongruent med både 0 og 12. 0≡12 mod12
Hvis klokken er 6 og ønsker å vite hva klokken er 8 timer seinere er, 6+8=14, så vil klokken være 2

Dette er addisjon modulo 12 hvor en sirkel er delt i n like store deler, for en klokke er n=12. Modulo finner resten etter deling av et heltall med et annet
To tall a og b sies å være kongruent (≡, merk forskjell fra likhetstegnet =) modulo n

$$a \equiv b(mod\ n) \quad hvis\ a - b = kn$$

for et heltall k. a og b kan også være negative heltall.
Tallene 37 og 57 er kongruente(≡) modulo 10, begge med rest 7 når de deles på 10 og 37-57=-20 som er delelig på 10

Modulær multiplikativ invers til et heltall a modulo n er et heltall x slik at:

$$a^{-1} \equiv x(mod\ n)$$

Dette er ekvialent med :

$$ax \equiv aa^{-1} \equiv 1(mod\ n)$$

Hvis vi vil finne x for a=3 og n=11, så vil x=4

Kongruens modulo n er en **ekvivalensrelasjon** og **klasseinndeling** av heltallene Z. a og b er ekvivalente hvis differansen mellom dem er delelig med n.
Hvis a er et positivt så har vi følgende undergruppe av heltallene Z:

$$\{\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots\}$$

Det er flere eksempler på bruk av modulær matematikk i tillegg til Diffie-Hellman-Merkle og RSA kryptografi.
I IBAN-nummeret (International Bank Account Numbers) som bankene benytter brukes modulo 97 for å beregne kontrollsummen for å finne feil bruk av bankkontonummer.

CAS-nummeret som brukes til å identifisere alle kjemiske stoffer har et unikt sistesiffer for ethvert kjemikalium. Dette beregnes ved å ta siste siffer i de to første delene av CAS-nummeret ganger 1, neste siffer ganger 2, neste siffer ganger 3 osv, som til slutt brukes til å beregne sum modulo 10.
Modulo 7 for å finne ukedag i kalenderen. Modulo 12 i tolvtonemusikk. Modulo 2 i summering av bits, samt innen en rekke disipliner økonomi, sosialvitenskap, spillteori og lignende.

Kryptografering og store primtall

Enigma siffermaskinen som ble brukt under andre verdenskrig var en siffermaskin med 26 roterende hjul på samme akse, og på hvert hjul var det et stokket alfabet. Bokstaven E er den vanligste og blant annet polske matematikere bidro til å løse enigma-koden. Ved kryptografi kan bokstaver omdannes til tall (substitusjon) og tallene kan stokkes (transposisjon).

Innen kryptografi for å kode meldinger brukes to store primtall *p* og *q*, hvert av dem med >300 siffer. Produktet av disse to primtallene gir et tall *N* ($p \cdot q = N$) som er en offentlig kjent nøkkel (”public key”) som kan brukes til å kode meldinger, men kan ikke brukes til å dekode meldingene. De to store primtallene *p* og *q* er hemmelig for alle andre enn den som laget koden, og kan for sikkerhets skyld ødelegges straks nøkkelen er laget. Nøkkelen *N* baserer seg på at faktorisering av store primtall er nesten en umulig oppgave selv med de raskeste datamaskinene i verden.
Whitfield Diffie og Martin Hellman utviklet i 1976 en kryptograferingsteknikk (Diffie-Hellman nøkkelutveksling) basert på primtallsfaktorisering, offentlig nøkkel og privat nøkkel.
I 1977 kunne Ronald Rivest, Adi Shamir og Leonard Adleman utvikle ***RSA* koden** basert på store primtall.
I tillegg trenger man to tall *k* til koding og *d* til dekryptering(dekoding).
Tallene *k* og *d* bestemmes ut fra formelen:

$$\frac{(p-1)\cdot(q-1)}{k\cdot d-1}$$

Tallene *N* og *k* er offentlige nøkler og *N* og *d* er private nøkler (”private key”), og som nevnt er de store primtallene *p* og *q* hemmelige og kastes.
En bokstavmelding må først omformes til tall og det kan gjøres enkelt ved av A=01, B=02, C=03, D=04 osv. mellomrom=00.
Hvis man har en bokstavmelding M så vil
M^k/N gi en rest *C* som er lik den kodete meldingen:

$$C = M^k \ mod \ N$$

Tallet *d* brukes til dekryptering hvor man kommer tilbake til den opprinnelige meldingen ved:

$$C^d \ mod \ N \ = \ M$$

Vi benytter oss av **Fermats lille teorem**:
Hvis *p* er et primtall og *n* er et heltall som ikke har *p* som faktor så er

$$n^{p-1} = 1 \ mod \ p$$

slik at n^{p-1} vil alltid ha rest 1 når dividert på *p*.
For eksempel hvis vi velger 5 som et primtall og tar et tilfeldig tall som ikke har 5 som faktor for eksempel 7 så har vi:

Potenser av 7	Potens av 7 modulo 5
7^1 =7	2
7^2 =49	4
7^3 =343	3
7^4 =2401	1
7^5 =16807	2

Vi ser at 7^{5-1}= 1 mod 5, og 7^5=2 mod 5 er tilbake til utgangspunktet

Dirichlets etafunksjon

Dirichlets etafunksjon, eta(η), også kalt den alternerende zetafunksjon, er en Dirichletserie som konvergerer for alle komplekse tall med reell del >0

$$\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} = \frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

Andre fremstillinger av Dirichlets etafunksjon er, med zeta(s) ζ(s) eller med gamma

$$\eta(s) = (1 - 2^{1-s})\zeta(s)$$

$$\eta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x + 1} dx$$

Noen utvalgte verdier av Dirichlets etafunksjon

$$\eta(1) = ln2 \quad \eta(2) = \frac{\pi^2}{12} \quad \eta(4) = \frac{7\pi^4}{720} \quad \eta(6) = \frac{31\pi^6}{302402}$$

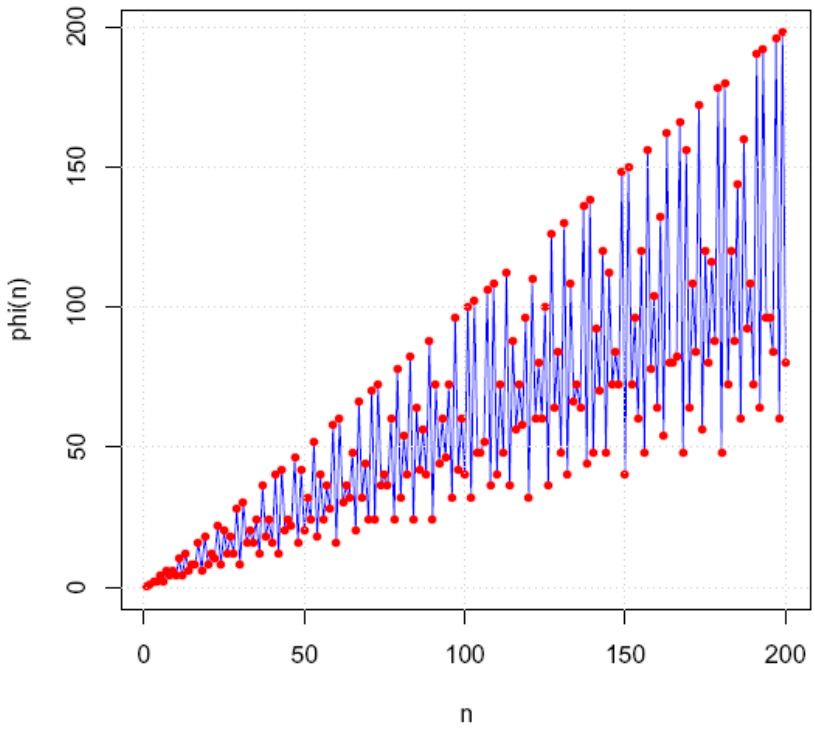
For et heltall k>1 og B_k er det k-te **Bernoulli-tall**

$$\eta(1-k) = \frac{2^k - 1}{k} B_k$$

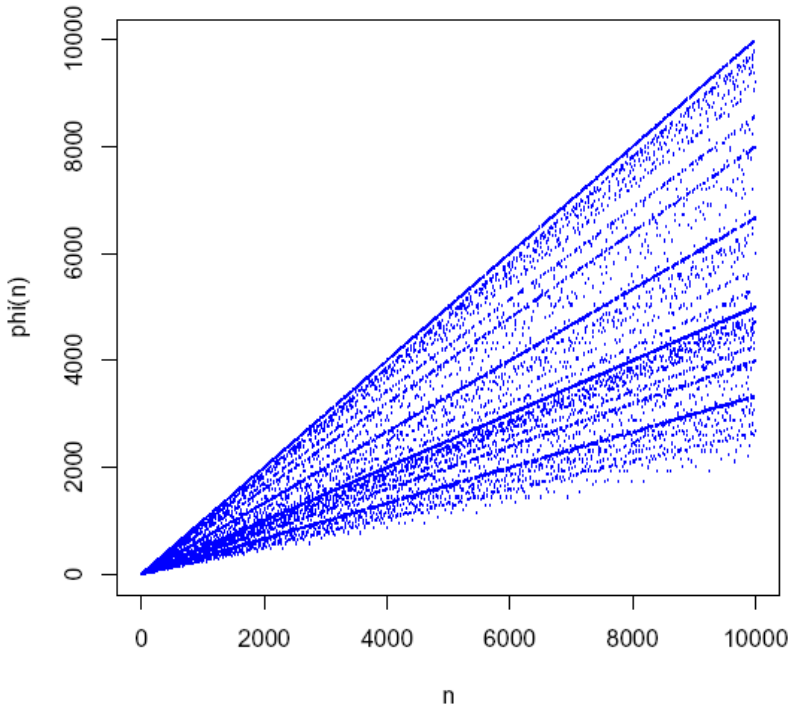
Eulers phi-funksjon

største felles divisor eller største felles faktor for to eller flere heltall, er det største tallet som deler tallene uten at det blir noen rest. Største felles divisor for a=8 og b=12 er lik 4. a og b kalles **koprimtall** hvis det eneste positive heltallet som deler begge av dem er lik 1. Det vil si at største felles divisor er lik 1. Antall heltall som er kprimtall til et positivt heltall n, mellom 1 og n, er gitt ved **Eulers phi-funksjon** φ(n), også kalt Eulers totient-funksjon. Phifunksjonen teller antall positive heltall mindre eller lik n som er relative primtall til n.

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$



Figur. Eulers phi-funksjon for n=0-200



Figur. Eulers phi-funksjon for n=0-10000.

Eulers phi-funksjon kan anvendes innen kryptografi. Man finner to ekstremt store primtall p og q, og renger ut n=pq og k=φ (n). Deretter finner man to tall e og d slik at $ed \equiv 1 \, mod \, k$

n og k er offentlige nøkler og d er privat dekrypteringsnøkkel.

Vi viser prinsippet for RSA med noen meget små primtall:

p=13 og q=17, samt k=7, n=187, φ(n)=160, d=23

Bokstaven A i ASCII tilsvarer desimaltall 65. Etter koding blir denne til tallet 91, tilsvarende venstre klammeparentes [i ASCII.

Skal man dechiffrere må man regne ut den private nøkkel d med Euklids algoritme

$$k \cdot d \equiv 1 \, (mod \, (p-1)(q-1))$$

Dvs. d=23

Vi kommer nå tilbake til M ved

$$M \equiv 11^{23} (mod \, 187)$$

Dette blir litt for store tall å hanskes med så vi kan bruke Kinesisk restteorem for å øke hastigheten for denne utregningen.

n	φ(n)	n	φ(n)	n	φ(n)	n	φ(n)	n	φ(n)
1	0	21	12	41	40	61	60	81	54
2	1	22	10	42	12	62	30	82	40
3	2	23	22	43	42	63	36	83	82

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

De 100 første φ(n)

φ(n) er multiplikativ så hvis to primtall m og n er relative primtall i forhold til hverandre så vil

$$gfd(m,n) = 1 \quad \rightarrow \ \varphi(mn) = \varphi(m)\varphi(n)$$

Flere egenskaper gjelder hvis a og b er koprimtall. Ikke noe primtall kan dele både a og b.
Det eksisterer heltall x og y slik at (Bézouts identitet)

$$ax + by = 1$$

Heltallet b er en multiplikativ invers modulo a, det vil si at det finnes et heltall y sli at

$$by \equiv 1(mod\ a)$$

Tallene a og b er koprimtall hvis og bare hvis 2^a-1 og 2^b-1 er koprimtall.
Hvis p er et primtall og k≥1 så:

$$\varphi(p)^k = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$$

Hvis vi har to heltall a og b, hva er sannsynligheten for at de er koprimtall ? Sannsynligheten for at et tall er delelig med et primtall p er lik 1/p, for eksempel er hvert 11te heltall delelig med 11. Sannsynligheten for at både a og b er delelig med et primtall blir $1/p^2$, og sannsynliheten for at

minst en av dem ikke er delelig med et primtall er $1-1/p^2$. Som produkt over alle primtall gir dette en ca. sannsynlighet 61%

$$\prod_p^{\infty}\left(1-\frac{1}{p^2}\right)=\left(\prod_p^{\infty}\left(1-\frac{1}{p^2}\right)\right)^{-1}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2}$$

Carmichaels lambdafunksjon λ(n) til et positivt heltall n er det minste positive heltallet m for hvert heltall a som er koprimtall til n:

$$a^m \equiv 1(mod\ n)$$

λ(n)= φ(n) hvis n=2,3,4,5,7,9,11,13,17,19,23,25…
λ(n)= ½ φ(n) hvis n=8,16,32,64,…

En **primtallstest** er en algoritme som avgjør om et tall sannsynligvis er et primtall eller ikke, testene gir vanligvis bare indikasjoner. Fermats primtallstest er en slik enkel test: gitt et heltall n, finn et heltalls koprimtall a og beregn
a^{n-1} (modulo n). Hvis dette blir lik 1, er det mulighet for at man har et primtall. a^{n-1} (modulo n)=1, men n ikke er et primtall så kalles n et pseudoprimtall med basis a.
Seinere fant man at Fermats lille teorem kan benyttes til primtallstesting. AKS primtallstesten er en polynomtid algoritme, type P.

Eksponentsiering ved kvadrering er en metode får å øke hastigheten når man har potenser med store heltall. Hvis n er et positivt heltall så gjelder, øverst for n er oddetall, nederst for n er liketall

$$x^n=\begin{cases} x(x^2)^{\frac{n-1}{2}} \\ (x^2)^{\frac{n}{2}} \end{cases}$$

Fermats lille teorem

For å teste om et tall er et primtall kan man bruke **Fermat´s lille teorem** som sier at hvis p er et primtall så vil a^p-a, hvor a er et heltall, være et heltallmultippel av p

$$a^p \equiv a(mod\ p)$$

Det sier også at hvis a ikke er delelig på p så tilsvarer dette at a^{p-1}-1 er et heltallmultippel av p:

$$a^{p-1} \equiv 1(mod\ p)$$

Et spesialtilfelle av Fermats lille teorem er at p er et primtall hvis og bare hvis

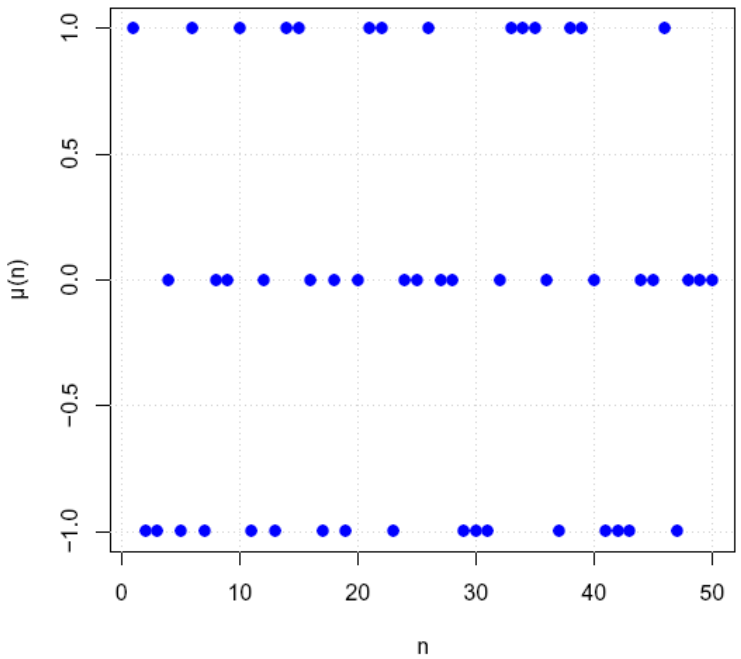
$$2^p \equiv 2(mod\ p)$$

En generalisering er Eulers teorem:

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

Möbius-funksjon

August Ferdinand Möbius (1790-1868), kjent for Möbiusbåndet i topologi, student hos Gauss, utviklet en Möbiusfunksjon *M(n)*:
M(n)=0 hvis et av primtallene i faktoriseringen av n har eksponenten 2 eller mer.
M(n)=1 hvis antall forskjellige primtall i faktoriseringen av n er et liketall
M(n)=-1 hvis antall forskjellige primtall i faktoriseringen av n er et oddetall.
M(0)=1;M(1)=1,M(2)=-1;M(4)=0;M(5)=-1;M(6)=1;M(7)=-1;M(8)=0;M(9)=0;M(10)=1
Det viser seg at Möbiusfunksjonen er relatert til den inverse av zetafunksjonen.



Figur. Möbius-funksjonen

Skrift og kryptografi

Selv om det ikke var skrevet i kode var de egyptiske hieroglyfene lenge en utfordring, var det lydskrift (fonogram) eller bildeskrift (piktogram,semagram) ? Thomas Young, kjent for oppdagelsen av lysets bølgenatur, gjorde noen innledende studier av innrammete hieroglyfer (kartusj), det var lydskrift, og Young kunne identifisere navn som Ptolemaios og Berenike.
Rosettasteinen fra 196 f.kr., med felles tekstinnskript i hieroglyfer, demotisk (en enklere og folkelig utgave av hieroglyfene) og gresk var et viktig hjelpemiddel. Imidlertid var det lingvisten Jean François Champollion som med kunnskaper i gammelkoptisk løste gåten, *Précis du système hiéroglyphique* (1824).
En annen utfordring er den eldre skriften Linear A og den yngre Linear B, oppdaget under Arthur Evans utgravninger på Knossos, Kreta. Var skriften minoisk eller gresk ? Alice Kober fant at Linear B inneholdt gramatikk med kasus, bøyningsformer, bindestavelser og stavelser med konsonanter og vokaler. Det var imidlertid Michael Ventris og John Chadwick som løste gåten, Linear B er arakisk gresk, *Evidence for Greek dialect in the Mycenaean archives* (1953). Et språk fra Odyssevs og Homers tid. Jfr. Faistos disken, nå i det Arkeologiske muséet, Heraklion.

Kryptografi (gr. *kryptos*- skjult; *graphein*-skrive) er hemmelig skrift som går ut på å skjule innholdet i en tekst i form av en tall- eller bokstavkombinasjoner, enten ved **transposisjon** (bokstavene stokkes og bytter plass i et anagram) eller **substitusjon** (bokstavene beholder sin plass, men bytter identitet). Betår meldingen av n bokstaver inkludert mellomrom er det n fakultet (n!) mulige kombinasjoner. Et **chiffer** (siffer) lages ved kryptering (koding, enchiffrering) hos avsender via en klartekst, en **kryptoalgoritme** og en **kodenøkkel**. Den chiffrerte meldingen blir dechiffrert (dekodet, dekryptert) hos mottaker vha. en dechiffreringsalgoritme og en kodenøkkel, og den opprinnelige klarteksten kommer tilsyne.
I enkleste form gis hver bokstav i alfabetet et fortløpende heltall med start 1. Julius Cæsar sendte under Gallerkrigen krypterte meldinger til Cicero. I en **Cæsar-forskyvning** forskyves alfabetet et bestemt antall

plasser, noe som gir 25 forskjellige chiffer (28 hvis æ,ø og å inkluderes. For eksempel forskyve alfabetet 3 plasser:

	bokstav nr	V3
1	A	D
2	B	E
3	C	F
4	D	G
5	E	H
6	F	I
7	G	J
8	H	K
9	I	L
10	J	M
11	K	N
12	L	O
13	M	P
14	N	Q
15	O	R
16	P	S
17	Q	T
18	R	U
19	S	V
20	T	W
21	U	X
22	V	Y
23	W	Z
24	X	A
25	Y	B
26	Z	C

For å gjøre det litt vanskeligere tok man hensyn til frekvensen av bokstavene i språket (homofon substitusjon), og kodet hver av de vanligst forekommende bokstavene med flere forskjellige symboler. En annen måte var å starte alfabetet med et nøkkelord, og deretter fortsette med de resterende bokstavene i alfabetet som ikke inngikk i nøkkelordet. I et **bokchiffer** startet man numrering av bokstavene forløpende i teksten i en bok som var avtalt på forhånd. Et

Vegienèrkvadrat (*tabula recta*) består av først et alfabet etter fulgt radvis av 26 (eller 29) alfabet, hver med en trinnvis fra 1 økende Cæsar-forskyvning. Det har fått navn etter Blaise de Vigenère 1523-1596) som bl.a. skrev en avhandling om hemmelig skrift, *Traité de chiffres ou secrètes maniéres d´escrive* (1586).
Gjennom historien er det laget en lang rekke chiffer: Maria Stuart chiffer; det tyske ADFGVX-chiffer fra 1. verdenskrig som var både et transposisjons- og substitusjonschiffer; de tyske chiffermaskinene Enigma og Lorenz (56 bits nøkler) fra 2. verdenskrig, som ga kodeknekkerne ved Bletchley Park en utfordring, bl.a. Marian Rejevski og Alan Turing. Datamaskinene ga mulighet for digital i stedet for mekanisk kryptografering
Enhver utfordring for koding består i å overføre kodenøklene på en trygg og sikker måte mellom avsender og mottaker. Muligheten lå ARPA-net frigitt til sivil bruk i 1982, grunnlaget for Internet, som muliggjorde utveksling av kryptografiske nøkler over et usikkert offentlig nett mellom to eller flere personer som ikke kjenner hverandre. De som ga seg i kast med utfordringen var bl.a, Whitfield Diffie (f. 1944), Martin Hellman (f.1946) fra Standford-universitetet og Ralph Merkle. Svaret lå i modulær matematikk. Det er nå Diffie forslår prinsippet med en **asymmetrisk nøkkel**, **Diffie-Hellman-Merkle-metoden**. En offentlig kjent krypteringsnøkkel som alle kan bruke til å kryptere meldinger, og en privat nøkkel som brukes til å dekryptere. Selv den som har kryptert meldingen kan ikke åpne den etter at den er kryptert, det er det bare den som har den private nøkkelen. Hva slags matematiske enveisfunksjoner er det som klarer dette ?
En klokke virker etter prinsippet addisjon modulo 12.
Man kan vise prinsippet ut fra følgende formel:

$$y^x = (mod\ m) \qquad y < m$$

Astrid og Bjørn avtaler uten hemmeligheter og uten å møtes to primtall p=23 og en base g=5. Dette er offentlige nøkler ”public key”) åpent tilgjengelig for alle.
Deretter velger Astrid et hemmelig tall (privat nøkkel, ”private key”) for eksempel a=6 som hun holder skjult for alle andre, og setter dette inn i formelen

$$A = g^a mod\ p$$

Dette gir tallet A=8 som hun sender til Bjørn.

Bjørn gjør tilsvarende og velger seg en hemmelig tall (privat nøkkel) for eksempel b=15,

$$B = g^b mod\ p$$

dette gir tallet B=19 som han sender til Astrid.
Astrid beregner:

$$S = B^a mod\ p$$

Bjørn gjør tilsvarende og beregner:

$$S = A^b mod\ p$$

Vips, nå har begge har nå samme nøkkel S=2, uten å ha sendt selve nøkkelen over nettet. Ukjent for innsyn er a, b og S

Selv om en utenforstående Luring skaffer seg tallene P=23, g=5, $A=g^a modp = 8$ og $B=g^b modp =19$ som er blitt sendt åpent over nettet, kan han vanskelig finne at nøkkelkoden S = 2, som nå både Astrid og Bjørn besitter. Dette blir eksempel på en symmetrisk nøkkel som kan brukes til både enchiffrere og dechiffrere.

Vi kan bytte ut p, g, a og b med andre tall og se at prinsippet stemmer, men man ser også at velger man store tall stanger man fort hodet i taket. I virkeligheten bruker man primtall p med flere hundre siffer og hemmelige slumptall a og b kan bestå av 100 siffer, mens g er et relativt lite primtall.

Litteratur:Wikipedia

RSA-koden

Selv om James Ellis, Clifford Cock og Malcolm Williamson ved GCHQ i Cheltenham, hadde funnet løsningen tidligere, så er det Ronald **R**ivest, Adi **S**hamir og Leonard **A**dleman ved MIT som sikret seg patentet på RSA metoden. Metoden baserer seg på en offentlig nøkkel n, kjent for

alle, som er produktet av to meget store primtall p og q, helst av samme bitslengde

$$n = p \cdot q$$

Primfaktorene p og q holdes hemmelig. n er modulus for både den offentlige og private nøkkelen. n uttrykt i bits angir nøkkellengde.
Beregner **Eulers phifunksjon**:

$$\varphi(n) = (p-1)(q-1)$$

hvor φ(n) også kalles **Eulers totient funksjon**.
I tillegg trenger man en offentlig nøkkel til, k, som skal brukes til koding, hvor 1<k<φ(n).
k og φ(n)må ikke ha noen felles faktorer.

Velger et heltall k med kort bitlengde og liten Hamming vekt som eksponent slik at

$$1 < k < \varphi(n)$$

og **største felles divisor** gfd(k,φ(n)=1, dvs. k og φ(n) er **koprimtall**. k er eksponenten i den offentlige nøkkelen. Hammingvekt er summen av antall symboler som er forskjellig fra null.
Alle bokstaver og tall har en decimal ASCII-kode, eller vi kan på annen måte angi bokstaver med tall, og derved kan vi nå nå kode og kryptere en hvilken som helst bokstav eller tall M til C ifølge formelen:

$$C = M^k (mod\ n)$$

For dekoding trenger mottakeren en privat nøkkel d, og den offentlige nøkkelen n, og vi kommer tilbake til M ved følgende:

$$C^d (mod\ n) = M$$

Dekrypteringseksponenten d i den private nøkkel velges slik at

$$k \cdot d \equiv 1\big(mod(p-1)(q-1)\big) \equiv 1(mod\ \varphi(n))$$

φ(n) må også holdes hemmelig.

For den som ønsker å vite mer har Simon Sing skrevet en utmerket bok: *The code book. The science of secrecy from ancient Egypt to quantum cryptography* (1999), som også foreligger på norsk.

Her kan man også lese om hvordan Phil Zimmermann utviklet kryptosystemet "Pretty Good Privacy", PGP, som er et symmetriske IDEA-chiffer som ligner DES. I PGP er alle prosessene automatisert, hvor bl.a. tilfeldige musebevegelser gir tilfeldige primtall p og q. I takt med datamaskiner med økt regnekapasitet er kryptosystemer stadig utsatt for angrep fra kodeknekkere, noe som krever stadig større primtall og bitslengde.

Slumptallsgeneratorer

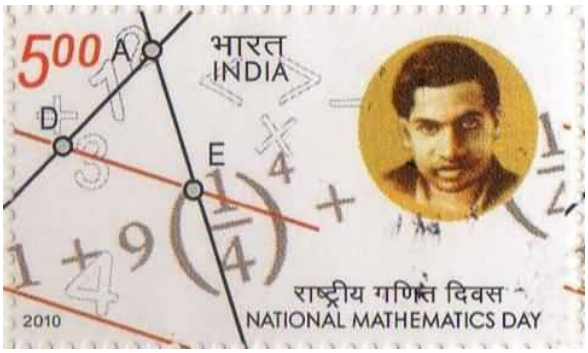
Slumptall er tilfeldige tall generert fra en statistisk fordeling. En ekte slumptallsgenerator er terningkast, men i datamaskiner er det uekte slumptallsgeneratorer (PRNG- pseudorandom number generator) som lager **pseudoslumptall** (pseudorandome tall) basert på en algoritme. Slumptall benyttes i Monte Carlo simuleringer og innen kryptografi. At tallene virkelig er tilfeldige og ikke følger et mønster er derfor av avgjørende betydning, noe som John von Neumann påpekte. Pseudoslumptall kan man hente fra forskjellige statistiske fordelinger. For å kunne reprodusere resultater er det viktig å starte slumptallsgeneratoren på samme sted hver gang. **Mersenne-twister** som baserer seg på en lineær kongruent generator kombinert med primtallene. Perioden for denne generatoren er 2^{199937}-1 tilnærmet lik $4.32 \cdot 10^{6001}$. Mersenne twister, utviklet av Makota Matsumoto og Tauji Nishimura i 1998, hvor perioden for gjentakelse er 2^{19937}-1 iterasjoner, 32-bits tall jevnt fordelt i 623 dimensjoner, jfr. Mersenne-primtall 2^n-1. Innen kryptografi må man ha kryptografisikre pseudoslumptallsgeneratorer.
Målet for en simulering er å gjenta en enkel prosedyre tusenvis av ganger, som erstatning for mer komplekse beregninger, og som det i mange tilfeller også er umulig å utføre.
Pseudorandome tall vil i pratisk bruk oppføre seg omtrent som tilfeldige tall.
Slumptall kan bli laget via en **lineær kongruent generator**:

$$x_{i+1} = ax_i + b(mod\ d) \qquad a > 0, b \geq 0, d > 0, i = 1, 2, 3, \ldots$$

hvor a er multiplikator, b er økningen og d er modulus.

Taxi-tall

Indiske Srinivasa Aiyangar Ramanujan (1887-1920) var en autodidakt (selvlært geni) med intuitive anlegg for tall. Han kom til universitetet i Cambridge hvor Godfrey Harold Hardy (1877-1947) og John Edensor Littlewood (1885-1977) arbeidet.



En av anekdotene var da Hardy kom på sykebesøk til Ramanujan og sa at han var kommet med taxi nr, 1729, et uinteressant tall ifølge Hardy. Hvorpå Ramanujan repliserte at dette var et meget interessant tall, det minste naturlige tallet som kan skrives på to forskjellige måter som summen av to kubiske tall:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3$$

som ga opphav til en type tall kalt taxi-tall.

Taxi-tall (TA(n)) er det minste tallet som kan uttrykkes som summen av to positive algebraiske kuber på n forskjellige måter.

De første taxitallene er Ta(1)=2=1^3+1^3, Ta(2)=1729, Ta(3)=87539319= 167^3+436^3=228^3+423^3=255^3+414^3.

Hardy-Ramanujantallet 1729 er også et **Carmichael-tall** (Robert Carmichael). De første Carmichael-tallene er 561 (3·11·17), 1105 (5·13·17) og 1729 (7·13·19).

Ramanujan oppdaget spesielle uendelige rekker bl.a. den følgende for resiproskverdien av pi (π).

$$\frac{1}{\pi} = \frac{2\sqrt{2}}{9801} \sum_{n=0}^{\infty} \frac{(4n)!\,(1103 + 26390n)}{n!^4\, 396^{4n}}$$

Denne rekken konvergerer eksponensielt og kan brukes til å regne ut π med mange siffer.
Rekken har tilknytning til

$$e^{\pi\sqrt{58}} = 396^4 - 104.000000177\ldots$$

og 5·7·13·58=26390, 99·99=9801, 4·99=396

Klassetallene *h(d)* er tall av typen

$$a + b\sqrt{-d}$$

hvor d er de ni **Heegner-tallene** 1,2,3,7,11,19,43,67 og 163. Gauss hadde dette som konjektur og det ble i 1952 bevist av Kurt Heegner.
Følgende tall kalles **Ramanujans konstant** og er et transendentalt tall, også oppdaget av Charles Hermite i 1859

$$e^{\pi\sqrt{163}} \approx 2.625374 \cdot 10^{17} \approx 640320^3 + 744$$

Komplekse tall

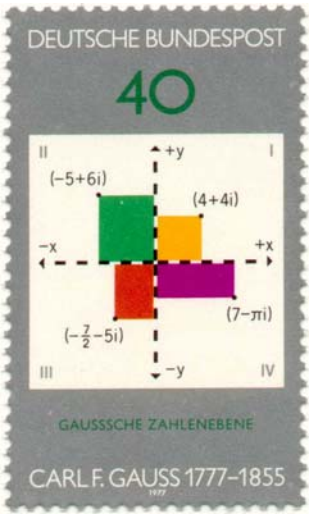
Vi ønsker å ha tall som gir svar i alle ligninger. Har vi ligningen:

$$x^2 + 1 = 0 \quad \rightarrow \quad x = \sqrt{-1}$$

Vi kan ikke ta kvadratrot av et negativt tall. Dette førte fram til de **komplekse tall**, som vi skal se på seinere.
René Descartes hadde i *Géometrie* (1637) tatt opp problemstillingen med kvadratroten til negative tall.

Det må være mulig å løse kvadratiske ligningen $x^2+1=0$, som har ingen relle løsninger, hvis tallrekken skulle være komplett. Det vil si $x^2=-1$ og $x=\pm\sqrt{-1}$, men hvor det komplekse tallet (0,1) er en løsning. x=i er en annen løsning.

Den italienske matematikeren Rafael Bombelli (1526-1572) presenterte i verket *L'Algebra* (1526) løsninger av ligninger etter metoden til Scipione Del Ferro (1465-1526) og Niccolo Fontana Tartaglia (1499-1557), men la også et grunnlag for de komplekse tallene.



Allerede 1797 hadde den norske matematikeren Caspar Wessel (1745-1818), i familie med dikteren Johan Herman Wessel, innført et komplekst plan med to akser (**Wessel-plan**). *"Han tegner landkart og leser loven, og er så flittig som jeg er doven".* Dette ble også gjort i 1806 av Jean-Robert Argand (1768-1822) (Argand plan), og deretter videre utviklet av Gauss i 1831. Komplekse tall kan fremstilles geometrisk i et **komplekst plan** med en horisontal reell x-akse og en vertikal imaginær yi-akse. Komplekse tall er todimensjonale vektorer, men med en ny type multiplisering. Euler innførte tallet *i* kalt imaginær enhet

$$i = \sqrt{-1} \qquad i^2 = -1 \quad i^3 = -i \quad i^4 = 1 \quad i^5 = i \qquad \frac{1}{i} = -i$$

På denne måten kan komplekse tall skrives som:

$$z = a + bi = (a, b)$$

hvor *a* er et reelt tall.

Lengden av z lik modulus z (|z|)blir ifølge Pythagoras hvor a og b er kateter og r=|z| er hypotenus:

$$|z| \equiv r = \sqrt{a^2 + b^2}$$

Komplekse tall kan uttrykkes i form av **enhetskoordinatvektorene** (1,0) og (0,1) slik at
(a,b) = (a,0) + b(0,1)
En vektor har lengde og retning, og i det **komplekse plan** har det komplekse tallet *z* det ordnete paret(*a,b*). Ethvert komplekst tall kan uttrykkes som et ordnet par. De komplekse tallene ($\mathbb{C}$) er en utvidelse av de relle tallene ($\mathbb{R}$) som bare har en reell del.

Geometrisk framstilling av det komplekse tallet (*x,y)*= *x*+*yi*.
Vi kan uttrykke (*x,y*) som polarkoordinater:

$$x = r\cos\theta \qquad y = r\sin\theta \qquad -\pi < \theta < \pi$$

Vi kan da skrive:

$$x + yi = r(\cos\theta + i\,\sin\theta)$$

Hvis vi har det komplekse tallet *z*:

$$z = x + yi$$

så kan det skrives som lengden (**modulus**) eller **absoluttverdi** |*z*| = *r* som er avstanden (*x,y*) til origo (0 + 0i).

$$mod|x + yi| = r = |x + yi| = \sqrt{x^2 + y^2}$$

og polarvinkelen θ (mot klokka) kalt **argument** til *x*+*yi*(*arg z*).

$$arg(z) = arg|x + yi| = \theta$$

Vi kan finne **modulus** til et komplekst tall, det vil si avstanden (r) fra origo til koordinatene (a,b) i et komplekst tall z=a+bi, i vårt eksempel (2,3).
Argumentet til det komplekse tallet er vinkelen mellom reell akse og vektoren som går fra origo (0,0) til (a,b), regnet mot klokka. Et komplekst tall kan derved skrives i form av polarkoordinater (r,φ).
Det komplekse tallet kan roteres inntil 2π (0, 2π), og i multipler av 2π, men det er vanlig å bruke intervallet (-π, π).

Det komplekse tallet 0 (0+ 0i) har modulus lik 0.
Et komplekst tall kan også ha en polar representasjon, hvor kooridinatpunktet (a,b) erstattes med (r,θ)

$$z = a + bi = |z|(cos\theta + isin\theta) = r(cos\theta + isin\theta) = rcos\theta + irsin\theta$$

hvor r er lik lengden (modulus) til z og vinkelen theta (θ) er argumentet til z:

$$\arg(z) \equiv \theta = atan\left(\frac{b}{a}\right) = atan\left(\frac{|z|sin\theta}{|z|cos\theta}\right) = atan\left(\frac{rsin\theta}{rcos\theta}\right)$$

Man må finne i hvilken kvadrant θ ligger.
Et komplekst tall presentert på trigonometrisk form som polarkoordianter blir:

$$z = x + yi \qquad z = rcos\theta + rsin\theta\, i \qquad z = re^{i\theta}$$

Det betyr at et komplekst tall med modulus=1, |z|=1
får retningsfaktoren:

$$cos\theta + sin\theta\, i$$

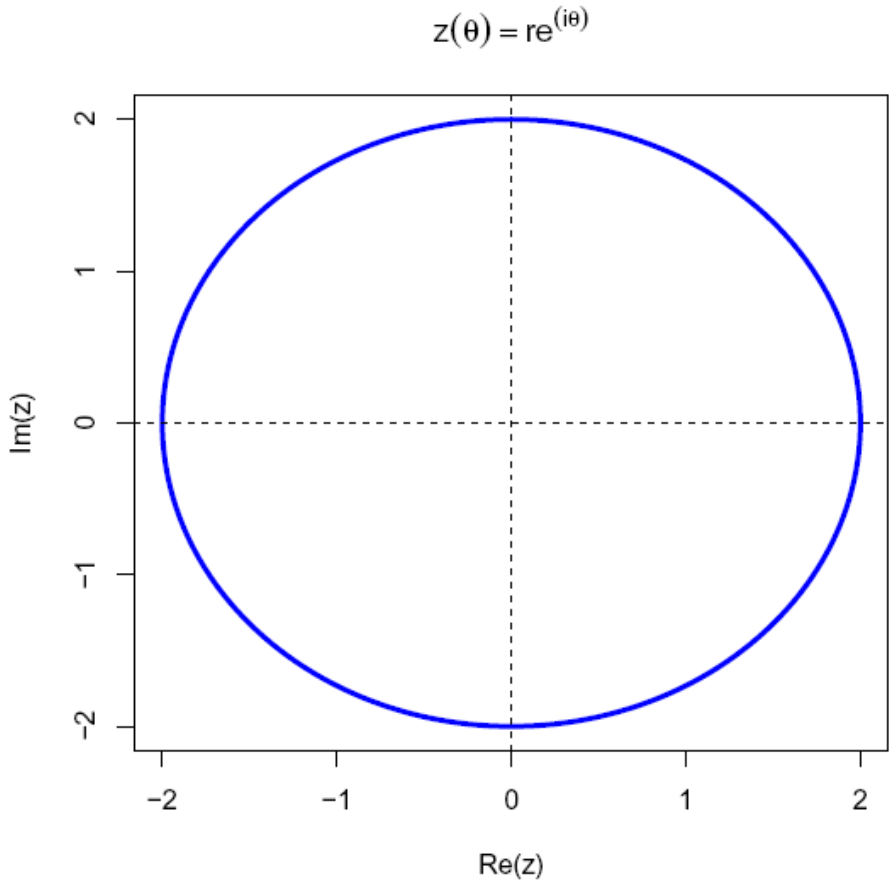
siden

$$cos^2\theta + sin^2\theta = 1$$

Funksjonen

$$z(t) = r \cdot e^{it}$$

blir en sirkel med radius r



Figur. Vinkel 2π-radianer og radius = 2

Vi benytter Eulers formel som viser sammenhengen mellom trigonometriske funksjoner og den komplekse eksponentialfunksjonen, hvor e er basis i naturlige logaritmer:

$$e^{i\theta} = cos\theta + isin\theta$$

gir dette at *z* kan også skrives som polar presentasjon:

$$z = re^{i\theta}$$

Vi har også:

$$\left|e^{i\theta}\right| = \sqrt{cos^2(\theta) + sin^2(\theta)} = 1$$

Euler fant sammenhengen:

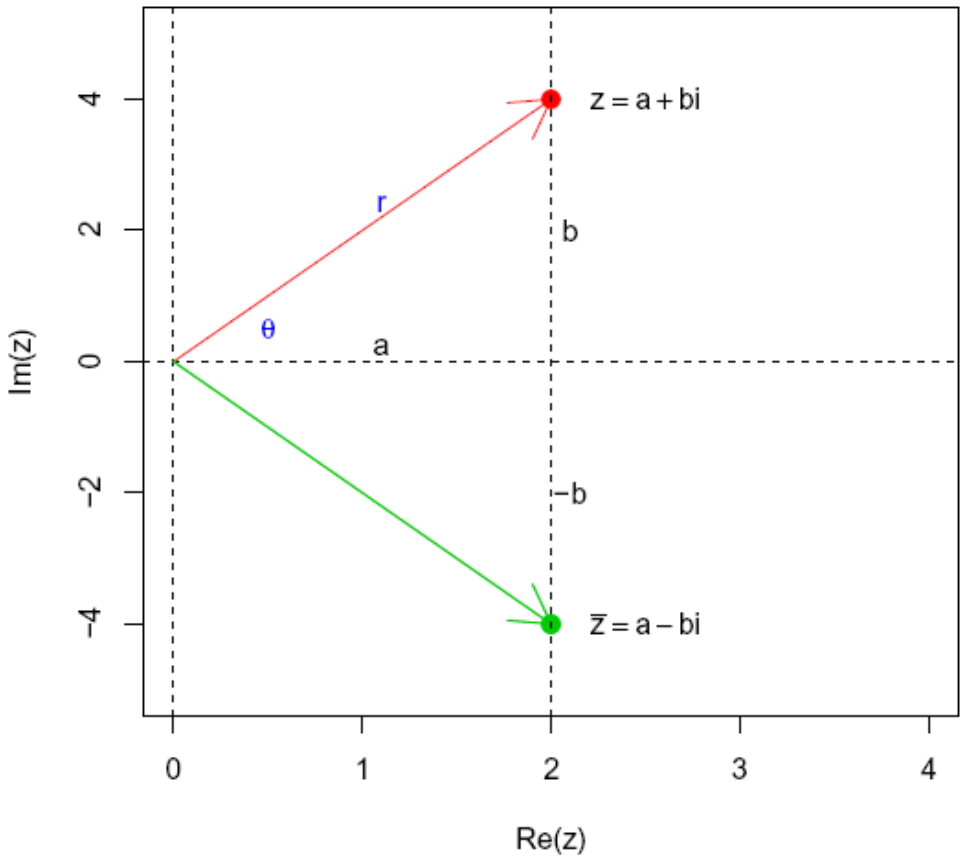
$$e^{i\pi} + 1 = 0$$

Hvis vi har et komplekst tall z=x+yi så vil **det komplekse konjugatet** $\bar{z}$= x-yi være speiling av *z* omkring x-aksen:

$$z\bar{z} = (x + yi)(x - yi = x^2 + y^2) = |z|^2$$

Multipliserer vi et komplekst tall z=a+bi med det komplekse konjugatet hvor fortegnet på i snus, så får vi et reelt tall:

$$z \cdot \bar{z} = a^2 + b^2 \qquad hvor\ \bar{z} = a - bi$$



Figur. Komplekst tall z = 2 + 4i og komplekst konjugat

Når vi betrakter komplekse tall som ordnete par (x_1,x_2) så kan vi addere og multiplisere på samme måte som for todimensjonale vektorer:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

$$a \cdot (x_1, x_2) = (ax_1, ax_2)$$

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1)$$

$$\frac{1}{(x_1, y_1)} = \left(\frac{x_1}{x_1^2 + x_2^2}, \frac{-x_2}{x_1^2 + x_2^2}\right) \qquad (x_1, x_2) \neq (0,0)$$

Nullkomplekstallet er lik (0,0).

De komplekse tallene er en utvidelse av de relle tallene som bare har en reell del. Vi kan summere komplekse tall:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Multiplisere komplekse tall:

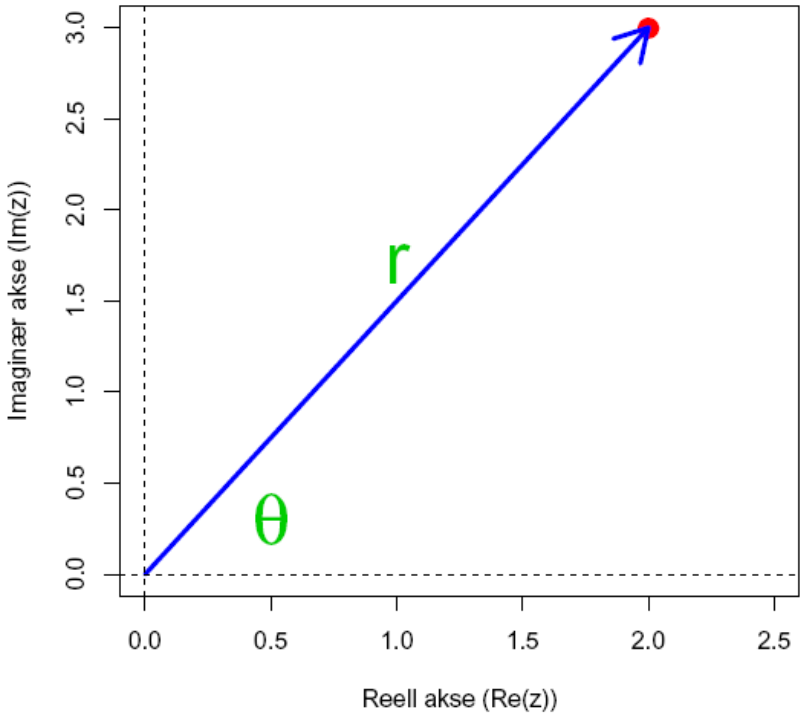
$$(a + bi) \cdot (c + di) = (ac - bd) + (bc + ad)i$$

Komplekse tall kan brukes i de fleste funksjoner. Vi kan plotte det imaginære tallet med en reell akse (Re(z)) og imaginær akse (Im(z)):

For det komplekse tallet:

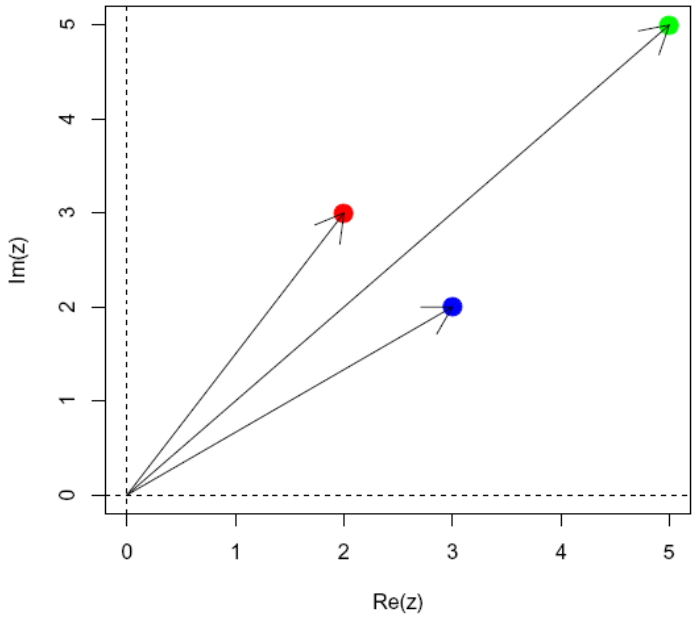
$$z = 2 + 3i$$

så er det 2 på den relle aksen og 3 på den imaginære aksen

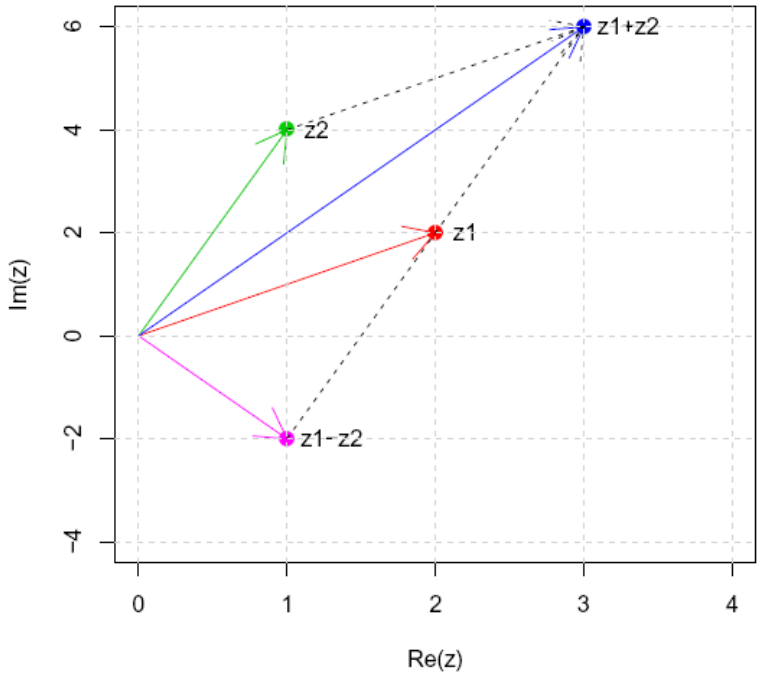


Figur. Det komplekse tallet z = 2 + 3i. Den greske bokstaven theta (θ)angir vinkelen, modulus z = 3.605551, og argument z er lik 0.9827937.

Vi kan summere komplekse tall på samme måte som for vektorer



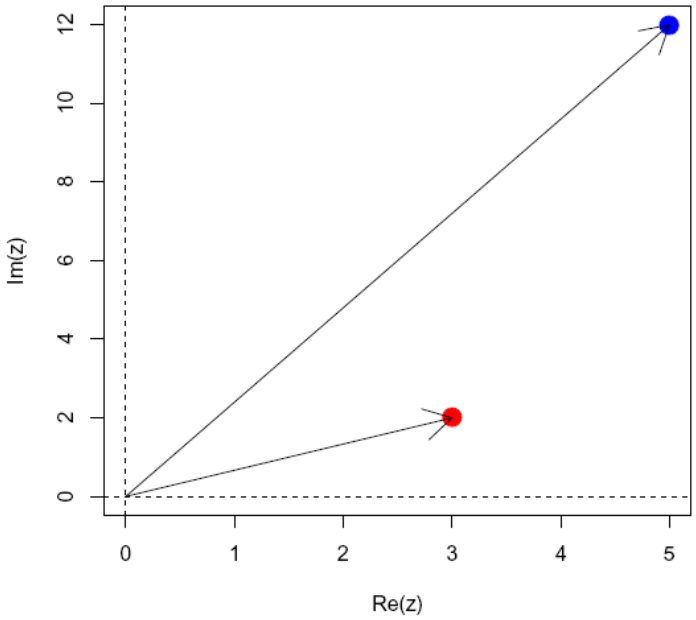
Figur. Summering av to komplekse tall. Summen av de to komplekse tallene z1 = 2 + 3i og z2 = 3 + 2i. z1 + z2 = z3, hvor z3= 5 + 5i . Re(z) er reell akse og Im(z) er imaginær akse. Origo er (0 + 0i). Summen av de komplekse tallene er diagonalen i et parallellogram med kanter dannet av de to komplekse tallene. Et parallellogram består av to kongruente trekanter.



Figur: To komplekse tall z1= 2 + 2i og z2 = 1 + 4i, summen av dem z1+z2 = 3 + 6i, og substraksjon z1-z2 = 1-2i.

Vi kan multiplisere to komplekse tall hvor vi erstatter i^2 med -1.

$$(a+bi)^2 = (a+bi)\cdot(a+bi) = (a^2-b^2)+(2ab)i$$



Figur. Multiplisering av det komplekse tallet z = 3+2i med seg selv og produktet z^2.
Multiplikasjon av et komplekst tall med seg selv dobler vinkelen og kvadrerer avstanden fra origo.

Multiplisering av komplekse tall, husk at $i^2 = -1$

$$(a+bi)\cdot(c+di) = (ac-bd)+(bc+ad)i$$
$$(2+3i)\cdot(4+5i) = (8-15)+(12+10)i = -7+22i$$

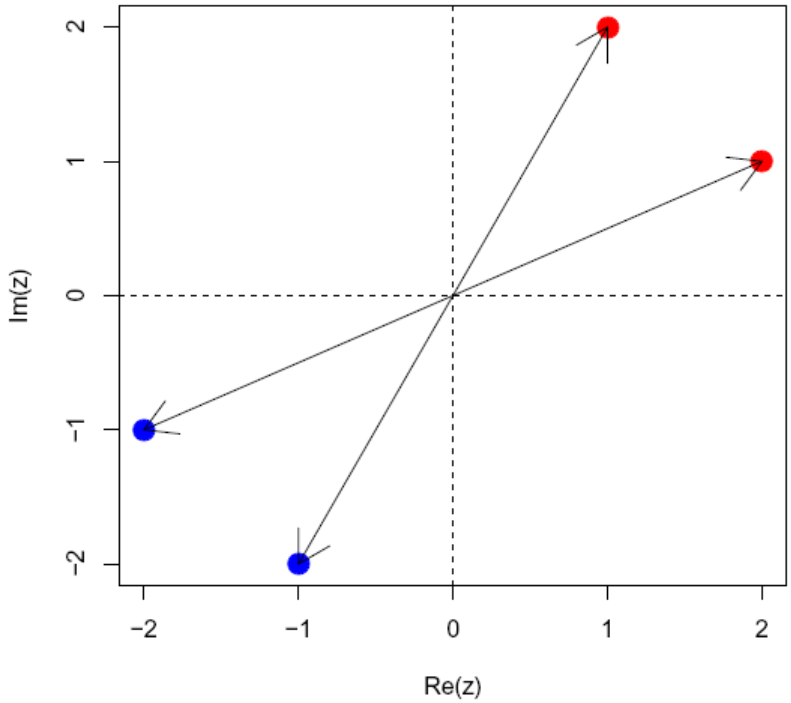
Multiplisering av to komplekse tall vil si å multiplisere moduli og summere polarvinklene.
Vi kan skrive opp de komplekse tallene i polar representasjon:

$$z = r_1(cos\theta + isin\theta) \qquad w = r_2(cos\varphi + isin\varphi)$$

$$z\cdot w = r_1\cdot r_2[(cos\theta cos\varphi - sin\theta sin\varphi)+(cos\theta sin\varphi + cos\varphi sin\theta)i]$$
$$= r_1\cdot r_2[cos(\theta+\varphi)+sin(\theta+\varphi)]$$

Vi kan finne den resiproke til et komplekstall (≠0):

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}$$



Figur. To komplekse tall rotert 180 grader (180°).

Hvis vi har det komplekse tallet *z* = *x* + *yi* så har vi det **komplekse konjugatet**:

$$\bar{z} = x - iy$$

som er speiling over den reelle aksen
Hvis man har et komplekst tall z = 2 + i så blir det komplekse konjugatet lik 2 – i.
Multiplikasjon av et komplekst tall z med det komplekse konjugatet til z gir et reelt tall≥0

$$z \cdot \bar{z} = |z|^2 = (a^2 + b^2)$$

Divisjon ved å multiplisere teller og nevner med det komplekse konjugat til nevner. Det betyr at nevner blir et reelt tall.

$$\frac{z_1}{z_2} = \frac{z_1 \bar{z}_2}{z_2 \bar{z}_2} = \frac{z_1 \bar{z}_2}{|z_2|^2}$$

Vi kan gjøre tilsvarende multiplikasjon og divisjon, men nå som polarkoordinater:

$$z_1 = |z_1| e^{i\theta_1} \qquad z_2 = |z_2| e^{i\theta_2}$$

Vi benytter nå eksponentialloven som også gjelder for komplekse tall:

$$z_1 \cdot z_2 = |z_1| \cdot |z_2| e^{i(\theta_1 + \theta_2)}$$

For divisjon bruker vi de Moivres formel:

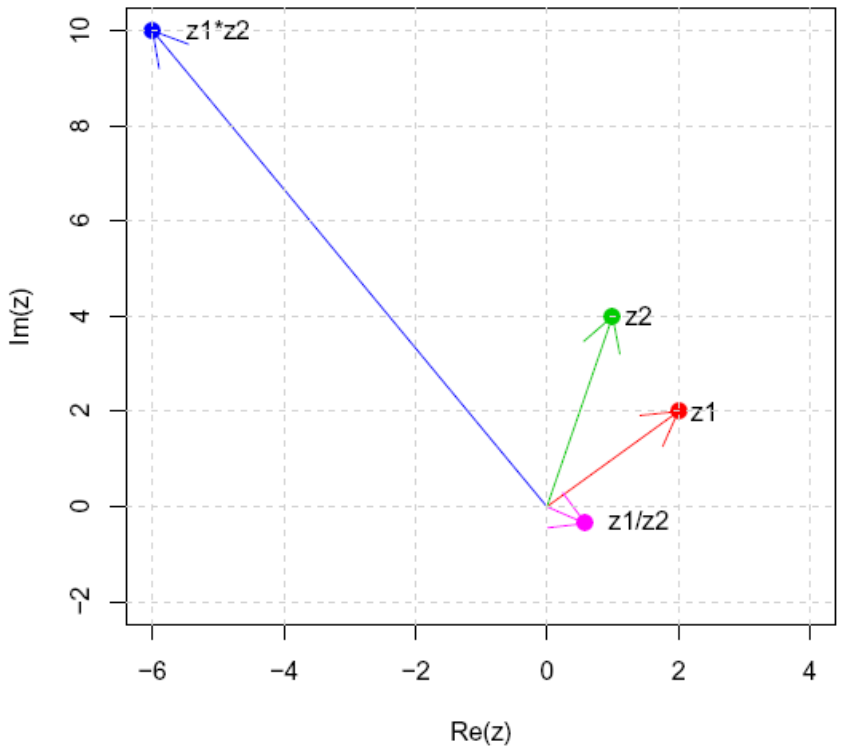
$$z = |z|(cos\theta + isin\theta) = |z|e^{i\theta}$$

Det komplekse konjugatet:

$$\bar{z} = |z|(cos\theta - isin\theta) = |z|e^{-i\theta}$$

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{e^{-i\theta}}{|z|}$$

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|} e^{i(\theta_1 - \theta_2)}$$



Figur. Komplekse tall z1= 2 + 2i og z2 = 1 + 4i, produktet z1·z2 = -6 + 10i og divisjonen z1/z2 = 0.59 -0.36i.

Hvis vi har to komplekse tall *z* (z≠0) og *w* har vi:

$$\frac{w}{z} = \frac{w \cdot \bar{z}}{z \cdot \bar{z}} = \frac{w \cdot \bar{z}}{|z|^2}$$

Kvadratroten av komplekse tall

Hvis vi har et komplekst tall

$$z = x + yi \qquad z = r(cos\theta + (sin\theta)i)$$

så blir kvadratet lik:

$$z^2 = (x + yi) \cdot (x + yi) = x^2 - y^2 + (2xy)i$$

$$z^2 = r^2(cos2\theta + (sin2\theta)i)$$

det vil si kvadrering av modulus og dobling av polarvinkelen.
Kvadratroten av z i form av polarvinkler blir:

$$\sqrt{z} = \pm\sqrt{r} \cdot \left(cos\frac{\theta}{2} + \left(sin\frac{\theta}{2}\right)i\right)$$

som er det samme som kvadratroten av modulus og halvering av polarvinkelen, og den andre kvadratroten blir det negative av dette.

Vi kan finne n-te roten av et komplekst tall slik at

$$w^n = z$$

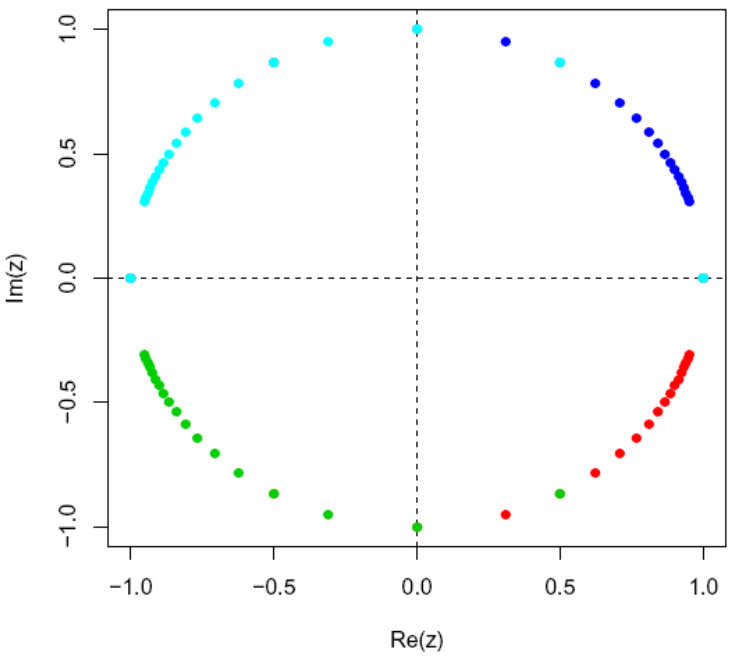
Hvis vi har $w^n=1$ så gjelder:

$$w_n = cos\frac{2(n-1)\pi}{n} + i\ sin\frac{2(n-1)\pi}{n}$$

Den **prinsipale n-te roten** av z er:

$$w = |z|^{\frac{1}{n}}\left(cos\left(\frac{\theta + 2\pi}{n}\right) + i\ sin\left(\frac{\theta + 2\pi}{n}\right)\right)$$

og alle røttene blir liggende på en sirkel med sentrum i origo og radius $|z|^{1/n}$.



Figur. n-te roten blir liggende på en sirkel med radius 1.

Inverst kompleks tall

Det finnes bare et inverst kompleks tall z^{-1} til z slik at

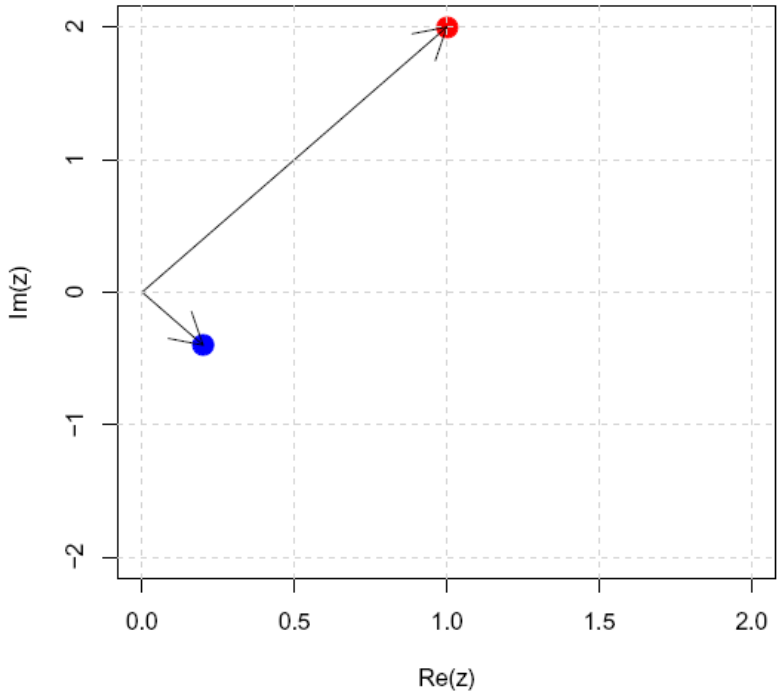
$$z \cdot z^{-1} = 1 \qquad z^{-1} = \frac{1}{z} \qquad z \neq 0$$

Det betyr også at

$$argz^{-1} = -argz$$

og at:

$$modz^{-1} = \frac{1}{modz}$$



Figur. Komplekst tall z= 1+ 2i og det inverse 1/z= 0.2 – 0.4i

Eksponentialfunksjonen for komplekse tall

Eksponentialfunksjonen for komplekse tall må kunne følge samme regneregler som for reelle tall dvs.

$$e^{z_1}e^{z_2} = e^{z_1+z_2}$$

og vi må kunne skrive:

$$e^{x+yi} = e^x \cdot e^{iy}$$

Hvis z=x+iy så vil e^z være et komplekst tall:

$$e^z = e^x(\cos y + i\, siny)$$

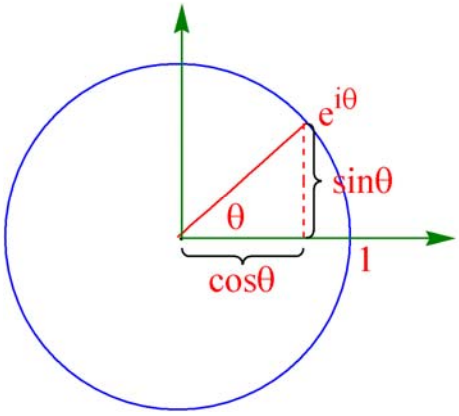
Hvis vi har vinkelen θ så har vi:

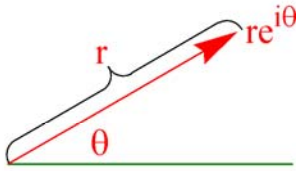
$$e^{i\theta} = cos\theta + isin\theta$$

Det betyr at komplekse tall kan uttrykkes som kompleks eksponentialfunksjon. Et komplekst tall z med modulus (absoluttlengde)r = |z| og med vinkel (argument) θ kan da skrives som:

$$z = x + iy = re^{i\theta} \qquad r = |x + iy| \qquad \theta = arg(x + iy) + 2n\pi$$

Dette er en nyttig formel for multiplikasjon og divisjon av komplekse tall. Vi kan betrakte $e^{i\theta}$ som et punkt på enhetssirkelen.





Hvis vi har to komplekse tall $z_1=r_1e^{i\theta}$ og $z_2=r_2e^{i\varphi}$ så vil:

$$z_1 z_2 = r_1 e^{i\theta} \cdot r_2 e^{\varphi} = r_1 r_2 e^{i(\theta+\varphi)}$$

$$\frac{z_1}{z_2} = \frac{r_1 e^{i\theta}}{r_2 e^{i\varphi}} = \frac{r_1}{r_2} e^{i(\theta+\varphi)}$$

For eksempel det komplekse tallet z = (1,1) = 1+i med argument lik π/4 og modulus lik $\sqrt{2} = 1.414214$ (|z|=r=|1+i|=$\sqrt{1^2+1^2}$ og kan skrives som $z=\sqrt{2}e^{(i\cdot\pi/4)}$.

Euler kunne vise at:

$$1 = cos^2\theta + sin^2\theta = (\cos\theta + i \cdot \sin\theta) \cdot (\cos\theta - i \cdot \sin\theta)$$

og fant videre den interessante sammenhengen mellom det naturlige tallet *e*, *π* og *i* ved:

$$e^{i\cdot\pi} = cos\pi + i \cdot sin\pi$$

Euler gjorde det derved mulig å løse ligningen $e^x = -1$ hvor svaret er $x = i\pi$. Det betyr at $e^{i\pi} = -1$

$$e^{i\cdot\pi} = \cos\pi + i \cdot \sin\pi = -1 + i \cdot 0 = -1$$

$$e^{\frac{i\cdot\pi}{2}} = i \qquad e^{i\cdot\pi} = -1 \qquad e^{\frac{3i\cdot\pi}{2}} = -i \qquad e^{i\cdot 2\pi} = 1 \qquad \ln(-1) = i\pi \qquad ln(\pm i) = \pm\frac{1}{2}\pi i$$

$$e^{i\cdot\theta} = cos\theta + isin\theta \qquad (Eulers\ ligning)$$

$$sin\theta = \frac{1}{2i}\left(e^{i\cdot\theta} - e^{-i\cdot\theta}\right) \qquad cos\theta = \frac{1}{2}\left(e^{i\cdot\theta} + e^{-i\cdot\theta}\right)$$

$$\sin(i\theta) = i\cdot sinh\theta \qquad \cos(i\theta) = cosh\theta \qquad \sinh(i\theta) = i\cdot sin\theta \qquad \cosh(i\theta) = cosh\theta$$

$$z = a + bi \quad \rightarrow \quad z^2 = (a^2 - b^2) + 2abi \qquad z^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$$

Hvis vi har et komplekst tall og det komplekse konjugatet:

$$z = a + bi \quad \bar{z} = a - bi \quad \rightarrow \quad |z|^2 = z\cdot\bar{z} = a^2 + b^2 \qquad e^z = e^a(cosb + i\cdot sinb)$$

Komplekse logaritmer

Logartimefunksjonen og eksponentialfunksjonen er inverse funksjoner og gjelder også for komplekse tall:

$$e^{lnz} = z = |z|e^{i\theta} = e^{ln|z|}e^{i\theta} = e^{ln|z|+i\theta}$$

Det betyr at:

$$lnz = ln|z| + iarg(z)$$

Den relle delen blir den naturlige logaritmen til z, men i den imaginære delen inngår argumentet til z, som man må vite.

Binære tall

De vanligst brukte tallsystemene er **10-tallsystemet** (dekadisk tallsystem) og det **binære tallsystem** (totallsystem), hvorav sistnevnte benyttes i datamaskiner.

10-tallsystemet bruker grunntall 10, og bygget opp således:

$$\ldots\ a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10^1 + a_0 10^0$$

og husk 10^0 =1, og $a_0, a_1, \ldots, a_n$ kan være et av tallene i mengden 0-9.

For eksempel blir tallet 1729 skrevet således:

$$\ldots 0 \cdot 10^4 + 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10^1 + 9 \cdot 10^0$$

Skal man skrive desimaltall settes komma er punkten etter 10^0 og så fortsetter rekken videre mot høyre 10^{-1}, 10^{-2} osv.

Det binære tallsystemet med 2 som grunntall:

$$\ldots a_4 2^4 + a_3 2^3 + a_2 2^2 + a_1 2^1 + a_0 2^0$$

$2^0=1$, og $a_0, a_1, \ldots, a_n$ kan være et av tallene 0 eller 1

De første naturlige tallene skrevet binært blir:

0=0	4=100	8=1000
1=1	5=101	9=1001
2=10	6=110	10=1010
3=11	7=111	11=1011

For eksempel tallet 9 skrevet binært:

$$\ldots 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 0 + 8 + 0 + 0 + 1 = 9$$

Babylonerne brukte grunntall 60 og vi finner dette igjen i inndelingen av sirkelen i 360 grader og 1 time = 60 sekunder. Mayafolket hadde grunntall 20 og vi finner dette igjen i snes (20) (et snes egg) og skokk (3·20=60) (en skokk unger), eller i den danske tellemåten (firs = 4·20 = 80) eller fransk quatre (20) vingt (4) = 80. Grunntallet 12, som også inngår i faktorisering av 60, finner vi 12 månefaser, dusin (12) (et dusin egg), et tylft tømmer (12), og gross (12·12=144). En klokke er syklisk, hvor når man kommer til klokken 12 er man tilbake til utgangspunktet. På en klokke har vi 6 + 12 = 6, det vil si 12 tilsvarer 0.

Totallsystemet har **grunntall 2** og bruker tallene 0 og 1 som **binære siffer**. Et binært siffer kalles bit, forkortelse for ”binary digit”, og tilsvarer lagerplassen for en elementær enhet. Et ord består av 8 lagerposisjoner og danner til sammen 1 byte, dvs. ordlengden er 8 bits. Dette gir mulighet for 256 kombinasjoner av 0 og 1.

$$2^8 = 256$$

Tallet 255 som binært blir 1 1 1 1 1 1 1 1 er det største tallet som kan skrives med ordlengden 8 bits.
Det binære tallsystemet har sin opprinnelse fra det gamle Kina og ble tatt i bruk av Leibniz.

De første desimaltallene 0-7 får tilsvarende binære tall:
0 = 0; 1 = 1; 2 = 11; 3 = 10; 4 = 100; 5 = 101; 6 = 110; 7 = 111
Hvis to tall med 8 bits summeres kan vi få tall som er 9 bits. Vi summerer to tall mellom 0 og 255 og blir tallet for stort trekker vi fra 256, addisjon modulo 256. I **flytende aritmetikk** skrives tall som $2^x \cdot y$ hvor x og y er hele tall som kan bli lagret over flere ord (byte).

Ethvert tall kan brukes som basis i et tallsystem. For eksempel et tallsystem med basis 6 og skrevet med tallene 0-5.
Tallet 1043 med basis 6

$$1 \cdot 6^3 + 0 \cdot 6^2 + 4 \cdot 6^1 + 3 \cdot 6^0 = 243$$

I et binært tallsystem uttrykkes alle tall, bokstaver og tegn i form av 0 (falsk) og 1 (sann). Et binært tall kalles en **bit**. Åtte binære tall kalles en **byte**. Man pleier å bruke større grupper med bytes, 32 bits = 4 bytes, 64 bits = 8 bytes. Med 32 bits kan man beskrive 232 tall, men siden disse skal brukes til både positive og negative tall er det største hele tallet som kan beskrives i et 32-bits system i praksis lik

$$(2^{31}) - 1 = 2147483647$$

For å beskrive et større antall bits eller bytes brukes følgende SI-enheter:

kilobyte	KB	10^3	petabyte	PB	10^{15}
megabyte	MB	10^6	exabyte	EB	10^{18}
gigabyte	GB	10^9	zetabyte	ZB	10^{21}
terabyte	TB	10^{12}	yottabyte	YB	10^{24}

To opphøyd i n-te hvor n: 0 – 10 gir følgende tall:

$$2^n$$

1 2 4 8 16 32 64 128 256 512 1024

Siden noen reelle tall har uendelig antall siffer vil det bli **avrundingsfeil** når man bruker et begrenset antall siffer. Dette kan gi relativt store feil i iterasjonsprosesser med mange iterasjon.

ASCII kode (American Standard Code for Information Interchange) hadde opprinnelig 2^7=128 mulige kombinasjoner hvorav 95 blir brukt til tall og store og små bokstaver. Dette ble seinere utvidet til 8-bits ASCII. Nå er ASCII delvis erstattet av **Unicode** (http://www.unicode.org/charts/)
UTF-8 er kompatibel med ASCII.
UTF-16 er 16 bits (2 byte) og gir 0-65535 tegn, men det finnes flere forskjellige typer UTF-16

$$2^{16} = 65536$$

UTF-32 er 32 bits og gir følgende antall tegn:

$$2^{32} = 4294967296$$

I sikkerhetskoder kan det brukes 128 bits nøkkel som gir antall kombinasjoner:

$$2^{128} = 3.402824 \cdot 10^{38}$$

Det finnes flere typer filutvidelseskoder e.g. .html, .jpg, .doc, .xls, .pptx, .mp3
Den første regnemaskin (pascaline)basert på tannhjul og gear som kunne addere og subtrahere ble laget av Blaise Pascal (1623-1662) i 1642.

Charles Babbage (1792-1871) dannet det teoretiske grunnlaget for regnemaskiner som realisert som Mark I ved Harvard universitetet på 1940-tallet. Kunne i løpet av 3 sekunder multiplisere to tall med 11 siffer

hver. I 1946 ble datamaskinen ENIAC (Electronic Numerical Inegrator and Computer)inneholdt flere tusen radiorør og ble bygget ved universitetet i Pennsylvania. I løpet av 3 millisekunder ble to 10-siffrede tall multiplisert. Signalene kan ikke overføres raskere enn lyshastigheten $3 \cdot 10^{10}$ cm/sek. 1 nanosekund er 10^{-9} sekund og på den tiden har lyset beveget seg 30 cm. Parallellprosessering.
Vi har et digitalkamera på 2048x1536 piksler, fargedybe 24 bits per piksel. Trenger 3 byte for å lagre en piksel. Da har kameraet følgende antall piksler:

$$2048 \cdot 1536 = 3145728$$

dvs. 3.1 megapiksler
Det betyr 27 bilder på en 256 MB minnebrikke
dots per tomme, dpi- dots per inch, en tomme er =2.54 cm
Ifm med minnebrukker brukes 1 byte=250 kombinasjoner. 1GB brikke lagrer ca. 982 MB.

Klassetall

Klassetallene *h(d)* er tall av typen

$$a + b\sqrt{-d} \qquad d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

Klassetall har tilknytning til Fermats siste sats og eliptiske kurver.
Det betyr for eksempel at tallet 6 kan faktoriseres på forskjellige måter:

$$6 = 2 \cdot 3 \qquad 6 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$$

hvor man benytter seg av prinsippet om faktorisering av Gaussheltall:

$$a^2 + b^2 = (a + bi)(a - bi)$$

Den største verdien for *h(d)=k* er for *h(d)*=1 er med *d*=163, *h(d)*=2 gir *d*=427 som største verdi.

Gaussheltall er komplekse tall av formen *a+bi* hvor *a* og *b* er heltall (integer). Gaussheltall er nyttige ved faktorisering. Faktorisering av vanlige heltall gir:

$$a^2 - b^2 = (a + b)(a - b)$$

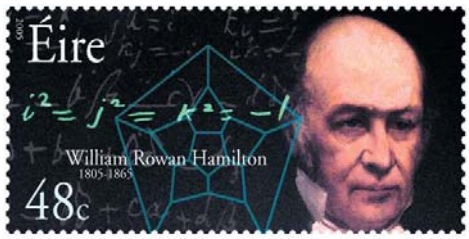
Med Gaussheltall kan faktorisering skje ved:

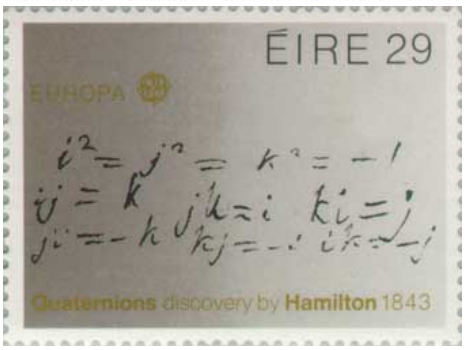
$$a^2 + b^2 = (a + bi)(a - bi)$$

Gaussprimtall er Gaussheltall som ikke kan reduseres til et produkt av Gaussheltall.

Hyperkomplekse tall og kvaternioner

William Rowan Hamilton (1805-1865) ønsket å utvide de komplekse tall fra det todimensjonalt Argand- (Wessel-)plan til et flerdimensjonalt system.





I det todimensjonale kompleksplanet har vi bare en imaginær akse *i* som er lik kvadratroten av -1. Hva med flere imaginære akser ? Det er umulig å lage et slikt system tilsvarende kompleksplanet i tre dimensjoner, men Hamilton laget et komplekssystem for fire dimensjoner, og kalte de komplekse tallene for kvaternioner, samt et for åtte dimensjoner (bikvaternioner,**oktonioner**). Et **kvaternion**, her kalt S, i rommet (*1,i,j,k*) kan uttrykkes som:

$$S = w + ix + jy + kz$$

hvor *w*, *x*, *y* og *z* er reelle tall, og *i*, *j*, *k* følger Hamilton-identiten:

$$i^2 = j^2 = k^2 = ijk = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$$

Vi har nå i stedet tre akser med kvadratroten av -1 (i,j,k). Rekkefølgen av hvordan man multipliserer er avgjørene. Vi ser over at ij=k, mens ji=-k. Kvaternionet til punktet (w,x,y,z) blir

$$w + ix + jy + kz$$

Vi har **enhetskvaternionet**:

$$w^2 + x^2 + y^2 + z^2 = 1$$

som også kan betraktes som en kvaternionkule. Multiplikasjon av to enhetskvaternioner gir et nytt enhetskvaternion. På samme måte som vi

ønsker å finne (retningen, derivere) tangenter til en todimensjonal funksjon, eller tangentfelt til flerdimensjonale funksjoner ved å se på de partiellderiverte (Hesse-matriser), så er man også interessert i å finne tangentplanet for kvaternioner. Vi kan benytte oss av at multiplisering av et enhetskvaternion med et annet gir et nytt enhetskvaterion for å lage akser som står normalt på hverandre i kvaternionrommet.

Oktonioner er 8-dimensjonale, hvor enhetsoktoniet har 7 dimensjoner (7-dimensjonal kule) Se også Cayley-tall. Vi ser nå at vi har tallet 1 for imaginær akse i kompleksplanet, 3 akser i kvaternionrommet og 7 akser i oktonionrommet. Det viser seg at det er bare dimensjonene 1, 3, 7 (og ?) som er paralleliserbare. John Willard Milnor og Michel André Kervaire (1927-2007) har vist at det finnes 28 deriverbare strukturer i det 7-dimensjonale kvaternionrommet. Det er relasjoner til Bouwers hårballteorem: Hvis man har en kule dekket av hår og man forsøker å gre alle flatt så vil minst ett hår stå rett opp (gjelder ikke for en torus, hvor alle hår kan gres flatt).
Vi har regneartene kvaternion multiplikasjon og addisjon, og multiplisering av et kvaternion med en skalar. Det er ikke-kommutativt slik at ij=k, mens ji=-k.
Polynomligninger for kvaternioner kan ha flere løsninger enn graden av polynomet. For eksempel vil $z^2+1=0$ ha uendelig mange kvaternionløsninger. For komplekse tall er det bare i og –i som er lik kvadratroten til -1, mens i H (Hamilton) er det uendelig mange kvadratrøtter av -1.
Hvis Pythagoras setning utvides til 3 dimensjoner legger man grunnlaget for Fermats siste sats. Utvides kompleksplanet (C) med reell og imaginær akse til 3 dimensjoner går ikke dette, men i 4 dimensjoner får man kvaternioner (H), en **4-tuppel**. Så blir det en pause før man i åtte dimensjoner har man **oktonier** (O), en **8-tuppel**. Oktonier ble oppdaget av John T.Graves i 1843, han kalte dem oktaver, men uavhengig ble de også oppdaget av Arthur Cayley, og kalles også Cayley-tall.
R-pakken onion kan brukes til å studere kvaternioner og oktonier
Et kvaternion q er definert som en reell skalar q_0 og en vektor $q=(q_1,q_2,q_3)$.
Den ortonormale basis (1,i,j,k)er gitt ved 1=(1,0,0,0), i=(0,1,0,0), j=(0,0,1,0) og k=(0,0,0,1) og kvaternionet q blir således:

$$q = q_0 + q = q_0 + q_1 i + q_2 j + q_3 k$$

Hvor q_0 er den skaralare delen, og $q_1 i + q_2 j + q_3 k$ er den imaginære delen
Et produkt av to kvaternioner blir et nytt kvaternion

x	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	

Kvaternionmultiplisering
Man kan også finne logaritmen og eksponentialfunksjonen til kvaternioner hvor også trigonometriske funksjoner inngår.
Hvis q er et kvaternion:

$$q = q_0 + q = q_0 + q_1 i + q_2 j + q_3 k$$

Så har vi et **komplekst konjugat** q*

$$q^* = q_0 - q = q_0 - q_1 i - q_2 j - q_3 k$$

Norm til et kvaternion ||p|| er en skalar, alltid et ikke-negativt reelt tall, lik kvadratroten av produktet av kvaternionet og dets komplekse konjugat.

$$\|q\| = \sqrt{q^* q}$$

Hvis norm er lik 1 kalles det en enhetskvaternion
Den inverse av et kvaternion q^{-1} er lik:

$$q^{-1} = \frac{q^*}{\|q\|^2}$$

Modulus til et kvaternion er lik kvadratroten av norm
Hvis vi har et kvaternion:

$$q = a + bi + cj + dk$$

så kan norm q også skrives som:

$$\|q\| = \sqrt{qq^*} = \sqrt{q^* q} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Kvaternioner ble erstattet av vanlig vektorregning, men når det gjelder rotasjoner har kvaternioner en fordel og bedre enn vanlige matriser, og har også vært benyttet til navigering, datagrafikk, molekylære dynamikk, samt til høydekontroll i romfartøyer. Vi skal se på hvordan kvaternioner

kan bli brukt til å rotere et 3D-objekt. Vanlig ortasjon i R^3 kan gjøres med en 3x3 ortogonal matrise med determinant lik 1. Imidlertid er kvaterioner velegnet til rotasjoner i R^3.
Eulers rotasjonsteorem sier at en rotasjon av et fast objekt eller koordinatsystem omkring et fast punkt er lik en rotasjon en gitt vinkel θ omkring en fast Eulerakse som går gjennom det faste punktet.

Mengdelære

Georg Cantor (1845-1918) innførte mengdelære. Cantor gjorde det mulig å telle uendelige mengder. Mengde A og B har samme styrke hvis det for ethvert element i A finnes ett element i B (en-til-en korrespondanse).
Bertrand Arthur William Russel satte likhetstegn mellom matematikk og logikk.
Klammeparentes { } angir en mengde, og a∈A betyr at *a* er et element i mengden *A*. **Nullmengden** ∅ inneholder ingenting.
Snittet av A og B (skrevet A∩B) er den mengden som er felles for A og B. Både A og B inntreffer.

$$A \cap B = \{x | x \in A \; og \; x \in B\}$$

Unionen av A og B (skrevet (AUB) er mengden som er i A, B eller i både A og B. Enten inntreffer A eller B eller begge.

$$A \cup B = \{x | x \in A \; eller \; x \in B\}$$

A^t er **komplement** til A, A inntreffer ikke.

Allerede i 1847 forsøkte George Boole (1815-1864) å lage logiske lover, **Booleske lover**. *An investigation of the laws of thought*. Fra disse kan man også si noe om sannsynligheter.
Den kommutative loven:

$$A \cap B = B \cap A \qquad A \cup B = B \cup A$$

Den assoissiative loven:

$$(A \cap B) \cap C = A \cap (B \cap C) \qquad (A \cup B) \cup C = A \cup (B \cup C)$$

Distributive lover:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$$

Dette sees enkelt hvis man tegner et **Venn-diagram** (John Venn (1834-1923).

Hvis A og B ikke innholder felles data så er snittet av A og B nullmengden:

$$A \cap B = \emptyset \quad \rightarrow \quad P(A \cup B) = P(A) + P(B)$$

Mengden *N* som mengden av alle hele tall bestående av liketall og oddetall:

$$N = \{\{2,4,6,8, \ldots..\}, \{1,3,5,7, \ldots..\}\}$$

Bertrand Russel introduserte begrepet "Mengden av alle mengder som ikke er medlem i seg selv".

En mengde som inneholder *n* elementer har 2^n **undermengder**.

Regneeksempler

Astronomi

Solsystemet består av en sol, 8 planeter, 3 dvergplaneter, mer enn 130 måner samt kometer og asteroider (flest mellom Mars og Jupiter). Det er 4 små indre steinplaneter (Merkur, Venus, Jorden, Mars) og 4 store ytre gassplaneter bestående bl.a. flytende hydrogen og helium (Jupiter, Saturn, Uranus, Neptun). Ifølge Keplers 1. lov beveger planetene seg i elipser med sola i et brennpunkt. Jordens baneplan, ekliptikken, heller ca. 7^o i forhold til Solens ekvator. Planetene dreier i samme retning, mot klokka sett fra Jordens nordpol, altså fra vest mot øst, bortsett fra Venus og Uranus som har retrograd rotasjon fra øst mot vest.
Det er kaotisk dynamikk i solsystemet. Helningen til Mars varierer kaotisk. Kaotisk betyr ikke i uorden. Kaotisk betyr irregulær atferd dvs. orden ispedd tilfeldigheter, og systemet er svært følsomt for initialbetingelsene.
Science 283, 5409, 19.mars 1999, 1877-1881.

Solen

Har differensiell rotasjon mellom det indre og ytre 25.4-36 døgn
Radius: 695 000 000 meter
Masse: $1.989 \cdot 10^{33}$ gram

$700 \cdot 10^6$ tonn hydrogen omsettes per sekund= $700 \cdot 10^{12}$ g s^{-1}, gir $695 \cdot 10^6$ tonn helium. Fire hydrogen gir ett helium. Massen til et proton: $1.6725 \cdot 10^{-27}$ kg, massen til en heliumkjerne: $6.644 \cdot 10^{-27}$ kg

$4 \bullet 1.6725 \cdot 10^{-27}$ kg- $6.644 \cdot 10^{-27}$ kg= $4.6 \cdot 10^{-29}$ kg
Vi finner hvor mye energi dette tilsvarer ved bruk av E=mc2

$E= (4.6 \cdot 10^{-29}$ kg$) \cdot (9.0 \cdot 10^{16}$ $m^2/s^2) = 4.14 \cdot 10^{-12}$ J
1 J = 1 kg m^2/s^2.
Solen sender ut $3.85 \cdot 10^{26}$ J s^{-1} (luminisitet)
$3.85 \cdot 10^{26}$ J $s^{-1}/4.14 \cdot 10^{-12}$ J/reaksjon = $9.29 \cdot 10^{37}$ reaksjoner/s

$4.6 \cdot 10^{-29}$ kg/$6.644 \cdot 10^{-27}$ kg= 0.069
dvs. ca. 0.7% av massen til hydrogen blir omdannet til energi.
Ca. 10% av Solens masse er tilgjengelig for å bli omdannet til energi.
Solen taper masse tilsvarende $1.353 \cdot 10^{20}$ g år. Overflatetemperatur: 5800 Kelvin, solflekker: 3800 K
Solvind med elektroner og protoner beveger seg 450 km/sekund.
Massetap på Solen i løpet av 5 milliarder år ($5 \cdot 10^9$ år)
$1.353 \cdot 10^{20}$ g år$\cdot 5 \cdot 10^9$ år= $6.765 \cdot 10^{29}$ g.

Månen

Beveger seg rundt jorda i samme plan som jorda
radius:$1.738 \cdot 10^6$ meter
Masse:$7.35 \cdot 10^{25}$ gram
Tid mellom to nymåner:29.5 dager, noe som er kortere enn omøpstiden i forhold til stjernene, fordi Jorden flytter seg samtidig i sin bane.
Gravitasjonskreftene mellom jord, måne og sol gir tidevann (flo og fjære), hver av dem ca. to ganger i døgnet. Gravitasjonen kraftigst på siden som vender mot månen, utbuling mot månen og tilsvarende på motsatt side, mest der det er vann. Jorden roterer mye raskere enn månen, noe som gir ca. 2 flo og 2 fjære per døgn. Jordrotasjonen gir flytting utbulingen framover i forhold til linjen jord-måne, noe som gjør at kreftene mellom jord og måne ikke befinner seg nøyaktig mellom tyngepunktene. Dette gir et dreiemoment på jorden og akselleras jon på månen, rotasjonsenergi overføres fra jord til måne, noe som gjør at rotasjonen av jorda forsinkes ca. 1.5 ms/100 år og øker avstand mellom jord-måne ca.

3.8 cm/år. Denne assymmetrien gjør at månens rotasjon ble forsinket av jorden, (jordrotasjonen forsinkes også av månen)slik at omløpstid ble tilnærmet lik rotasjonstid, =bundet rotasjon, samme side vender mot jorda hele tiden. Nå er systemet stabilisert

Keplers lover

Johannes Kepler(1571-1630) basert på Tycho Brahe´s observasjoner.
Keplers først lov: plantene følger elipser med sola i det ene fokalpunktet.
Keplers andre lov: en linje mellom planet og sol sveiper over like arealer per tidsenhet. Betyr at planetene beveger seg raskere når de er nærmest Solen.
Keplers tredje lov: kvadratet av omløpstiden til planeten er proporsjonal med solavstanden i tredje.
Elipser i stedet for episykler. Newton: gravitasjonsloven invers kvadratlov.

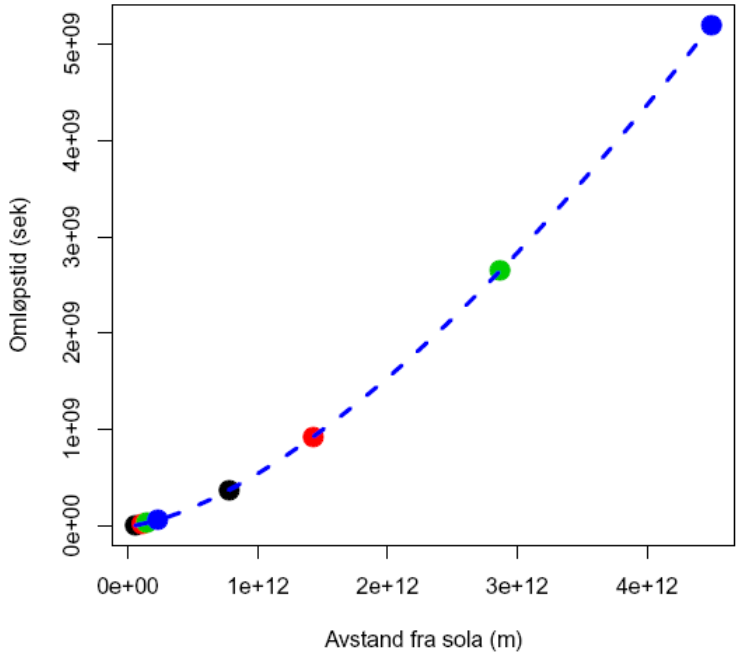
Planet	Masse m	Radius r	Fra sol	Omløpstid	eksentris
	gram	meter	meter	sek	Sirkel=0
Merkur	$3.30 \cdot 10^{26}$	$2.439 \cdot 10^{6}$	$57.91 \cdot 10^{9}$	$7.6 \cdot 10^{6}$	0.206
Venus	$4.87 \cdot 10^{27}$	$6.052 \cdot 10^{6}$	$108.2 \cdot 10^{9}$	$1.94 \cdot 10^{7}$	0.0068
Tellus	$5.98 \cdot 10^{27}$	$6.378 \cdot 10^{6}$	$149.6 \cdot 10^{9}$	$3.15 \cdot 10^{7}$	0.0167
Mars	$6.42 \cdot 10^{26}$	$3.397 \cdot 10^{6}$	$227.94 \cdot 10^{9}$	$5.93 \cdot 10^{7}$	0.0934
Jupiter	$1.90 \cdot 10^{30}$	$71.492 \cdot 10^{6}$	$778.33 \cdot 10^{9}$	$3.74 \cdot 10^{8}$	0.0485
Saturn	$5.69 \cdot 10^{29}$	$60.268 \cdot 10^{6}$	$1426.94 \cdot 10^{9}$	$9.29 \cdot 10^{8}$	0.0556
Uranus	$8.69 \cdot 10^{28}$	$25.559 \cdot 10^{6}$	$2870.99 \cdot 10^{9}$	$2.65 \cdot 10^{9}$	0.0472
Neptun	$1.02 \cdot 10^{29}$	$24.764 \cdot 10^{6}$	$4497.07 \cdot 10^{9}$	$5.2 \cdot 10^{9}$	0.0086

masse: masse i gram
radius: radius i meter ved ekvator
avstand: avstand fra sola i meter
periode: omløpstid i sekunder
eksentrisitet i banen

Planet	AU	Tetthet
		g/cm^3
Merkur	0.38	5.44
Venus	0.72	5.23

Tellus	1.00	5.52
Mars	1.52	3.95
Jupiter	5.20	1.30
Saturn	9.54	0.68
Uranus	19.2	1.21
Neptun	30.1	1.65

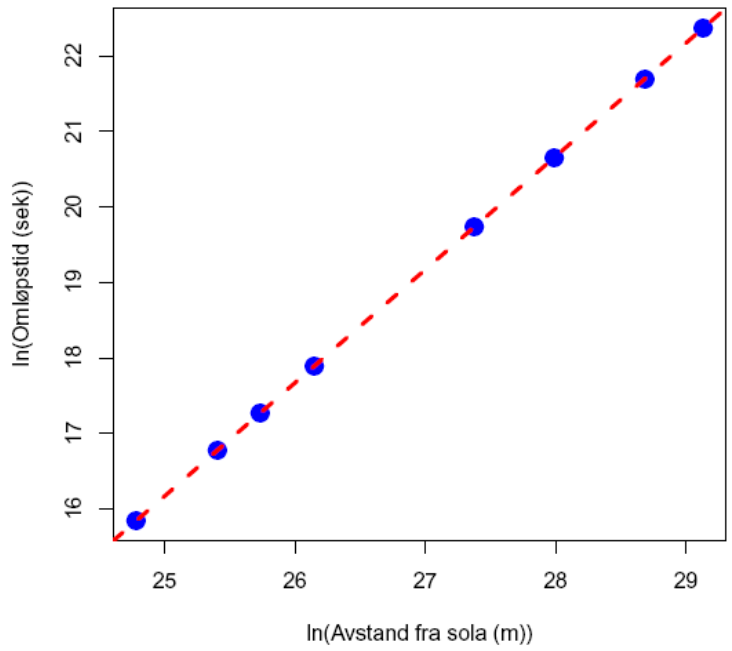
AU: avstand fra Solen, astronomisk enhet
tetthet: tetthet i g/cm^3



Tilpasse en funksjon for perioden (omløpstid):

$$periode = a \cdot avstand^b$$

$$ln(periode) = lna + b \cdot ln(avstand)$$



ln(periode) = -2.132 +1.5·log(avstand)

Ifølge Keplers 3. lov er periode^2/avstand^3=konstant, og det ser vi stemmer

Elektrisitet

Stephen Gray (1670-1735) oppdaget forskjellen melom ledere og isolatorer. Benjamin Franklin (1698-1790) kunne lede lyn, via en drage sendt opp i tordenvær, ned i en Leidnerflaske.
Hans Christian Ørsted (1777-1851) fant at elektrisk strøm i en ledning gir utslag på en kompassnål.
William Gilbert (1544-1603) studerte magneter, og mente Jorden var en magnet (*De magnete*), og la grunnlag for konstruksjonen av Birkelands Terella. Jern har magnetiske egenskaper, en dipol med N og S.

Elektrisitet er strøm av elektriske ladninger. Elektron betyr rav (fossil størknet harpiks), navn fra gnidningselektrisitet (statisk elektrisitet) ved å gi rav med ulltøy. Strømmen kan være likestrøm (DC), eller vekselstrøm (AC) hvor strømmen skifter retning. Strøm av elektroner måles i ampére (A), elektrisk potensial måles i volt (V). Det er proporsjonalitet mellom potensialforskjellen over en leder og strømmen (ladninger per tidsenhet,I)som går gjennom den, Ohms lov, hvor R er elektrisk motstand (resistanse) målt i ohm (Ω):

$$V = IR \qquad I = \frac{V}{R}$$

Oppkalt etter Georg Simon Ohm (1789-1854) som gjorde matematisk analyse av elektrisitet. Konduktanse er den inverse av resistanse, 1/R. Resistansen påvirkes av materialet størmmen går igjennom. Resistansen er proporsjonal med lengden, L, av lederen, og omvendt proporsjonal med tverrsnittet,S. Resistivitet (spesifikk resistivitet) ρ er en konstant spesifikk for materialet:

$$R = \rho \frac{L}{S}$$

Allesandro Volta (1745-1827) laget et galvanisk batteri, en voltasøyle bestående av alternerende lag med plater av zink og kobber atskilt med tøystykker med svak svovelstyre.

Hvis spenningen er 240 V og strømstyrken 10A er motstanden 24 ohm. Elektrisk kraft er energi per tidsenhet:

$$P = VI = \frac{V \cdot V}{R} = \frac{V^2}{R}$$

20V og 1.5 A gir 30 W.
12 V batteri og motstand 24 ohm gir kraft 6 W og strømstyrke 0.5 A.

Luigi Galvani (1737-1798) studerte bioelektrisitet i elektriske skater, og fant at strøm kan gi sammentrekning av lårmuskelen hos frosk.

André Marie Ampère (1775-1836) skrev *Théorie des phenomènes electrodynamiques* (1826), og viste at hvis det ble sendt strøm gjennom et par parallelle ledere så vil lederne frastøte hverandre hvis strømmen sendes i motsatt retning i de to lederne, og de vil tiltrekke hverandre hvis strømmen sendes samme vei. 1 ampéré-sekund (As) er lik 1 coulomb (C). Ampéré-time (Ah) er elektrisk ladning, 1 ampéré i kretsen i 1 time, 1Ah=3600 C.

Michael Faraday (1791-1867) oppdaget elektromagnetisk induksjon. Elektrisk strøm gir et magnetfelt, og strøm gjennom en spole gir en elektromagnet.
Hvis en magnet påvirker en spole kan det lages elektrisk strøm, basis for dynamoen. Polariasjonsplanet kan dreies av et magnetfelt (Faraday effekt). Faradays konstant 96485 coulomb/mol angir ladningen av ett mol elektroner eller protoner. Faradays bur.

James Clerk Maxwell (1831-1879) viste med fire differensialligninger at det er kobling mellom elektrisk strøm, magnetisk felt og ladning. Ladning i bevegelse (elektrodynamikk) gir et elektrisk felt og Maxwell kunne matematisk forklare Faradays magnetiske og elektriske krefter.
Lys er elektromagnetiske bølger med en elektrisk og magnetisk vektor.
Elektrisk strøm i ro gir statisk elektrisitet.

Hvis man kveiler opp en leder i spiral blir det en spole eller solenoide (gr. solen-rør,oides lik), og sender strøm gjennom den oppfører den seg som en magnet, en elektromagnet. Rundt alle strømførende ledere er det et magnetfelt.

Nikola Tesla (1856-1943) utviklet teorien for vekselstrømsmotoren og flerfasestrøm. Tesla er måleenhet for magnetisk flukstetthet. Trefasestrøm kommer fram til de fleste hus i Norge, men inne er det vanligvis kontakter for tofasestrøm. Trefase i Norge inneholder 4 ledninger, hvorav en jordledning som ikke brukes. I utlandet har trefasestrøm fem ledninger. Hvis en metallplate omkveilet med en spoleformet leder festet til to metallringer roteres mellom N- og S-polen på en magnet, skjæres de magnetiske feltlinjene. Det blir indusert en strøm som ledes videre via børster, og dette blir vekselstrøm ettersom feltlinjene skjæres i forskjellig retning når platen roterer. Skal det lages likestrøm brukes det i stedet en kommutator i stedet for de to metallringene. Kommutatoren er delt i to deler med et mellomrom, og børster festes til en positiv del, den andre børsten til en negativ del. En trefasemotor gir et magnetfelt som dreier motoren og den trenger ikke børster og kommutator. Kommutator på tofasemotorer er en ring med kobberlameller rundt akselen på motoren som står i kontakt via kullbørster. Frekvensen i vekselstrømmen er 50-60 Hz, i fly 400 Hz. Vekselstrømmen har den fordelen at den kan transformes til høy spenning som kan overføres over lange avstander uten stort energitap.

Coulombs lov: De elektrostatiske kreftene som virker mellom to ladninger q_1 og q_2 er proporsjonalt (k=9.0·10^9 N m^2 C^{-2}) med produktet av ladningene og omvendt proporsjonal med kvadratet av avstanden r mellom dem.

$$F = \frac{k \cdot q_1 \cdot q_2}{r^2}$$

Oppdaget av Charles Augustin de Coulomb (1736-1806).

Retningen på de elektriske kreftene er avhengig av fortegnet på ladningene q_1 og q_2. Ladningen på et elektron eller proton er $e=1.60\cdot10^{-19}$ C.
I hydrogenatomet er det et negativt ladet elektron (masse $m_1=9.11\cdot10^{-31}$ kg) som beveger seg i sirkelbane med radius $5.29\cdot10^{-11}$ m rundt et positivt ladet proton (masse $m_2=1.67\cdot10^{-27}$ kg).
Kreftene som tiltrekker hverandre er:

$$F = \frac{k \cdot e^2}{r^2} = 9 \cdot 10^9\ Nm^2C^{-2} \cdot \frac{(1.6 \cdot 10^{-19}C)^2}{(5.29 \cdot 10^{-11})^2} = 8.23 \cdot 10^{-8}N$$

Ved vekselstrøm kan spenning (V), strøm (I) og impedanse representeres som vektorer i kompleksplanet. Fasevektorne følger en sinusbølge med amplitude (topp) og vinkelfrekvens omega (ω). I en AC-krets kommer ikke spenning og strøm på topp til samme tid, det er en faseforskjell. Man kan angi vinkelen som spenningen kommer før strømmen. Elektrisk impedanse Z i en AC-krets er det komplekse ratio Z=V/I. Z er

$$Z = |Z|e^{i\theta} \qquad Z = R + ix \qquad V = IZ = I|Z|e^{i\theta}$$

$$V = |V|e^{i(\omega t+\theta)}$$

hvor |Z| ratio spenningsforskjellamplitude/strømamplitude. Omega (ω) er vinkelfrekvens til signalet laget fra spennings- eller strømkilde, t er tid, theta (θ) er initiell fase for henholdsvis strøm og spenning.

Gravitasjon og akselleresjon

Gravitasjonskreftene som virker mellom massene m_1 og m_2 med avstand *r* mellom dem er lik:

$$F = -\frac{Gm_1m_2}{r^2}$$

G er **gravitasjonskonstanten** $6.67 \cdot 10^{-11}$ N m^2 kg^{-2}.
Hvor sterke er gravitasjonskreftene som virker mellom et elektron og proton ?

$$F = -\frac{Gm_1m_2}{r^2}$$

$$= -6.67 \cdot 10^{-11}\, Nm^2kg^{-2} \cdot \frac{(1.67 \cdot 10^{-27}kg) \cdot (9.11 \cdot 10^{-31}kg)}{(5.29 \cdot 10^{-11})^2}$$

$$= 3.63 \cdot 10^{-47}N$$

altså helt neglisjerbart.
I atomær skala er gravitasjonskreftene uten betydning.

Enheten for kraft er newton (*N*). Gravitasjonskraften som vikrer på et objekt kalles vekt (*w*). Massen til et objekt er vekten dividert på tyngdens akselleras jon (*g*).

$$m = \frac{w}{g} \qquad w = m \cdot g$$

Enheten for masse er kg

$$1N = 1\ kg\ m\ s^{-2}$$

Et objekt med gravitasjonsmasse 1 kg veier 9.8 N

$$w = m \cdot g = 1kg \cdot 9.8\ m\ s^{-2} = 9.8\ N$$

Vekten av en kvinne med masse 60 kg har vekt 60·9.8=588 N. Vekten balanseres av et motsatt rettet kraft som er like stor som vekten.

Tetthet ρ er masse dividert på volum målt i kg m^{-3}:

$$\rho = \frac{masse}{volum}$$

Newtons første lov: Et objekt som er i hvile fortsetter å være i hvile. Et objekt i bevegelse fortsetter å bevege seg i rett linje med konstant hastighet.

Newtons andre lov: Kraft (*F*) er masse (*m*)·akselleras jon (*a*):

$$F = m \cdot a$$

Hastigheten *v(t)* til et objekt som beveger seg i rett linje funksjon av tiden er:

$$v(t) = \frac{dx}{dt}$$

Objektet endrer også posisjon og forflytningen langs linjen er i tidsintervallet [a,b]lik:

$$forflytning = \int_a^b v(t)dt$$

Hvis hastigheten endrer seg med tiden kalles det akselleresjon *a(t)* Hvis *a(t)*>0 så øker hastigheten og er *a(t)*<0 så minsker hastigheten:

$$a(t) = \frac{dv}{dt} = \frac{d^2x}{dt^2}$$

Forandring i hastighet i tidsintervallet [a,b] kan uttrykkes som et integral:

$$endring\ i\ hastighet = \int_a^b a(t)dt$$

Hvis vi har et objekt som beveger seg med hastighet *v(t)* langs x-aksen så vil objektet befinne seg ved posisjon *x*, hvor a og v_0 er konstanter:

$$x = v_0 t + \frac{1}{2}at^2$$

Hastigheten til objektet *v(t)=dx/dt* blir:

$$v(t) = \frac{dx}{dt} = v_0 + at$$

Hvis et objekt faller og bare påvirkes av tyngdens akselleresjon (*g=9.8 m/s*^{2}) så blir:

$$\frac{dv}{dt} = \frac{d^2x}{dt^2} = -g \qquad v(0) = v_0$$

Vi løser differensialligningen. Hastigheten ved t=0 kalt v_0 er lik integrasjonskonstanten c og vi får:

$$v = gt + v_0$$

Forflytningen, her kalt høyden h, er lik integralet av hastigheten (se over):

$$h = \int (gt + v_0)dt = \frac{1}{2}gt^2 + v_0 t + h_0$$

Hvis vi slipper en stein fra høyden h_0 over bakken så vil høyden til steinen etter *t* sekunder være gitt ved:

$$h(t) = h_0 - 4.9t^2$$

Den deriverte av av høyden (*h´(t)*) blir lik hastigheten i meter per sekund:

$$h'(t) = -9.8 \cdot t$$

Hvis vi kjenner hastigheten til et fallende objekt så kan vi finne høyden ved integrering.

En person som har masse 70 kg vil ha tyngen 686.7 N hvor 9.81 ms^{-2} er tyngdens akselleresjon
70 kg ·9.81 m/s^2= 686.7 N

$$1N = \frac{1\ kg\ m}{s^2}$$

Effekt i Watt (W) er lik joule (J) per sekund (s)(James Watt 1736-1818)

$$W = \frac{J}{s} = \frac{Nm}{s} = \frac{kg\ m^2}{s^3} = V \cdot A$$

Kraft måles i Newton(N)

$$1N = \frac{1\ kg\ m}{s^2}$$

Kraften som trekker 1 kg masse nedover er 9.81 N.
Hvis en person med masse 70 kg skal gå opp en stigning på 100 meter trengs følgende energimengde 68670 J

70 kg · 9.81 m/s^2·100 m = 68670 J
Hvis denne stigningen skal gjøres på 10 minutter=10·60s så vil energibehovet være 114 W.

Metabolismen i kroppen på eksistensminimum trenger mattilførsel (fri energi) tilsvarende 2625 kcal per person og døgn. Dette tilsvarer ca. 11 MJ kjemisk energi per person og dag. 1 kalori =4.187 J. Den kjemiske energien omdannes til termisk energi og muskelarbeid.
$2625 \cdot 10^3 \cdot 4.187$= 10990875

Dette tilsvarer varmeproduksjon (effekt) ca. 127W. Har man 10 personer i et rom produserer disse ca. 1270 W varme=1.27kW.

10^3W=kilowatt(kW),10^6W=megawatt(MW), 10^9W=gigawatt (GW), 10^{12}W=terrawatt (TW). Watt er joule per sekund, men ofte regnes det om til timer.

Hydrostatisk trykk

Organismer som lever i vann utsettes for et hydrostatisk trykk *p* ved dybde *h*, uttrykt som kraft per arealenhet, og som skyldes vekten av væskesøylen over dem. Tettheten til vann, δ≈ 1000 kg m^{-3}, og tyngdens akselleras jon g= 9.8 m s^{-2}. Hvis vi har en kubisk vannsøyle med areal A og høyde h, så blir volumet V=A·h.
Vekten av denne vannsøylen blir: V·δ·g= A·h·δ·g
Trykket p ved dybde h blir (1 N=1 kgm s^{-2})

$$p = \delta g h = 9800\, h\, \frac{N}{m^2}$$

Ved en bestemt dybde blir trykket like stort i alle retninger, og trykket øker med ca. 1 atmosfære for hver 10. meter (Pascals lov). Ved 10 meters dybde er det ca. 2 atmosfærers trykk (lufttrykket + 1 atmosfære (10m)).

Radioaktivitet

Nedbrytningen av en radioaktiv nuklide over tid *t* skjer ifølge:

$$x = x_0 e^{-kt}$$

hvor *k* er en nedbrytningskonstant, x_0 er mengden ved tid *t*=0.

Vi kan finne halveringstiden (eller doblingstiden for noe som øker):

$$2x_0 = x_0 e^{kt_{1/2}}$$

Vi forkorter vekk x_0 og tar logaritmen på begge sider:

$$ln2 = -k \cdot t_{1/2} \qquad t_{1/2} = \frac{ln2}{k}$$

Etter kjernekraftulykken ved Tsjernobyl i 1986 ble det bl.a. sluppet ut store mengden cesium-137 (^{137}Cs) som sender ut betastråling (elektroner, e) og gammastråling (γ) og har halveringstid 30 år. Cesium hører med til alkalimetallene og står i samme gruppe som kalium i det periodiske system. Det betyr at cesium og kalium har mange like egenskaper, og er det cesium tilstede vil plantene ta opp cesium, og viderefører dette til beitende dyr for eksempel sau.

$$^{137}_{55}Cs \rightarrow {}^{0}_{-1}e + {}^{0}_{0}\gamma + {}^{137}_{56}Ba$$

 # Nedbrytningskonstant k
log(2)/30= 0.02310491

Vi kan se at i år 2016, 30 år etter ulykken har vi fremdeles halvparten (50%) av opprinnelig mengde e.g. 1 g

$$x = 1 \cdot e^{-0.02310491 \cdot 30}$$

$e^{(-k*30)}$= 0.5
Hvilket betyr at vi kan ha mye ”glede” av denne ulykken med nedforing av sau og reinsdyr (i hvert fall hvis det hadde vært samme tiltaksgrense for rein som for sau) mange år nedover.

I PET-scanning (positron emmisjons tomografi) som brukes innen medisin kan man benytte fluorisotopen F-17 bundet til sukker:

$$^{17}_{9}F \rightarrow {}^{0}_{1}e + \nu + {}^{17}_{8}O$$

Et positron er et positivt ladet elektron og v er et nøytrino.

Lyd og decibelskala

En lydbølge (trykkbølge) som passerer gjennom luft i atmosfæren gir en øyeblikkelig liten sammenpressing av gassene. Det skjer et lite netto varmetap ved sammenpressingen og utvidelsen.
Med den generelle gassloven blir lydhastigheten v:

$$v = \sqrt{\frac{\gamma R}{m} T}$$

hvor R er gasskonstanten 8.314 $JK^{-1}mol^{-1}$, gamma (γ) er spesifikk varmeratio for luft 1.405, m molekylvekt til gassen $29 \cdot 10^{-3}$ kg mol^{-1}, T er absolutt temperatur i Kelvin (K).
Vi ser at lydhastigheten blir bare avhengig av temperaturen, ved 20°C ca. 344 ms^{-1} :

$$v = a\sqrt{T}$$

Lydbølger kan også presse sammen vann, selv om vann er vanskelig sammenpressbart. Lydhastigheten i vann er ca. 1500 m s^{-1}, raskere enn i luft. Derfor kommuniserer sjøpattedyr med lydbølger under vann.

Et ungt menneske har hørsel fra bass med frekvens 20 Hz til diskant 20 kHz.
Herz, 1Hz=$1s^{-1}$, eller fra 10^{-16} W cm^{-2} til 10^{-4}W cm^{-2}.
Dette tilsvarer bølgelengder (λ) fra 17.2 meter til 1.72 centimeter:

$$\lambda = \frac{c}{f} = \frac{344\ m\ s^{-1}}{20\ s^{-1}} = 17.2\ m \qquad \lambda = \frac{344\ m\ s^{-1}}{20\ 000 s^{-1}} = 1.72\ cm$$

En flaggermus kan høre lyd med frekvens opp til 120 kHz. Hva blir bølgelengden ? (Fasit:0.287 cm). Øvre høregrense for hunder (44 kHz), rotter (72 kHz), insekter (100kHz). En menneskestemme har effekt ca. 1 mW.

Lydstyrke (lydintensitet) måles i dB(decibel) på en logaritmisk skala med grunntall 10. Måleenhet ble oppkalt etter oppfinneren av telefonen, Alexander Graham Bel. Lydintensitet (lydtrykket) er effekt per flate. Høregrense, den svakeste lyden vi kan høre med frekvensen 1kHz, hvor øret er mest følsomt, tilsvarer 0dB. Den tilsvarende lydintensiteten ved høregrense, høreterskel, er:

$$I_{min} = 10^{-12}\ W\ m^{-2}$$

Intensiteten (I) til en lydbølge er proporsjonal med kvadratet av amplitude:

$$I = \frac{(\Delta P)^2}{2\rho c}$$

hvor ΔP=amplitude, lydhastighet c= 344 m s^{-1} og lufttetthet ρ=1.20 kg m^{-3}.

Den maksimale amplityden som ikke skader øret er ca. 28 Pa. Atmosfæretrykket er $1.013 \cdot 10^5$ Pa, slik at amplituden blir bare en liten del av lufttrykket. Vi finner *I* som ikke skader øret:

$$I = \frac{(\Delta P)^2}{2\rho c} = \frac{(28Pa)^2}{2(1.20kg\ m^{-3})(344\ ms^{-1})} = 0.9496\ Wm^{-2}$$

Lydnivå β i dB

$$\beta = 10 \cdot log \frac{I}{I_{min}}$$

slik at ørets tålegrense blir 120 dB

Lydnivå, støy, tonehøyde og lydkvalitet er subjektive egenskaper tilkoblet den enkeltes følelesapparat via sentralnervesystemet.

Dobling av effekt eller spenning i en forsterker gir ca. 3dB økning, dB=10·log(2)≈3

Tonehøyde (pitch) er antall vibrasjoner per sekund.

dBm – desibelmeter er sammenlignet med 1mW i en 600Ω krets.

En menneskestemme har effekt ca. 1 mW (1W=1J s^{-1}).

Stemmebåndenes utforming og virkningsmekanisme.

Lydkilde	Lydintensitet	dB
Ubehagelig høy lyd	$I_o \cdot 10^{12}$	120
Rushtrafikk	$I_o \cdot 10^{8}$	80
Livlig klasserom	$I_o \cdot 10^{7}$	70
Hvisking	$I_o \cdot 10^{3}$	30
Skogsus	$I_o \cdot 10^{2}$	20
Høregrense	$I_o \cdot 10^{0}$	0

I_0 (høreterskel)10^{-12} W m^{-2}.

Sterk lyd via smell eller hodetelefoner gir hørselskader.

Tell sekunder fra lynglimt til tordenskrall og beregn tordenværets avstand.

Frekvensfordeling i fuglesang, sangorganet hos fugl.

Lydorgan og hørsel hos fisk og sjøpattedyr.

Klangfarge i blåse- og strenginstrumenter.

Sonar og U-båtleting

Fra et utrykningsbil med sirener som kommer mot oss blir bølgetoppene tettere, frekvensen blir høyere. Når lydkilden beveger seg vekk fra oss blir antall bølgetopper per tidsenhet lavere, frekvensen blir lavere, tonen synker. Dette er doppler-effekt. Prinsippet brukes også i medisinsk diagnostikk, ultralyd. Gjelder også for lys (jfr. Einstein).

Kontinuerlig lyd fra en punktkilde brer seg ut som et kuleskall. Hvis effekten P fra lydkilden for eksempel er 50 mW
så vil energifluksen (per flate- og tidsenhet) på et kuleskall med radius 2 m fra objektet være:

$$I = \frac{P}{4\pi r^2} = \frac{50 \cdot 10^{-3}\, W}{50.26548} \approx 10^{-3}\ \frac{W}{m^2}$$

Richters skala

Det er mange typer bølger: lysbølger, lydbølger, havbølger, flodbølger, tidevannsbølger, jordskjelvbølger, atmosfæriske bølger, trafikkbølger, epidemiologiske bølger og populasjonsbølger. Tsunami er et japansk ord for er spesiell type bølge forårsaket av jordskjelv eller vulkanutbrudd på havbunn eller kystområder, eller via under- eller oversjøisk ras. Bølgelengden for tsunami er svært lang, de beveger seg rakst og det er først når de kommer inn på grunt vann ved kystområder at høyden på bølgen øker dramatisk, ofte med katastrofale følger. Langs Stillehavet er det mange jordplater (platetektonikk og Wegener) som møtes, gnisser og skyves under hverandre, derav mye jordskjelv og vulkansk aktivitet. Eksempler på tsunamier er Thera/Santorini (1450 f.kr.), som utryddet den minoiske kulturen på Kreta (sagnet om Atlantis), Krakatoa (1883) ved Java, Lisboa (allehelgensdag 1755), og Chile (mai 1960).

Richters skala er en standard for å karakterisere styrken på jordskjelv. Man bruker en minimumintensitet som referanse og nullnivå, med amplitude P0 for en seismisk bølge.

$$Richter\ tall = log_{10}\left(\frac{P}{P_0}\right)$$

hvor P er amplituden på den seismiske bølgen man måler og skal bestemme. Økning med 1 på Richters skala tilsvarer 10 gangers økning i amplitude.

Litteratur:

Apostol, T.M. *Calculus* (Vol I + II). Blaisdell Publ. Comp. 1962.

R Development Core Team (2011). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. ISBN 3-900051-07-0, URL http://www.R-project.org/.

Rottmann, Karl: *Matematische Formelsammlung*. Bibliographisces Insitutt. Hochschultaschenbücher-Verlag. 1960.

Wikipedia