GRUNNFORSKNING SKAL IKKE VÆRE NYTTIG. ET EKSEMPEL OM PRIMTALL

Blackeberg, Kungsholmen, Spånga, Åsö, Norra R.

20-22-23 mars 2001, 19-21 mars 2002

Innledning.

grunnforskning

Vi ser stadig krav på at **grunnforskningen** skal være nyttig, og at forskning skal lønne seg for samfunnet. Det vanligste spørsmålet om matematikk er hva den kan brukes til, og på skoler og universitet er bøkene fulle av **motivasjon** og **eksempler**. Krav på nytte og styring av forskning har aldrig ført til betydelige fremskritt. Det har alltid vært nysjerrighet og jakten på det ukjente som har ledet til de vitenskapelige revolusjonene. De tekniske nyvinningene og nytten har vært konsekvenser av grunnforskning og ikke årsaken til den. **Telefonen**, anvendelse av **radiobølger** og **transistorer** er resultatet av forskning, **mobiltelefonen** er utviklingsarbeide. Arbeidet med å gjøre telefoner og datorer mindre og hurtigere er rutinearbeide. Nesten alt som skrives i media om forskning er utviklingsarbeide. For eksempel *genomprosjektet* som ble beskrevet som den største triumfen for forskningen i forrige århundret er bare utvilklingsarbeide. Betydningen av forskning er det få som innser.

nytte

Krav på nytte og lønnsomhet fører den tekniske utviklingen fremover, men i små steg. Med denne formen for rutinearbeide skulle fremskrittene langsomt stoppe opp. De store gjennombruddene som endrer vårt syn på verden og kommer fra grunnforskningen. En fascinerende side ved forskningen er at resultater som blir funnet **uten tanke på praktiske anvendelser** alltid kommer til nytte. Ofte oppdager man anvendelsene lang tid etter at det opprinnelige forskningen blir gjort, og mange ganger krever det geni for å forstå hvordan grunnforskningen skal anvendes. Eksempler på oppdagelser som baseres på matematikk gjort for lang tid siden er **genetikk**, **koder** og **tomografi**. Vi skal her skildre hvordan **offentlig nøkkel** kodning, som anvendes ved all hemmelig overføring av elektronisk informasjon, er basert på et matematisk resultat fra midten av sekstenhundretallet.

anvendelser

offentlig nøkkel

Navn og referenser.

William Shakespeare	1564-1616
Galileo Galilei	1564-1642
Claudio Monteverdi	1567-1643

Frans Hals	1581-1666
Gerolama Frescobaldi	1583-1643
Georg Stiernhielm	1598-1673
Pierre de Fermat	1601-1665
Rembrandt van Rijn	1606-1669
John Milton	1608-1674
Jean Baptiste Molière	1622-1673
Isaac Newton	1643-1727
Carl Friedrich Gauss	1777-1855.

R.D. Carmichael

R.L. Rivest, A. Shamir, L.M. Adleman

W. Alford, A. Granville, C. Pomerance

Referenser:

Neal Koblitz, *A course in number theory and cryptography.* Graduate Texts in Mathematics 114. Springer Verlag, Berlin 1987. ISBN 3-540-96576-9.

R.D. Carmichael, *On composite numbers P which satisfy the Fermat congruence* $a^{p-1} \equiv 1 \pmod{p}$. Amer. Math. Monthly 19 (1912), p. 22-27.

W.R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers.* Ann. of Math. (2) 139 (1994), no. 3, 703–722.

Kodning.

Det har i alle tider vært stort behov av koder. I en mengde situasjoner vil vi kommunisere meddelelser til andre uten at utenforstående skal kjenne til innholdet i meddelelsen. Å kode en meddelelse betyr å skive om den på en slik måte at bare den man vil skal lese meddelelsen kan avkode den til den opprinnelige meddelelsen. Skjematisk har vi

$$\text{Meddelelse} \to \text{Kodning} \to \text{Sending} \to \text{Avkodning}.$$

Koder

I prinsippet er det lett å kode meddelelser. Avsender og mottager kan bare skaffe seg en **kodebok** som ingen andre kjenner til og bruke denne til kodning og avkodning. Spesielt kan den som har kodet meddelelsen selv avkode den. Dette er en brukbare metode om det er få meddelelser som skal sendes mellom et fåtall personer. Ved **e-handel** og bruk av **kontokort** er det et stort antall personer som vil sende kodete meddelelser til en enkelt person. Da kreves en kodningsmetode der alle kan kode, og bare en kan avkode. Spesielt skal senderen selv ikke kunne avkode sin egen meddelelse. Dette kalles **offentlig nøkkel kodning**. Det var lenge et åpent spørsmål om dette var mulig inntil R.L. Rivest, A. Shamir og L.M. Adleman fant en genial medtode for å kode med

RSA

en offentlig nøkkel. Metoden som kalles RSA etter navnene til opphavsmennene er basert på Fermats Lille Sats og på at det er enormt tidskrevende å **faktorisere** hele tall. Fermats Lille Sats er oppkalt etter en av de mest betydningsfulle matematikerne Pierre de Fermat som levde under treveårskrigen. Han var dommer i Toulouse i Frankrike men brukte all sin fritid på matematikken. Fermat har gjort store innsatser i mange deler av matematikken og sannsynlighetsteorien, men er mest kjent for sine oppdagelser i tallteorien. Spesielt er han kjent for sin Store, eller Siste Sats, som egentlig var en formodning som ble vist så sent som i 1995 av R. Taylor og A. Wiles.

Fermats Lille Sats.

residyregning

La n være et positivt heltall. For alle hele tall a og b betyr notasjonen

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

det samme som at n deler $a - b$. Denne notasjonen kan virke underlig, men er fundamental i matematikken. Den ble innført av en av historiens fremste matematikere C.F. Gauss, og reflekterer at vi kan regne med restene av heltall ved divisjon med n på samme måte som vi kan regne med vanlig tall. Du kan selv overbevise deg om dette ved å gjøre følgende oppgave.

Oppgave 1: La n være et positivt heltall.

(1) Vis at for hvert heltall a så finnes det et eneste tall b blandt tallene $0, 1, \ldots, n-1$ slik at $a \equiv b \pmod{n}$.
(2) Vis at om $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n}$ så vil $a + c \equiv b + d$ og $ac \equiv bd \pmod{n}$.
(3) Vis spesielt at om $a \equiv b \pmod{n}$ så vil $a^m \equiv b^m \pmod{n}$ for alle positive heltall m.

Fermats lille

Fermats Lille Sats 2: *La p være et primtall. For hvert tall a som ikke er delbart med p vil*

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

Merk 3: Vi kan også uttrykke Fermats Lille Sats ved

$$a^p \equiv a \pmod{p}$$

for alle tall a.

Eksempel 4: Om $p = 7$ sier Fermats Lille Sats at $a^6 \equiv 1 \pmod{7}$ for alle tall a som ikke er delbare med 7. På grunn av (1) i Oppgaven 1 behøver vi bare kontrollere at dette holder for tallene

$1, 2, \ldots, 6$. Vi har $1^6 \equiv 1 \pmod 7, 2^6 \equiv (2^3)^2 \equiv 8^2 \equiv 1^2 \equiv 1 \pmod 7, 3^6 \equiv (3^2)^3 \equiv 9^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7, 4^6 \equiv (4^2)^3 \equiv 16^3 \equiv 2^3 \equiv 1 \pmod 7, 5^6 \equiv (5^2)^3 \equiv 25^3 \equiv 4^3 \equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$.

Merk 5: Om n er et positivt heltall større eller lik 2 som ikke er et primtall er det ikke alltid sant at vi for hvert tall a har at

$$(*) \qquad a^{n-1} \equiv 1 \pmod n.$$

For det første er det aldrig sant at $(*)$ holder om a og n har en felles faktor d større enn 1, fordi om d deler n må den også dele $a^{n-1} - 1$, og deler den a må den derfor også dele 1 som er umulig. Selvom a og n er innbyrdes primiske behøver ikke $(*)$ å holde, som vi ser av følgende eksempel.

Ekesmpel 6: La $n = 6$. Ligningen $*$ i dette tilfellet er $a^5 \equiv 1 \pmod 6$. Som vi bemerket holder ikke $(*)$ når a og 6 har felles faktorer, det vil si når a er $2, 3$ eller 4. Når $a = 1$ har vi $1^5 \equiv 1 \pmod 6$, men når $a = 5$ har vi $5^5 \equiv (5^2)^2 \cdot 5 \equiv 25^2 \cdot 5 \equiv 1^2 \cdot 5 \equiv 5 \pmod 6$.

Carmichael

Definition 7: Et heltall større enn 1 som ikke er et primtall og som er slik at $a^{n-1} \equiv 1 \pmod n$ for alle tall a som er primiske med n kalles et **Carmichael tall**.

Merk 8: Vi skal senere beskrive en metode basert på Fermats Lille Sats for å finne primtall. Metoden avhenger av at det finnes veldig få Carmichael tall. Det minste Carmichael tallet er 561 og det var først i 1994, etter mange års intens forskning at Alford, Granville og Pomerance kunne vise at det finnes uendelig mange Carmichael tall.

Lemma 9: *La p og q være to ulike primtall og la d og e være to heltall slik at $de \equiv 1 \pmod{(p-1)(q-1)}$. Da har vi at $a^{de} \equiv a \pmod{pq}$ for alle tall a.*

Bevis. Vi kan skrive $de = 1 + m(p-1)(q-1)$ for noe heltall m. Om hverken p eller q deler a følger det av Fermats Lille Sats at $a^{p-1} \equiv 1 \pmod p$ og $a^{q-1} \equiv 1 \pmod q$. Vi får derfor at $a^{de} \equiv a^{1+m(p-1)(q-1)} \equiv a(a^{m(p-1)})^{q-1} \equiv a \pmod q$, og tilsvarende at $a^{de} \equiv a \pmod p$. Med dette betyr at $a^{de} \equiv a \pmod{pq}$.

Om p deler a så deler den a^{de} og derfor er det klart at $a^{de} \equiv a \pmod p$. Derfor holder også Lemmaet om en eller begge primtallene p og q deler a.

RSA kodning.

For å forklare RSA kodningen antar vi at alle meddelelser består av **desimaltall** $a_r a_{r-1} \cdots a_0$ som er mindre enn et gitt heltall n. For eksempel når $n = 143$ vil mulige meddelelser være tallene $001, 002, \ldots, 142$. Vi vil nu kode et gitt tall $P = a_r a_{r-1} \cdots a_0$ mindre enn n til et tall $c(P) = b_r b_{r-1} \cdots b_0$ mindre enn n slik at bare en eneste person kan få tilbake tallet P fra $c(P)$.

Koden får vi ved å ta to primtall p og q og sette $n = pq$. Vi velger et vilkårlig tall e som er primisk med $(p-1)(q-1)$. Da kan vi bestemme et tall d slik at $de \equiv 1 \pmod{(p-1)(q-1)}$. Den **offentlige nøkkelen** er tallene e og n som alle kjenner til. En person kan nu kode meddelelsen $P = a_r a_{r-1} \cdots a_0$ til tallet som er resten av P^e ved divisjon med n. Det vi si, vi har at $c(P) = b_r b_{r-1} \cdots b_0$ er mindre enn n og vi har at $c(P) \equiv P^e \pmod{n}$.

avkodning

Den som skal **avkode** meddelelsen kjenner til d og n. For å avkode meddelelsen $c(P)$ tar mottakeren resten av tallet $c(P)^d$ ved divisjon med n. Det vil si at mottakeren får et positivt tall mindre enn n og dette tallet tilfredsstiller $c(P)^d \equiv P^{de} \pmod{n}$. Men Lemma 9 viser at $P^{de} \equiv P \pmod{n}$. Derfor har mottageren fått tilbake tallet P.

bryte koder

For å kunne avkode en meddelelse med denne metoden må vi kjenne til tallet d. Ettersom vi kjenner e ville dette være lett om vi kjente p og q. Men for å finne p og q må vi faktorisere tallet n. Om n har omkring 400 sifre eller mer kan dette ta tusentalls år, selv med de hurtigste maskiner. Koden kan derfor ikke brytes før vi lærer oss å faktorisere heltall hurtig.

Eksempel 10: Ta $p = 7$ og $q = 11$. Da er $n = 77$ og $(p-1)(q-1) = 60$. Vi velger $e = 13$. Da vil $d = 37$ ettersom $37 \cdot 13 \equiv 481 \equiv 1 \pmod{60}$. Vi har meddelelsene $00, 01, 02, \ldots, 76$. Ta for eksempel meddelelsen $P = 05 = 5$. Den kodes til $c(5) \equiv 5^e \equiv 5^{13} \equiv (5^3)^4 \cdot 5 \equiv 29^4 \cdot 5 \equiv 6^2 \cdot 5 \equiv 26 \pmod{77}$. For å avkode meddelelsen $c(5) = 26$ tar vi $c(5)^d = c(5)^{37} \equiv 26^{37} \equiv (26^2)^{18} \cdot 26 \equiv (17^2)^9 \cdot 26 \equiv -19^9 \cdot 26 \equiv -32 \cdot 19^8 \equiv -32 \cdot 24^4 \equiv -32 \cdot 40^2 \equiv -32 \cdot 60 \equiv 5 \pmod{77}$.

Primtallstesting.

For å konstruere RSA-koder har vi sett at vi må finne store primtall. Dette kan vi også gjøre med Fermats Lille Sats.

Lemma 11: *La n være et positivt tall. Om det finnes et tall a som er primisk med n og er slik at $a^{n-1} \not\equiv 1 \pmod{n}$, da vil minst halvparten av tallene b blandt $1, 2, \ldots, n-1$ også tilfredsstille $c^{n-1} \not\equiv 1 \pmod{n}$.*

Bevis. La $a_1, a_2, \ldots, a_r$ være tallene blandt $1, 2, \ldots, n-1$ som er slik at $a_i^{n-1} \equiv 1 \pmod{n}$. Spesielt vil $a_1, a_2, \ldots, a_r$ være primiske

med n. Vi har at $(aa_i)^{n-1} \equiv a^{n-1}a_i^{n-1} \equiv a^{n-1} \not\equiv 1 \pmod{n}$. Restene til tallene $aa_1, aa_2, \ldots, aa_r$ ved divisjon med n er ulike. Dette er fordi om n deler $aa_i - aa_j = a(a_i - a_j)$, eller $a_i < a_j$ respektive $a_j - a_i$ så må n dele $a_i - a_j$ fordi n er primisk med a. Men $a_i - a_j$ er mindre enn n og større enn $-n$ så det er umulig at n deler $a_i - a_j$. Det finnes altså minst r tall blandt $1, 2, \ldots, n-1$ slik at $b^{n-1} \not\equiv 1 \pmod{n}$.

Primtallstest

La n være et positivt heltall. Ta et slumpmessig tall blandt $1, 2, \ldots, n-1$. Vi sjekker først om b er primisk med n. Er den ikke det kan ikke n være et primtall ettersom den har en divisor. Deretter kontrollerer vi om $b^{n-1} \equiv 1 \pmod{n}$. Er den ikke det følger det av Fermat Lille Setning at n ikke er et primtall. Den eneste muligheten for at n skal være et primtall er følgelig at $b^{n-1} \equiv 1 \pmod{n}$. Det følger av Lemma 11 at om det finnes et eneste tall a slik at $a^{n-1} \not\equiv 1 \pmod{n}$ så er sjansen mindre enn $1/2$ at b skal tilfredsstille likningen $b^{n-1} \equiv 1 \pmod{n}$.

Velger vi slumpmessig tall $b_1, b_2, \ldots$ og vi finner at $b_1^{n-1} \equiv 1 \pmod{n}$, $b_2^{n-1} \equiv 1 \pmod{n}$, $\ldots$, $b_r^{n-1} \equiv \pmod{n}$ så er sjansen for at n skal være et primtall minst $1 - (1/2)^r$, medmindre n er et Carmichael tall. Etter en liten mengde tester finner vi at n enten er **sammensatt**, eller at det er primtall, med **stor sannsylinghet**.