mat

MATILDE

TEMA:
Sandsynlighedsregning

NYHEDSBREV FOR DANSK MATEMATISK FORENING

NR 35 SEPTEMBER 2008

Leder

Af: Bent Ørsted

Temaet for denne måneds Matilde er sandsynlighedsregning; der er forskellige aspekter præsenteret, herunder i artikler af Flemming Topsøe, Jørgen Hoffmann-Jørgensen og Søren Asmussen. Det er bemærkelsesværdigt, så sent teorien for sandsynligheder blev udviklet, og det blev muligt at foretage beregninger med sådanne; samtidig er det et af de mest anvendte matematiske emner i det moderne samfund, hvor stokastiske metoder findes lige fra biologi og genetik til finansiering.

Det er blevet stadig tydeligere, at begrebet stokastisk variabel på mange måder og i mange sammenhænge er mere naturligt og anvendeligt end den klassiske variabel, overleveret fra den græske matematik og dennes størrelseslære. Ligeledes vil vi (eller hvis ikke os, så fremtidens matematikere - man har jo lov at forestille sig matematik også om 1000 år) måske se den klassiske logik erstattet af en anderledes og stokastisk opbygget logik, hvor Cantors mængdelære og den tilhørende Aristoteliske spændetrøje er gået i glemmebogen. Det er i hvert fald rigtigt, at vi i det daglige liv sjældent kan anvende nagelfast logik og være helt sikre på udfaldet af de valg vi foretager: Det vil tage for lang tid at undersøge hver en centimeter af det hus vi er i færd med at købe, sikre os at forsikringer, lån og kommende friværdi er helt rigtige og logisk vandtætte - på et tidspunkt slår vi til, tager chancen, lader intuitionen tage over - og køber hele herligheden.

I en artikel fra 1999 skriver David Mumford om disse ting under overskriften, The Dawning of the Age of Stochasticity; hvor han før arbejdede med (såkaldt) ren matematik, og så på statistik som »kogebogs-nonsens«, er han nu anderledes omvendt (som titlen antyder), arbejder med teorier for det menneskelige syn og den menneskelige intelligens, og ser mange anvendelser og en stor fremtid for sandsynlighedsregning og statistik. Og det er da også ubestrideligt at netop disse fag og deres metoder har haft en stor fremgang i de sidste 20 år, herunder haft succes med at vise nye resultater i ren matematik. Det mest spektakulære er imidlertid stokastiske differentialligninger, hvor altså de optrædende variable igen kan være stokastiske variable.

Her er et citat fra Mumford's artikel (abstract): For over two millenia, Aristotle's logic has ruled over the thinking of western intellectuals. All precise theories, all scientific models, even models of the process of thinking itself, have in principle conformed to the straight-jacket of logic. But from its shady beginnings devising gambling strategies and counting corpses in medieval London, probability theory and statistical inference now emerge as better foundations for scientific models, especially those of the process of thinking and as essential ingredients of theoretical mathematics, even the foundations of mathematics itself. We propose that this sea change in our perspective will affect virtually all of mathematics in the next century.

Javist, her lægges ingen fingre imellem (og der er endda et helt aktuelt ekko af »change«, som vi nok har hørt om i den amerikanske valgkamp); men der er nok noget om snakken. Videre skriver Mumford: ...thought is the weighing of relative likelihoods of possible events and the act of sampling from the »posterior«, the probability distribution on unknown events, given the sum total of our knowledge of past events and present context. If this is so, then the paradigmatic object is not a proposition, standing in all its eternal glory with its truth emblazoned on its chest, but the random variable x, its value subject to probabilities but still not fixed.

Jævnfør her spil, herunder hasard, men også de utallige steder hvor metoder fra sandsynlighed og stokastiske variable har haft indflydelse; vi bringer da her også som eksempel en artikel om arbejder af Green og Tao, især de revolutionerende om fordelingen af primtal i aritmetiske progressioner.

Næste nummer af Matilde vil have som tema, rekreativ matematik - i erkendelse af, at det ikke behøver at være svært for at være sjovt. Eventuelle ideer eller yndlingsrekreationer er velkomne, mon ikke nogle af disse har med spil at gøre?

mat

Matilde – Nyhedsbrev for Dansk Matematisk Forening
medlem af
European Mathematical Society

Nummer 35
September 2008

Redaktion:
Bent Ørsted, Aau
(ansvarshavende og TEMA-REDAKTØR)

Carsten Lunde Petersen, Ruc
Jørn Børling Olsson, Ku
Poul Hjorth, Dtu
Mikael Rørdam, Ku
Carl Winsløw, Ku

Adresse:

Matilde
Institut for Matematiske Fag
Københavns Universitet
Universitetsparken 5
2100 København Ø

Fax: 3532 0704
e-post:
matilde@mathematics.dk
URL:
www.matilde.mathematics.dk

ISSN: 1399-5901

Matilde udkommer 4 gange om året

Indlæg til næste nummer skal være redaktionen i hænde senest fredag 14. november 2008

Tema:
Rekreativ matematik

Indhold:

Forsidefoto: *Blaise Pascal*

Sandsynligheder

af Jørgen Hoffmann-Jørgensen
Institut for matematiske fag, Aarhus Universitet
DK-8000, Aarhus C, Denmark
E-mail:hoff@imf.au.dk

Sandsynligheder
Hvad er de for nogen og hvor kommer de fra?

Sandsynlighedsteoriens opgave er at beskrive, forudsige og regelsætte tilfældige hændelser. Da tilfældige hændelser er karakteriseret ved at de er ubeskrivelige, uforudsigelige og totalt kaotiske, kan sandsynlighedsteoriens opgave formuleres således:

> Beskriv det ubeskrivelige, forudsig det uforudsigelige, og find orden, hvor ingen orden findes.

Så det er noget af en opgave! I det følgende vil jeg fortælle lidt om, hvorledes det lykkedes at løse denne tilsyneladende umulige opgave.

Sandsynlighedsteorien har sin oprindelse i spil. Vi mennesker har spillet lige siden, vi kravlede ned fra træerne og begyndte at gå på to ben. Det første spilleredskab, vi har kendskab til er en knogle, der hedder *astragulus* (den sidder lige over hæleknoglen, og især hos får og andre mindre klovdyr har den en form, som gør den velegnet som terning – den har dog kun 4 sider den kan lande på). De ældste astraglii, man har fundet, og som bærer tydlige tegn på at have været anvendt som spilleredskab, er ca. 50.000 år gamle. Den første (seks-sidet) terning, som vi kender den fra i dag, er ca. 5.500 år gammel, og blev fundet i det nordlige Irak. Dette betyder at vi mennesker har erfaringer med tilfældige hændelser, som rækker mindst 50.000 år tilbage i tiden. Til trods for denne lange erfaringsrække er sandsynlighedsbegrebet forholdsvist nyt (ca. 450 år gammel). I perioden 400 f.kr. til år 0 udviklede grækerne matematikken (algebraen og geometrien) til et meget højt stade, men selv om de havde de nødvendige algebraiske redskaber til rådighed kom de aldrig på tanke, at tilfældige hændelser kunne beskrives med tal. Dette skyldes formodentligt, at de opfattede udfaldet af spil, som et udtryk for Guds, eller gudernes eller skæbnens vijle (en opfattelse, som mange spillere stadig har). Vi skal helt frem til år 1550 før nogen fandt på at sætte tal (odds og/eller sandsynligheder) på udfaldet af et tilfældigt spil.

Gerolamo Cardano (1501–1576) var læge, matematiker, sagfører og meget andet, samt en passioneret spiller. Omkring 1550 kom han på den tanke, at tilfældige spil (terningespil, kortspil etc.) kunne beskrives med tal (odds), og han skrev en bog *Liber de Ludo Alea* ("Bogen om terningespil") om regning med odds og sandsynligheder. Bogen har karakter af en dagbog, hvor han skrev sine daglige opdagelser ned. I begyndelsen af bogen begår han mange fejl, som bliver rettet senere i bogen. Det lykkes ham at finde de to fundamentale regneregler for sandsynligheder:

> **Additionsreglen:** Sandsynligheden for at mindst én af to eksklusive hændelser indtræffer er lig summen af sandsynlighederne. Mere præcist, hvis A og B er *disjunkte*; dvs. $A \cap B = \emptyset$, da gælder:
>
> (a) $P(A \cup B) = P(A) + P(B)$
>
> **Multiplikationsreglen:** Sandsynligheden for at både den ene og den anden af to uafhængige hændelser indtræffer er lig produktet af sandsynlighederne. Mere præcist, hvis A og B er uafhængige, da gælder:
>
> (b) $P(A \cap B) = P(A) \cdot P(B)$

Ud fra disse to regler kan alle andre regneregler kan deduceres. F.eks. forsøgte Cardano at udregne sandsynligheden for at få mindst én 6'er i to slag med en terning. Han første bud var $2 \cdot \frac{1}{6} = \frac{1}{3}$. Senere i bogen konstaterer han, at resultatet er forkert – de to hændelser "6'er i første kast" og "6'er i andet kast" er *ikke* eksklusive, så additionsreglen kan *ikke* benyttes. Ved hjælp af multiplikationsreglen finder han det korrekte resultat $1 - \frac{25}{36}$, og han finder den generelle (og korrekte) formel $1 - (\frac{5}{6})^n$ for sandsynligheden for at få mindst én 6'er i n slag med en terning. Gerolamo holdt sine opdagelser hemmelige, og hans bog blev først læst af andre ca. 150 år efter hans død i 1576. Dette skyldes formodentlig, at han var en passioneret spiller, og da han var den eneste i hele Verden, som han kendskab til odds og sandsynligheder, ville det være uklogt at dele denne viden med andre. Det er tankevækkende, at Gerolamo er den eneste sandsynlighedsteoretiker i historien, som jeg har kendskab til, som var professionel spiller. Årsagen til dette finder vi bedst beskrevet i forordet til Abraham de Moivre's fremragende bog *Doctrine of Chances* (1756):

> *Your Lordship* (her hentydes til de Moivre's velgører, Lord Carpenter) *does easily perceive, that this Doctrine is so far from encouraging Play, that it is rather a Guard against it, by setting in clear Light, the Advantages and Disadvantages of those Games wherein Chance is concerned.*

Sandsynlighedsteoriens beklagelige budskab til alle spillere er: **You can't beat the odds!** Hvis odds er imod dig, så findes der ingen strategier, der kan ændre dette beklagelige faktum. Så hvis du vil gøre spil til din levevej, skal du købe et casino og lade være med at spille på andres casinoer.

Pierre de Fermat (16601–1665) & Blaise Pascal (1623–1662) genopfandt i perioden fra maj 1654 til november 1654 sandsynlighedsteorien i en række breve, hvoraf alle pånær det første brev er bevaret. Det andet brev (fra Fermat til Pascal) begynder således:

> *Monsieur,*
> *Si j'entreprends de faire un point avec un seul dé en huit coups; si nous convenons, après que l'argent et dans le jeu, que je ne jourai pas les premier coup, il faut, par mon principe, que je tire du jeu $\frac{1}{6}$ du total pour être désintéressé, à raison dudit prèmier coup.*

Bemærk, at Fermat fastslår det i dag almindeligt accepterede princip: "Terningen har ingen hukommelse" – et princip som var under debat i flere hundrede år. F.eks. hævdede den franske matematiker d' Alembert, at hvis en terning ikke havde vist en "sekser" i mange kast, så ville sandsynligheden for en "sekser" forøges i de følgende kast. Daniel Bernoulli (1700–1782) opponerede kraftigt mod d'Alembert's synspunkt. De to matematikere diskuterede problemet ihærdigt uden at nå til enighed.

Problemet i Fermat's brev er følgende: Hvad er sandsynligheden for at få mindst én 6'er i 8 slag med en terning? Blaise Pascal havde åbenbart sendt en forkert løsning i det første brev, og i det andet brev løser Pierre de Fermat problemet korrekt: $1-(\frac{5}{6})^8$. I det tredie brev (fra Pascal til Fermat) viser det sig, at Pascal har fundet fejlen og fundet den korrekte løsning før modtagelsen af det andet brev – og han skriver begejstret: "Sandheden er den samme i Toulouse, som i Paris" (Fermat var dommer ved kassationsrettens afdeling for borgelige retssager i Toulouse, og Pascal boede på det tidspunkt i Paris). Fermat var teoretikeren, som fastlagde den grundlæggende model (*Fermat's model)*:

> Hvis, vi har en mængde Ω med N lige sandsynlige udfald $\omega_1, \ldots, \omega_N$, og $A \subseteq \Omega$ er en given hændelse, da er sandsynligheden for A lig antallet af udfald i A divideret med det totale antal af mulige udfald; dvs. $P(A) = \frac{|A|}{N}$, hvor $|A|$ betegner antallet af elementer i A .

Pascal var praktikeren som ved hjælp af Fermat's model udregnede sandsynligheder for lang række hændelser. Bemærk at Fermat's model reducerer problemet med at udregne sandsynligheder til at tælle antallet af mulige udfald i en given hændelse. Ved første øjekast, synes dette at nemt – vi skal jo bare tælle antallet af elementer i en given endelig mængde – men dette ikke altid så let endda; f.eks.: 5 kort udtrækkes tilfældigt og uden tilbagelægning fra et sædvanligt kortspil med 52 kort. På hvor mange måder kan dette gøres, og på hvor mange måder kan disse 5 kort udtrækkes på, så at vi får et "full house" (dvs. 2 ens og tre ens, f.eks. to konger og tre 4'ere)? Pascal opdagede at binomialkoficienten

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k}$$

er lig med antallet af måder man kan udtrække k elementer (uden tilbagelægning) ud af mængde med n elementer; f.eks. kan 5 kort udtrækkes tilfældigt og uden tilbagelægning på $\binom{52}{5} = 2.598.960$ måder. Binomialkoefficienterne var kendt længe før Pascal blev født, men i en ganske anden forbindelse. Hvis vi ganger *binomet* $a+b$ med sig selv ialt n gange, får vi (*binomial formlen)*:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k}$$

Binomial formlen blevet fundet af en arabisk matematiker. Jeg har ikke været i stand til at opstøve navn og årstal, men den kom til Europa engang i 1100–tallet.

Christiaan Huyghens (1629–1695) kom til Frankrig i 1656 for at studere matematik og fysik ved Universitetet i Anger. Før han tog til Anger besøgte han Paris, og der fik han kendskab til Fermat og Pascal's brevudveksling. Hverken Fermat eller Pascal nedskev deres opdagelser i sandsynlighedsteorien i bogform, men Huyghens blev så interesseret i sandsynlighedsteorien, at han skrev den første egentlige lærebog i sandsynlighedsteori *De Ratiociniis in Alea Ludo* ("Hvorledes man ræssonerer i terningespil"). Huyghens opfandt middelværdibegrebet eller i hans terminologi "værdien af min chance". I bogen indfører han middelværdien således:

> Hvis jeg har lige store chancer for at vinde a kr og b kr, da er værdien af min chance lig $\frac{1}{2}\,a + \frac{1}{2}\,b$
>
> Hvis jeg har lige store chancer for at vinde a kr, b kr og c kr, da er værdien af min chance lig $\frac{1}{3}\,a + \frac{1}{3}\,b + \frac{1}{3}\,c$
>
> Hvis jeg har sandsynlighed p for vinde a kr og sandsynlighed $q = 1-p$ for vinde b kr, da er værdien af min chance lig $p\,a + q\,b$

Med disse tre regler går Huyghens udfra at læseren har set systemet og at den almindelige formel for middelværdien af stokastisk variabel X lyder således

> Hvis X kan antage værdien a_1 med sandsynlighed p_1 , værdien a_2 med sandsynlighed p_2 , værdien a_3 med sandsynlighed p_3 etc., da er middelværdien af X lig $a_1p_1 + a_2p_2 + a_3p_3 + \text{etc.}$

Ved hjælp af sit middelværdibegreb, løste Huyghens en række problemer. F.eks. følgende: To spiller spiller α og β kaster på skift to terninger, så at α foretager det første kast. Hvis α opnår en sum på 6 før β opnår en sum på 7, vinder α . Hvis β opnår en sum på 7 før α opnår en sum på 6, vinder β . Hvad er sandsynligheden for at α vinder spillet? Bemærk, at sandsynligheden for at få en sum på 6, henholdsvis 7, i et slag med to terninger er lig $\frac{5}{36}$, henholdsvis $\frac{1}{6}$. Så odds er en smule mindre for α end for β , men α har fordelen at starte, og han kan

vinde allerede i første slag uden at β kommer til at kaste. Huyghens løser problemet på følgende elegante måde:

Lad a være den indsats der spilles om, lad x være β's middelgevinst, hvis α begynder, og lad y være β's middelgevinst, hvis β begynder. Da er $a-x$ lig α's middelgevinst. Hvis α slår, har han sandsynlighed $\frac{5}{36}$ for at vinde her og nu, men hvis han ikke opnår sum 6, går slaget videre til β, og vi er nu iden situation at β begynder. Dette betyder, at $x = \frac{31}{36}\,y$. Hvis β slår, har han sandsynlighed $\frac{1}{6}$ for at vinde her og nu, men hvis han ikke opnår sum 6, går slaget videre til α, og vi er nu iden situation at α begynder. Dette betyder, at $y = \frac{1}{6}\,a + \frac{5}{6}\,x$, og vi har to ligninger med to ubekendte:

$$x = \frac{31}{36}\,y \text{ og } y = \frac{1}{6}\,a + \frac{5}{6}\,x$$

Løses disse ligninger, får vi $x = \frac{31}{61}\,a$ og $a-x = \frac{30}{61}\,a$, og da $a-x$ er α's middelgevinst, ser vi at sandsynligheden for at α vinder er lig $\frac{30}{61}$, som stadig er $< \frac{1}{2}$, med dog $> \frac{5}{36}$.

Bemærk, at det ovenstående problem falder langt uden for Fermat's model – der er ingen øvre grænse for antallet af spil (faktisk er det muligt at spillet aldrig bliver afgjort), så der er uendelig mange mulige udfald. Til trods for dette lykkes det Huyghens at udregne den korrekte sandsynlighed.

Jacob Bernoulli (1654–1705) er den næste stjerne på sandsynlighedsteoriens himmel. Han var, som så mange andre i Bernoulli-familien, matematiker, med særlig interesse for sandsynlighedsteori. I sin bog *Ars conjectandi* ("Kusten at gætte") finder han den første af sandsynlighedsteoriens *fire perler*, nemlig den første version af *de store tals lov*. NB: Bernoulli kaldte sætningen for *den gyldne sætning*. I en moderne udgave lyder *de store tals lov* således

Theorem 1 (De store tals lov) *Lad $X_1, X_2, \ldots$ være en følge af uafhængige stokastiske variable med samme middelværdi μ og med varianser, der alle er $\leq c$ for et givet $c > 0$. Lad $S_n = X_1 + \cdots + X_n$ betegne de succesive summer. Da gælder at sandsynligheden for, at gennemsnittet $\frac{S_n}{n}$ afviger fra middelværdien μ med mere end en foreskreven nøjagtighed konvergerer mod nul når n går mod uendelig. Eller på "matematisk":*

$$\lim_{n\to\infty} P\Big(\big|\tfrac{S_n}{n} - \mu\big| > \epsilon\Big) = 0 \;\; \forall\, \epsilon > 0$$

Dette betyder, at hvis n er tilstrækkelig stor, så er gennemsnittet $\frac{S_n}{n}$ et godt bud på middelværdien μ. Men hvad er "tilstrækkelig stor"? Hvis varianserne er $\leq c$, giver *Chebyshev's ulighed* følgende svar

$$P\left(\big|\tfrac{S_n}{n} - \mu\big| > \epsilon\right) \leq \tfrac{c}{n\,\epsilon^2}$$

Så hvis $c = 1$, siger Chebyshev's ulighed at hvis $n \geq 200.000$, da er sandsynligheden for at gennemsnittet $\frac{S_n}{n}$ stemmer overens med middelværdien μ på de to første decimaler større end 95%. Jacob Bernoulli viste sætningen omkring år 1700 i tilfældet, hvor X_n kun antager værdierne 0 og 1 med sandsynlighederne p og $q = 1-p$. Idette tilfælde er middelværdien μ lig p og gennemsnittet $\frac{S_n}{n}$ er lig frekvensen af 1'er i følgen $X_1, \ldots, X_n$. De store tals lov er siden blevet udvidet til en lang række andre situationer og det er ikke længere en sætning, men et stort kompleks af sætninger, som der stadig i dag ydes nye bidrag til. De store tals lov er af umådelig betydning, da den giver os mulighed for at estimere sandsynligheder for komplicerede hændelser, som f.eks. sandsynligheden for at et fragtskib forliser på vej fra København til New York.

Abraham de Moivre (1667–1754) var oprindelig franskmand. Hans familie tilhørte den franske version of protestanter (de såkaldte huguenot'er). I 1685 ophævede den franske konge *ediktet i Nantes* (som var en fredsaftale mellem katolikkerne og protestanterne i Frankrig, som gav protestanterne ret til at udøve deres religion i visse byer i Frankrig). Dette startede en forfølgelse af de franske huguenot'er, og som 18 årig blev de Moivre sat i fængsel. Tre år senere lykkedes det ham at flygte til England, hvor han tilbragte resten af sit liv (Danmark modtog ved den lejlighed et stort antal franske flygtninge, som bosatte sig i Fredericia). Det eneste han medbragte var sin viden og talent for matematik. Han tjente til livets ophold ved at undervise rige folks børn i matematik, men selvom han blev en af sin tids bedste matematikere, opnåede han aldrig af få en stilling ved et af de europæiske universiteter. Han skrev en fremragende og meget pædagogisk lærebog i sandsynlighedsteori *Doctrine of Chances*. Den er speciel ved, at den er skrevet på engelsk, og at den henvendte sig til lægfolk. Bogen indeholder en lang række dybe og svære resultater fra sandsynlighedsteorien.

Lvovich Pafnufty Chebyshev 1821–1884 underviste i sandsynlighedsteori ved universitetet i Moskva. Han indførte begrebet *stokastisk variabel* på følgende måde:

> En stokastisk variabel er en reel variabel, som kan antage forskellige værdier med forskellige sandsynligheder.

og han beviste den berømte ulighed:

> **Chebyshev's ulighed**: Hvis X er en stokastisk variabel med middelværdi μ og varians σ^2, da gælder:
>
> $$P(|X-\mu| \geq a) \leq \tfrac{\sigma^2}{a^2} \;\; \forall\, a > 0$$

Chebyshev's idé var, at en stokastisk variabel er en reel variabel X, som ligger og flyder tilfældigt rundt på den reelle akse, men hvor sandsynligheden $P(X \in A)$ er kendt og givet for "tilstrækkeligt pæne" mængder $A \subseteq \mathbf{R}$ (idag betyder "tilstrækkeligt pæn mængde" en Borel mængde). F.eks. hvis X har tæthedsfunktion $f_X(s)$ og A er en Borel mængde, da er $P(X \in A)$ givet ved

$$P(X \in A) = \int_A f_X(s)\,ds$$

Felix Hausdorff

og hvis X er diskret med sandsynligheds funktion $p_X(s) := P(X = s)$, da er $P(X \in A)$ givet ved

$$P(X \in A) = \sum_{x \in A} p_X(s)$$

Chebyshev's definition er naturligvis upræcis og uden et solidt matematisk grundlag, men definitionen beskriver det væsentlige indhold af begrebet "en stokastisk variabel" langt bedre end den gængse (præcise) definition: en $\mathcal{F}$-målelig funktion. Chebyshev's definition fokuserer på det væsentlige – nemlig at det er fordelingen for X, der er vigtig, og ikke hvad X er for en funktion (dette er også grunden til at vi i sandsynlighedsteorien undertrykker argumentet ω, f.eks. når vi skriver $\{X \in A\}$ i stedet for $\{\omega \mid X(\omega) \in A\}$).

Jeg nævnte ovenfor at de store tals lov er den første af af sandsynlighedsteoriens *fir perler*. De tre andre er *den centralegrænseværdi sætning*, *den iterede logaritmelov* og *arcussinus loven*:

Theorem 2 (Den centralegrænseværdi sætning) *Lad $X_1, X_2, X_3, \ldots$ være en følge af uafhængige stokastiske variable med samme fordeling, endelig middelcærdi μ og endelig varians σ^2. Lad $S_n = X_1 + \cdots + X_n$ betegne partial summen for $n = 1, 2, 3, \ldots$. Da gælder*

$$\lim_{n\to\infty} P\Big(a < \frac{S_n - n\mu}{\sigma\sqrt{n}} < b\Big) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-x^2/2}\, dx \;\; \forall\, a < b$$

Den centrale grænseværdissætning blev først bevist af Abraham de Moivre (ca. 1730) i tilfældet, hvor X_i kun antager vædierne 0 og 1 med sandsynlighederne p og $q = 1 - p$. Dog med integraludtrykket erstattet af en uendelig sum. Løst sagt, siger den centrale grænseværdi sætning at en sum af mange, men "små" uafhængige stokastiske variable, er approksimativt normalt fordelt. Dette er dog en sandhed med modifikationer. Der findes en stor klasse af fordelinger, kaldet de *uendelige delelige fordelinger*, der har denne egenskab, hvor "små" afhænger af fordelingen. F.eks. tilhører eksponential fordelingen, gammafordelingen, Poisson fordelingen og den geometriske fordeling denne klasse, men binomialfordelingen og den uniforme fordeling tilhører IKKE denne klasse. Der er således mange kandidater til "normal fordelingen", men den sædvanlige normal fordeling er i en vis forstand den mest "normale" blandt de mulige kandidater.

Theorem 3 (Den iterede logaritmelov) *Lad $X_1, X_2, X_3, \ldots$ være en følge af uafhængige stokastiske variable med samme fordeling, endelig middelværdi μ og endelig varians σ^2. Lad $S_n = X_1 + \cdots + X_n$ betegne partial summen for $n = 1, 2, 3, \ldots$. Da gælder*

$$P\left(\limsup_{n\to\infty} \frac{S_n - n\mu}{\sqrt{2n\,\log\log n}} = \sigma\right) = 1$$
$$P\left(\liminf_{n\to\infty} \frac{S_n - n\mu}{\sqrt{2n\,\log\log n}} = -\sigma\right) = 1$$

Den iterede logaritmelov er af nyere dato – den blev i sin første udgave vist af Khichine i 1924. Ligesom de store tals lov, er den centrale grænseværdi sætning og den iterede logaritmelov i dag store sætnings komplekser, som der stadig ydes nye bidrag til.

Theorem 4 (Arcussinus loven) *Lad $X_1, X_2, X_3, \ldots$ være en følge af uafhængige stokastiske variable med samme fordeling, middelværdi lig 0 og endelig varians σ^2. Lad $S_n = X_1 + \cdots + X_n$ betegne partial summen for $n = 1, 2, 3, \ldots$ og lad N_n betegne antallet af de første n summer $S_1, \ldots, S_n$, som er strengt positiv. Da gælder*

$$\lim_{n\to\infty} P\Big(a < \frac{N_n}{n} < b\Big) = \frac{1}{\pi} \int_a^b \frac{1}{\sqrt{t\,(1-t)}}\, dt \;\; \forall\, 0 \le a < b \le 1$$

Arcussinus loven blev vist i 1953 af den danske matematiker Erik Sparre Andersen, og er siden blevet udvidet væsentligt. Arcussinus loven har følgende spilteoretiske fortolkning. En spiller deltager i en række uafhængige, identiske og fair spil. Hvis X_n betegner hans gevinst/tab i n'te spil, da er $X_1, X_2, X_3, \ldots$ en følge af uafhængige stokastiske variable med samme fordeling, og da spillet er fair, har vi at middelværdien lig 0. Bemærk at N_n er lig antallet af gange, at spilleren har "ført" i de n første spil, og at $\frac{N_n}{n}$ er den del af tiden at spilleren har "ført" i de n første spil. Arcussinus loven siger nu at $\frac{N_n}{n}$ cirka har tæthedsfunktion givet ved

$$f(t) = \tfrac{1}{\pi}\, \tfrac{1}{\sqrt{t\,(1-t)}} \;\; \forall\, 0 < t < 1$$

Specielt ser vi, at middelværdien af $\frac{N_n}{n}$ cirka er lig $\frac{1}{2}$, hvilket er forventet, da spillene er fair. Da $f(t)$ antager sit minimum for $t = \frac{1}{2}$, ser vi at $\frac{1}{2}$ er den mest usandsynlige værdi for $\frac{N_n}{n}$. Da $f(t)$ konvergerer mod ∞ for t gående mod 0 eller 1, ser vi at med stor sandsynlighed har spilleren enten har ført det meste af tiden eller har været bagud det mest af tiden, og kun sjældent vil spilleren have ført cirka halvdelen af tiden. Dette giver en sandsynlighedsteoretisk forklaring på de velkendte begreber "sidde i held" og "sidde i uheld".

Indtil år 1900 var Fermat's model (men nogle få justeringer) den eneste matematisk præcise model for sandsynlighedsteorien, men anvendelserne gik ofte langt udover modellen. Dette betød, at en stor del af sandsynlighedsteorien savnede et præcise grundlag, og i slutningen af 1800-tallet startede en søgen efter et fast og matematisk korrekt grundlag. Det første forsøg skyldes Émile Borel (i året 1900), som foreslog at bruge enheds intervallet $[0, 1]$ med Lebesgue målet som en model for sandsynlighedsteorien. Borel's forsøg var for uhandigt, og i 1933 kom Andrei Nikolevich Kolmogorov (1903–1991) med den model, der idag stort set er enerådende. I hans berømte bog *Grundbegriffe der Wahrscheinlichkeitsrechnung* fra 1933 opstillede han de fem axiomer for sandsynlighedsteorien:

Lad Ω være en given mængde. Da lader vi 2^Ω betegne mængden af samtlige delmængder af Ω. En delmængde

af 2^Ω kaldes en *brolægning* af Ω. Dvs. en brolægning på Ω er en mængde $\mathcal{A}$ af delmængder af Ω. Hvis $\mathcal{F} \subseteq 2^\Omega$ er en brolægning, da siges $\mathcal{F}$ at være en *σ-algebra*, hvis $\mathcal{F}$ opfylder følgende 3 axiomer:

(1) $\mathcal{F}$ er ikke tom

(2) Hvis $F \in \mathcal{F}$, så vil komplementærmængden $F^c := \Omega \setminus F$ tilhøre $\mathcal{F}$

(3) Hvis $F_1, F_2, \ldots \in \mathcal{F}$, da vil foreningsmængden $\cup_{i=1}^{\infty} F_i$ tilhøre $\mathcal{F}$

Lad $\mathcal{F}$ være en σ-algebra på Ω. Ifølge Axiom 1, findes der en mængde $A \in \mathcal{F}$, og ifølge Axiom 2 har vi $A^c \in \mathcal{F}$. Da $\Omega = A^c \cup A = A^c \cup A \cup A \cup \cdots \cup A \cup \cdots$, har vi ifølge Axiom 3, at $\Omega \in \mathcal{F}$, og da $\emptyset = \Omega^c$, har vi ifølge Axiom 2, at $\emptyset \in \mathcal{F}$. Hvis $F \curvearrowright P(F)$ er en funktion fra $\mathcal{F}$ ind i $\mathbf{R}$, da siges $(\Omega, \mathcal{F}, P)$ at være et *sandsynlighedsrum*, hvis P opfylder følgende 2 axiomer:

(4) $P(\Omega) = 1$ og $0 \leq P(F) \leq 1 \quad \forall F \in \mathcal{F}$

(5) Hvis $F_1, F_2, \ldots \in \mathcal{F}$ er *disjunkte* mængder (dvs. $F_k \cap F_n = \emptyset \ \forall k \neq n$), da gælder $P(\cup_{n=1}^{\infty} F_n) = \sum_{n=1}^{\infty} P(F_n)$

Bemærk, at Axiom 5 er en uendelig udgave af Cardano's addtionsregel, og da $A \cup B = A \cup B \cup \emptyset \cup \emptyset \cdots$, ser vi at Cardano's addtionsregel faktisk er en følge af Axiom 5. Vi er dermed vendt tilbage til udgangspunktet! Bemærk, at Cardano's multiplikationsregel IKKE er medtaget if axiomerne, men den medtages som en *definition*: Lad $A, B \in \mathcal{F}$ være givne hændelser, da indfører vi følgende definition:

- A og B er *uafhængige*, hvis og kun hvis $P(A \cap B) = P(A) \cdot P(B)$

som netop udtrykker Cardano's multiplikationsregel. I Kolmogorov's model defineres en stokastisk variabel således:

- X er en *stokastisk variabel*, hvis og kun hvis X er en funktion fra Ω ind i de reelle tal R, som opfylder $\{\omega \in \Omega \mid X(\omega) \leq t\} \in \mathcal{F} \ \forall t \in \mathbf{R}$

Ved hjælp af disse 5 axiomer og 2 definitioner, kan samtlige sætninger i sandsynlighedsteorien (f.eks. de store tals lov, den centrale grænseværdi sætning, den iterede logaritme lov og arcussinus loven) udledes på logisk korrekt måde. Så Kolmogorov's axiomer har ført sandsynlighedsteorien tilbage til matematikken efter ca 150 år i eksil.

Cardano

Fermat

Sandsynlighed og Information

af Flemming Topsøe
Københavns Universitet
Institut for Matematiske Fag
Universitetsparken 5, 2100 København Ø, Danmark
topsoe@math.ku.dk

Abstract

Formålet med nedenstående tekst er at forberede læseren på det paradigmeskift der er på vej vedrørende tolkning og nyudvikling af væsentlige dele af sandsynlighedsregning og statistik.

1 Hvad er en sandsynlighed?

Efter et livslangt studium af grundlaget for sandsynlighedsregning med tilhørende begreber og fundamentale resultater publicerede de Finetti i 1977 en sammenfattende fremstilling "Theory of Probability", [2] . Den uforberedte læser kan allerede i forordet undrende læse *"probability does not exist"*.

Et nederlag af dimensioner, vil man sige, om en disciplin der netop i den grad er rettet mod at forstå fænomener fra virkelighedens verden – alle de mange fænomener, hvor vi enten af principielle grunde eller på grund af manglende indsigt ikke kan vide, hvilke af flere mulige hændelser vil indtræffe og derfor er overladt til spekulation eller til ofte besværlige eller bekostelige observationer.

Lad os sammenligne med et andet vidensområde, geometrien. Kan man forestille sig, at Euklid som slutstenen på sit virke i geometriens tjeneste kunne have sammenfattet sin indsigt med konstateringen *"sted og form eksisterer ikke"*. Nej, vel?

Det uhåndgribelige ved vore erfaringer omkring stokastiske (tilfældige) fænomener gør det vanskeligt at udkrystallisere systematiske betragtninger, der er velegnede som grundlag for en praktisk anvendelig teoridannelse. Der har altid været – og er stadig – problemer med at nå frem til en forståelse, der kan opnå bred accept.

Er dette nu helt rigtigt? Efter urmenneskets primitive, vel ofte religiøse forestillinger om det tilfældige, efter menneskets mere end tusindårige fascination af spilsituationer, efter mere metodiske overvejelser i renæssancen omkring spil (udregning af odds m.v.) og efter en forfining gennem de sidste ca. 300 år, *var* det ikke netop lykkedes Kolmogorov med det skelsættende arbejde *"Grundbegriffe der Wahrscheinlichkeitstheorie"* [8] fra 1933 at skabe et accepteret fælles teoretisk grundlag for en lang række stokastiske fænomener?[1] Joh, på en måde. Forankringen i målteorien var en kæmpe hjælp, der efter en kort tilvænningsperiode blev grebet med kyshånd af forskerne. Nu endelig fik de fast grund under fødderne og en sand strøm af konsoliderende arbejder til benefice for statistik, forsikringsvidenskab, studiet af stokastiske processer, anvendelser i fysik, økonomi, socialvidenskaberne med mere så dagens lys. "Grundbegriffe's" betydning har været overvældende. Men ret beset er det "blot" en teknisk velfunderet og raffineret metode til at *regne* med sandsynligheder. Og disse regninger må altid baseres på sandsynligheder, der på en eller anden måde er kendte i forvejen. En meget nyttig fremgangsmåde, men, hvor kom sandsynlighederne oprindeligt fra, hvad er det for en slags størrelser, hvad er deres *"inderste sande natur"*, deres *ontologi*? Det sagde "Grundbegriffe" ikke noget om.

Gennem tiderne har der været flere forsøg på svar, men der er stadig ikke konsensus på området, snarere forskellige skoler, der fører sig frem. Vi nøjes her med at pege på ganske få mulige opfattelser. Først Laplace, der, til dels byggende på tidligere betragtninger, fremfører et princip der typisk bunder i *symmetribetragtninger*. Laplace kunne således hævde, at hvis der *ikke er grund til at tro noget andet*, må sandsynlighederne hørende til endeligt mange mulige *hændelser* være lige store, se [11]. Dette er Laplace's *principle of insufficient reason*. En moderne og langt mere vidtrækkende udgave af dette princip finder vi i Jaynes *maksimum entropi princip*, [7], fra 1957. Vi vender siden tilbage hertil og noterer blot her, at Jaynes, der var fysiker, kunne bygge dels på kendte betragtninger fra statistisk fysik (Claudius, Boltzmann, Gibbs) og desuden på den moderne indføring af entropibegrebet i den matematisk/ingeniørmæssige litteratur som var givet nogle år forinden af Shannon i et banebrydende arbejde fra 1948, se [13]. Shannon beskæftiger sig med repræsentation og kommunikation af "information". Vigtig er optimeringsmetoder, der knytter sandsynligheder og information sammen, specielt nævnes, at Shannon opfatter entropi som et talmål for optimal komprimering af data. Det er interessant at Kolmogorov, den moderne sandsynlighedsregnings fader, tog Shannons ideer til sig, videreudviklede dem, specielt med indførelse af et *kompleksitetsbegreb*, og omkring 1970 som konklusion nåede frem til, citeret efter [9], at *"information theory must precede probability theory and not be based on it "*. Så Kolmogorov, der om nogen havde vist vejen til teoretisk sikre manipulationer med sandsynligheder, fandt altså, at der manglede noget, at der var et behov for at grave dybere for at finde frem til sandsynlighedernes "sande natur". Det vil vi tænke nærmere over!

[1] Kolmogorov's arbejde er det vigtigste bidrag til den målteoretisk baserede indgang til sandsynlighedsregning. Som vigtig forudgående forskning må især Hausdorff's *"Grundzüge"* fra 1914 fremhæves, [6], se også Doob's artikel [3].

2 Sandsynlighed og information

For at gennemføre Kolmogorov's program er det en hjælp at udnytte betragtninger omkring *spil*. Det er der sådan set ikke noget nyt i. Spil er ofte blevet brugt til belysning af sandsynlighedsbegrebet[2]. Vi griber det dog lidt anderledes an og skal kun se på to-personers nul-sum spil, endda med specielle roller tiltænkt de to spillere. Den ene spiller repræsenterer *"naturen"*, den anden *iagttageren*. Måske kan figuren hjælpe til at holde styr på tankegangen.

"Naturens" side
Spiller I
kender af sandheden

Iagttagerens side (dig!)
Spiller II
henvist til tro

Iagttageren studerer et bestemt fænomen fra virkelighedens verden. Han må være forberedt på at forskellige muligheder kan indtræffe. Hvorfor skulle han ellers interessere sig for fænomenet? Men der er principielle forskelle på fænomener. Måske drejer det sig om bestemmelse af den specifikke modstand i et materiale. Her forventer iagttageren at nå frem til en bestemt værdi, der kan findes ved måling og bekræftes af andre gennem reproduktion. Anderledes med de principielt stokastiske fænomener. Her kan resultatet af iagttagerens undersøgelser ikke repræsenteres ved en enkelt talværdi. Flere kunne så komme på tale og føres vi så ikke direkte til sandsynligheder? Måske, men der er en mere fundamental måde at tænke på: Netop fordi flere muligheder kan forekomme, ønsker vi at *repræsentere disse* så vi til enhver tid kan holde styr på, hvad der er sket og eventuelt kommunikere iagttagelser videre som det måtte vise sig hensigtsmæssigt. Vi hæfter os ved repræsentation på binær form, velegnet til registrering i en computer. Nærmere betegnet vælges *binære koder* som mulige repræsentationer.

Eksempel: En fremmed, der for første gang stifter bekendtskab med det danske er nysgerrig og vil se nærmere på vores sprog. Bogstaverne først! Ikke bare selve bogstaverne – det er jo bare en liste på 29 tegn, hvoraf nogle ganske vist ser lidt sære ud. Nej, han vil også vide, hvad han kan vente sig af et tilfældigt bogstav fra en typisk dansk tekst.

På forhånd aner han ikke noget herom og vælger en repræsentation, der behandler bogstaverne stort set ens. Det er koden κ_0 i Tabel 1. Efter nogen tid finder han ud af at det ikke er så smart og erstatter koden med en anden, koden κ_1. Den virker bedre. Han skal nu bruge mindre tid på registrering, færre bits. Hvor han før skulle bruge de 85 bits 0001100100100010010010001001001001111000011010001101000001101001101011000000110100011 til at repræsentere en interessant tekststump, han faldt over, kan han med den nye kode nøjes med de 68 bits 01100000010000001000001001011010001101101000111010011010100100 – en besparelse på 20%. Begge koder κ_0 og κ_1 er valgt så snedigt, at man altid kan afgøre, hvornår ét kodeord hører op og det næste begynder. Det har vi sikret os ved at sørge for at koden er *præfix-fri*, d.v.s., at intet kodeord i kodebogen er begyndelsen til et andet.

alfabet	κ_0	κ_1
a	00000	1001
b	00001	101100
c	00010	101101110
d	00011	0110
e	00100	000
f	00101	11010
g	00110	1111
h	00111	11011
i	01000	1000
j	01001	10110110
k	01010	01110
l	01011	1100
m	01100	01010
n	01101	0011
o	01110	1110
p	01111	101110
q	10000	10110111111
r	10001	0010
s	10010	1010
t	10011	0100
u	10100	010110
v	10101	01111
w	10110	10110111100
x	10111	10110111101
y	11000	1011010
z	11001	10110111110
æ	1101	0101111
ø	1110	0101110
å	1111	101111

Tabel 1: To koder over det danske alfabet (κ_1 er fra [14])

Repræsentation med prefix-fri koder er en generel praktisk metode, der behandler alle fænomener ens – hvor forskellige de end måtte være i semantisk henseende. Vi kan også tænke på koder som *semantikuafhængige beskrivelser*. Om en kode er god eller dårlig afhænger af forbruget af bits. Dybest set er det kun erfaringen vedrørende det studerede fænomen, der kan fortælle os om en kode er god eller dårlig. At koden κ_1 af de danske bogstaver er fornuftig, kan bl.a. ses af at bogstavet "e" , som vi har erfaring for optræder hyppigere end andre bogstaver, er tildelt det korteste kodeord (000).

Effektiviteten af en kode afhænger af *længden* af kodeordene. Derimod spiller den "indre struktur" af koden ingen væsentlig rolle. At "sandheden" – her den danske befolknings udvikling af sproget frem til nutidens brug – spiller en rolle for effektiviteten er soleklart, men det er noget den fremmede ingen indflydelse har på. Han skal bare tilpasse sig efterhånden som erfaringen giver ham mere indsigt. Valget af metode, her givet ved en kode, bør vælges under hensyntagen til den viden, den *information*, iagttageren til enhver tid har om det studerede fænomen. □

[2]klassisk er overvejelser af Fermat og Pascal, se f.eks. Feller [4]. Nyere overvejelser findes bl.a. i føromtalte bog af de Finetti, [2] og ganske ny er Shafer og Vovk's bog [12], se også anmeldelser og videre diskussion heraf på http://www.probabilityandfinance.com/.

Om længden af ordene i en kode gælder et centralt resultat: Til opgivne naturlige tal $k_1, \cdots, k_n$ (tænk på $n = 29$ svarende til eksemplet) kan man finde en præfix-fri kode med netop disse tal som kodeordslængder, hvis og kun hvis *Kraft's ulighed*

$$\sum_{i=1}^{n} 2^{-k_i} \leq 1 \tag{2.1}$$

gælder. Beviset er let, men ikke det væsentlige her, se [1] eller evt. [15]. Tilfældet med lighedstegn i (2.1) svarer til præfix-fri koder uden overflødige cifre (d.v.s. det er umuligt at slette binære cifre fra koden uden at ødelægge egenskaben om præfix-frihed). Disse koder er derfor dem, der kan optræde som *optimale beskrivelser*. Vi kan nu *definere* sandsynligheder som tal af formen 2^{-k}, der kan optræde i Krafts ligning ((2.1) med lighedstegn). Med en passende approksimationsbetragtning, som vi her forbigår, kan man også indkredse sandsynligheder, der ikke nødvendigvis er negative heltalspotenser af 2. Sandsynligheder er dermed knyttet til *optimale beskrivelser*[3].

Sammenhængen mellem sandsynligheder og kodeordslængder (i en præfix-fri kode uden overflødige cifre) kan, med let forståelige betegnelser, udtrykkes i ligningen $p_i = 2^{-k_i}$ eller, ækvivalent, $k_i = \log \frac{1}{p_i}$ (her har vi brugt totals-logaritmer). Hvis man tager udgangspunkt i sandsynlighederne, er en kode med netop de angivne kodeordslængder *optimal* i den forstand at den *vægtede kodeordslængde* $\sum_1^n p_i k_i$ er minimal. Og minimumsværdien $\sum_1^n p_i \log \frac{1}{p_i}$ er netop den størrelse, Shannon definerede som *entropien* af $(p_i)_{i \leq n}$.

Vi har set, at sandsynligheder kan sættes ind i en større ramme, der omhandler iagttagelse, indhentning af oplysninger og beskrivelse af information på en form der er velegnet til videreforarbejdning og kommunikation. Som Kolmogorov sagde: "Information før sandsynlighed!"

Ganske vist er der en del detaljer, der skal på plads, før den idé, vi har skitseret, er ført frem til et overbevisende nyt fundament for sandsynlighedsregningen. Meget store dele er udviklet i dag, men der er stadig sider af den informationsteoretiske tilgang til sandsynlighedsregning og statistik, der venter på en afklaring. Spændende bliver det at se det større arbejde [5], Peter Harremoës og medforfatter har på bedding – selv håber jeg også at barsle med en samlet fremstilling, der kan støtte det paradigmeskift, der er på vej.

Med Kraft's ligning er et centralt element i relationen mellem information og sandsynlighed på plads. Til yderligere belysning ser vi på *maksimum entropiprincippet*, MaxEnt, indført af Jaynes som omtalt tidligere. Jaynes peger på at i mange situationer kan man udtrykke den *viden* man har om et "system" ved at angive mængden – nedenfor omtalt som *modellen* – bestående af alle sandsynlighedsmål, der er forenelige med ens viden. Hvis det f.eks er symmetribetragtninger der ligger til grund, kan man som model vælge alle sandsynlighedsmål, der er invariante over for den relevante symmetrigruppe. Og ved man intet, kan man tage mængden af samtlige sandsynlighedsmål som model. Jaynes argumenterer for at blandt alle sandsynlighedsmål i modellen bør man hæfte sig ved det mål, der har størst entropi. Det vil være det, der bedst inddrager ens viden eller, sagt på en anden måde, bedst undgår at inddrage forhold, man faktisk ikke ved noget om. Tankegangen harmonerer med konfliktsituationen der er søgt sammenfattet i vores lille figur. Der må man tænke sig, at Naturen stritter imod og modarbejder iagttagerens søgen efter indsigt. Hvis vi forestiller os, at dette ikke var tilfældet, ville det svare til at vi *ville have vidst noget mere* og dette burde vi så have inddraget i modellen. Efterhånden som iagttageren indhenter ny viden, kan flere forhold tages i betragtning ved at indsnævre modellen og opsøge maksimum entropi fordelingen i den nye model som en naturlig repræsentant. Fremgangsmåden finder udstrakt anvendelse i statistisk fysik og i statistik (hvor en videreudvikling af Kullback, se [10], spiller en særlig rolle).

[3] en tak til Peter Harremoës for hjælp med fremstillingen i dette afsnit

3 Konklusion

Hvor ufuldstændig ovenstående skitse end er, peger den frem mod følgende konklusion, delt op i 5 trin:

* For langt de fleste formål *kan* arbejde med sandsynlighedsregning og statistik som hidtil baseres på Kolmogorov's "Grundbegriffe" og det væld af metoder og resultater der er fulgt efter.

* En dybere forståelse af sandsynlighedsbegrebet opnås gennem studiet af "information" , specielt beskrivelser heraf.

* Den igangværende udvikling af sandsynlighedsregning og statistik har allerede vist, omend det ikke er erkendt i bredere kredse, at den klassiske tilgang ofte med fordel kan erstattes af en *informationsteoretisk tilgang*.

* Udviklingen vil uvægerligt føre til et *paradigmeskift*, som dog først vil tage fart med udgivelse af samlede fremstillinger af den informationsteoretiske indføring i det stokastiske univers.

* En forudsigelse: Fra 2020, om ikke før, vil alle respekterede indføringer på området udnytte den informationsteoretiske tilgang som det vigtigste bærende element: *INFORMATION FØR SANDSYNLIGHED!*

References

[1] T. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, 1991.

[2] B. de Finetti. *Theory of Probability*. Wiley, London, 1974. Italian original 1970; see also review by Good, BAMS 83, vol.1, pp.94-97.

[3] J. L. Doob. Kolmogorov's early work on convergence theory and foundations. *Ann. Probab.*, 17:815–821, 1989.

[4] W. Feller. *An Introduction to Probability Theory and its Applications*, volume II. Wiley, New York, second edition, 1971.

[5] P. Harremoës and A. Dukkipati. Probability and Information – Occam's razor in action. Book manuscript, available from http://homepages.cwi.nl/˜ph/Listpub/listpub.pdf, 2008.

[6] F. Hausdorff. *Grundzüge der Mengenlehre*. Verlag Veit & Co, Leipzig, 1914. Reprinted by Chelsea Pub. Co., 1949, 1965.

[7] E. T. Jaynes. Information theory and statistical mechanics, I and II. *Physical Reviews*, 106 and 108:620–630 and 171–190, 1957.

[8] A. N. Kolmogorov. *Grundbegriffe der Wahrscheinlichkeitsrechnung*. Springer, Berlin, 1933.

[9] A. N. Kolmogorov. Combinatorial foundations of information theory and the calculus of probabilities. *Russian Mathematical Surveys*, 38:29–40, 1983. (from text prepared for the International Congress of Mathematicians, 1970, Nice).

[10] S. Kullback. *Information Theory and Statistics*. Wiley, New York, 1959.

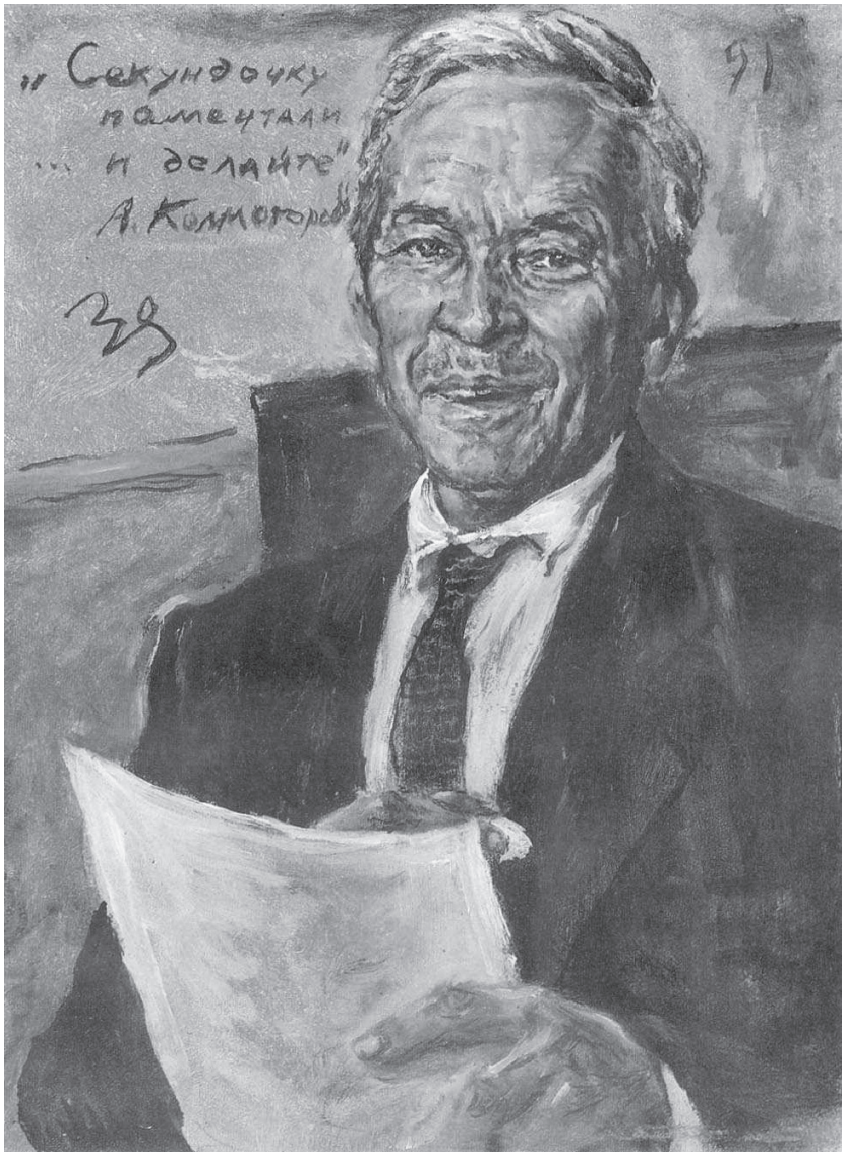
[11] P.-S. Laplace. *Théorie Analytique des Probabilités. Paris, 1812.*

[12] G. Shafer and V. Vovk. Probability and finance. It's only a game! *Wiley, Chichester, 2001.*

[13] C. E. Shannon. A mathematical theory of communication. Bell Syst. Tech. J.*, 27:379–423 and 623–656, 1948.*

[14] F. Topsøe. Informationsteori. *Gyldendal, København, 1973.*

[15] F. Topsøe. Entropy and Codes. In Eichstätter Kolloquium zur Didaktik der Mathematik, vol. 17*, pages 65.1–65.20, 2001. Available at http://www.math.ku.dk/˜topsoe/entropy.pdf.*



Kolmogorov

Forskelligt om risiko

af Søren Asmussen
Institut for matematiske fag, Aarhus Universitet
DK-8000, Aarhus C, Denmark
email: asmus@imf.au.dk

En række af sandsynlighedsregningens vigtigste anvendelsesområder kan sammenfattes under fællesbetegnelsen risikoberegning. Det første substantielle eksemplel var måske de Moivre's ruinproblem (hvad er sandsynligheden for at en spiller går fallit før hans gevinst når et givet mål?), formuleret omkring 1730. Siden formulerede og løste Lundberg og Cramér problemer relaterede til forsikringsrisiko i Sverige i de første årtier af det 20de århundrede. Erlang's resultater fra hans virksomhed på KTAS på omtrent samme tid handler om risikoen for opkald tabte på grund af overbelastning af en central. Siden er kommet beregninger for risikoen for ekstreme vejrsituationer, flykatastrofer, katastrofer på atomkraftværker etc., og på det seneste er emnet risiko (eller snarere eliminering af risiko) blevet centralt i finansmatematik.

Eksemplerne er så mange og problematikken så forskelligartet at studiet af risiko som følge af stokastiske faktorer ikke er et område af homogen karakter, men er spaltet ud i en række delområder, med opdelingen motiveret dels fra anvendelsesområde og dels fra den matematiske metodik. Jeg har her valgt nogle eksempler ud som er taget først og fremmest fra forsikring og finans, men man skal som sagt have for øje at risikoberegning er et langt bredere område.

1 de Moivre's problem

En spiller starter med en kapital på $R_0 = u > 0$ KR (et heltal). Hver gang han spiller (møntkast, sort eller rødt på roulette etc.) enten taber han eller vinder 1 KR. Hans mål er at stoppe når hans kapital er nået op på $v > u$. Spillet indebærer jo imidlertid risikoen for at formuen går ned på 0, i hvilket tilfælde spilleren er ruineret og ikke kan fortsætte. Hvad er sandsynligheden $\psi_v(u)$ at ruineres før målet nås?

For at udregne denne behøver vi som i alle andre sammenhænge en model. Den oplagte her er at udfaldene af på hinanden følgende spil er stokastisk uafhængige med sandsynlighed p for gevinst i hvert. D.v.s. at kapitalen til tid n er $R_n = R_0 + X_1 + \cdots + X_n$, hvor $X_1, X_2, \ldots$ er uafhængige stokastiske variable med sandsynlighed p for $+1$ og sandsynlighed $1-p$ for -1.

Med denne model kan $\psi_v(u)$ let beregnes: ved at betinge med udfaldet X_1 af første spil fås

$$\psi_v(u) \;=\; p\psi_v(u+1) + (1-p)\psi_v(u-1)$$

for $0 < u < v$. Idet vi har de oplagte randbetingelser $\psi_v(0) = 1$, $\psi_v(v) = 0$, ses let at der er entydig løsning givet ved

$$\psi_v(u) \;=\; \frac{\big[(1-p)/p\big]^v - \big[(1-p)/p\big]^u}{\big[(1-p)/p\big]^v - 1} \qquad (1)$$

[for $p = 1/2$ (fair spil) skal dette modificeres til $\psi_v(u) = 1 - u/v$].

2 Cramér-Lundberg teorien

Problemet formuleret af Lundberg og løst af Cramér er at sige noget om sandsynligheden $\psi(u) = \mathbb{P}\big(\inf_{n=1,2,\ldots} R_n \le 0\big)$ for at et forsikringsselskab ruineres før eller senere (her er R_n kapitalen til tid n og $R_0 = u > 0$). Dette ligner altså de Moivre's problem meget, men afviger bl.a. ved at der ikke er nogen øvre grænse v. Dette er dog ikke i sig selv afgørende: vi kan jo blot observere at $\psi_v(u) \to \psi(u)$ for $v \to \infty$, så hvis vi lader $v \to \infty$ i (1) fås

$$\psi(u) \;=\; \big[(1-p)/p\big]^u \qquad (2)$$

[under antagelsen $p > 1/2$ der motiveres nedenfor].

Et alvorligere problem er imidlertid at de Moivre's model med tilvækster X_k på $+1$ eller -1 er alt for simpel i forsikringssammenhængen, hvor X_k er differensen mellem indgående præmier og udbetalte erstatninger i år k. En væsentlig forbedring er derfor at tillade X_k at være en generel stokastisk variabel, lad os sige med Lebesgue tæthed $f(x)$ (vi bibeholder uafhængighedsantagelsen). Videre vil forsikringsselskabet vil næppe sætte sine præmier så det lider et forventet tab, så vi kan nok uden videre gøre antagelsen svarende til $p > 1/2$ ovenfor ($\mathbb{E}$ = forventet værdi),

$$\mathbb{E}X_k \;=\; \int_{-\infty}^{\infty} x f(x)\,\mathrm{d}x \;>\; 0\,. \qquad (3)$$

I denne formulering kan man ret hurtigt komme frem til informative konklusioner. Ruintiden er $\tau = \inf\{n : R_n \le 0\}$ (med konventionen $\tau = \infty$ hvis $R_n > 0$ for alle n), så

$$\psi(u) \;=\; \mathbb{P}(\tau < \infty) \;=\; \sum_{n=0}^{\infty} \mathbb{P}(\tau = n)\,.$$

Her er det enkelte led (i princippet!) blot er et integral: for enhver hændelse A_n kun afhængig af $X_1, \ldots, X_n$ gælder

$$\mathbb{P}(A_n) \;=\; \int\cdots\int_{A_n} f(x_1)\cdots f(x_n)\,\mathrm{d}x_1\,\cdots\,\mathrm{d}x_n$$

(i ruinsammenængen er $A_n = \{\tau = n\} = \{s_1 > -u, \ldots, s_{n-1} > -u, s_n \le -u\}$ hvor $s_k = x_1 + \cdots + s_k$).

Tricket er nu at omskrive dette integral til en forventet værdi i et sandsynlighedsmål $\widetilde{\mathbb{P}}$ hvor tætheden af X'erne ikke er $f(x)$ men $\widetilde{f}(x)$, og hvor dette målbytte fører til noget simpelt. For at definere $\widetilde{f}(x)$ ser vi på den Laplacetransformerede $\widehat{f}[\alpha] = \int \mathrm{e}^{-\alpha x} f(x)\,\mathrm{d}x$ af f. Denne er konveks som blanding af de konvekse funktioner $\mathrm{e}^{-\alpha x}$ af α, og ved at differentiere under integraltegnet ses at $\widehat{f}'[0]$ reduceres til minus middelværdien (3) og altså er < 0 pr. antagelse. For at undgå at blive for tekniske antager vi nu også at f har endelig støtte, f.ex. indeholdt i $[-K, K]$ og at støtten ikke er indeholdt i $[-K, 0]$. Så

$$\begin{aligned}
&\mathbb{P}(\tau = n)\\
=\;& \int\cdots\int_{A_n} f(x_1)\cdots f(x_n)\,\mathrm{d}x_1\,\cdots\,\mathrm{d}x_n\\
=\;& \int\cdots\int_{A_n} L_n(x_1,\ldots,x_n)\widetilde{f}(x_1)\cdots\widetilde{f}(x_n)\,\mathrm{d}x_1\,\cdots\,\mathrm{d}x_n\\
=\;& \int\cdots\int_{A_n} \mathrm{e}^{\gamma s_n}\widetilde{f}(x_1)\cdots\widetilde{f}(x_n)\,\mathrm{d}x_1\,\cdots\,\mathrm{d}x_n\\
=\;& \mathbb{E}\big[\mathrm{e}^{\gamma S_n}; A_n\big]\\
=\;& \mathbb{E}\big[\mathrm{e}^{\gamma S_n}; \tau = n\big] \;=\; \widetilde{\mathbb{E}}\big[\mathrm{e}^{\gamma S_\tau}; \tau = n\big]
\end{aligned}$$

hvor $\mathbb{E}[Z; A]$ står for middelværdien af Z multipliceret med indikatoren for A. Ved at summere over $n = 0, 1, 2, \ldots$ fås derfor

$$\psi(u) \;=\; \widetilde{\mathbb{E}}\mathrm{e}^{\gamma S_\tau}\,. \tag{4}$$

Men pr. definition af τ har vi $S_{\tau-1} > -u$ og $S_\tau \le -u$. Antagelsen om støtten af f (og derfor af $\widetilde{f}$) giver derfor $-u - K < S_\tau \le -u$ og, ved at kombinere med (5),

$$\mathrm{e}^{-\gamma(u+K)} \;\le\; \psi(u) \;\le\; \mathrm{e}^{-\gamma u}\,. \tag{5}$$

D.v.s. *ruinsandsynligheden $\psi(u)$ er af størrelsesorden* $\mathrm{e}^{-\gamma u}$ for store u. Med noget mere arbejde og sofistikering kan man vise Cramér's resultat fra 1930, at under svagere betingelser (bl.a. evt. ubegrænset støtte) findes der en konstant C så

$$\mathrm{e}^{\gamma u}\psi(u) \;\to\; C\,. \tag{6}$$

Dette regnes den dag i dag for en milepæl ikke bare i ruinteorien, men også i teorien for random walks og sandsynlighedsteori i sin helhed. Cramér's bevis var anderledes ligesom til en vis grad modellen: han arbejdede i Lundberg's mere specielle forsikringsmodel hvor man kan udregne den Laplacetransformerede af τ explicit, og anvendte kompleks analyse på inversionsintegralet.

3 Finansmatematik og dens risikoneutrale verden

I dagens finansielle verden handles i stort omfang en række produkter af væsentlig mere kompliceret art end aktier og obligationer, nemlig optioner, swaps etc. Fælles for disse er at produktets afkast beror på udviklingen af andre produkter, og de kaldes derfor med et fælles ord *derivatives*.

Ruinproblemer kommer ind for at beregne priserne på en del sådanne produkter. Et simpelt eksempel er et *equity default swap*, som udbetaler 1 KR hvis prisen på en given aktie går ned under en nedre grænse L i en givet tidsperiode $[0, T]$. D.v.s. det fungerer som forsikring for en aktionær mod store tab. Mere præcist kan vi lade aktieprisen til tid t være $S(t)$ hvor $S(0) > L$ og sætte $\tau = \inf\{t : S(t) < L\}$. Det kan da ikke komme overraskende at prisen for et sådant produkt involverer beregningen af sandsynligheden for at $\tau \le T$. Mere overraskende er at sandsynligheden skal udregnes ikke i den verden vi lever i, men i en *risikoneutral verden*. Denne defineres som en verden hvor risikobelastede (stokastiske) investeringer giver samme forventede afkast som sikre (deterministiske) investeringer [en risikobelasted investering er f.e.x. køb af en aktie, og en sikker er f.e.x. køb af en obligation eller at sætte penge i banken]. D.v.s. at hvis r er bankrenten og $\mathbb{P}^*, \mathbb{E}^*$ sandsynlighed og forventet værdi i den risikoneutrale verden, gælder specielt $\mathbb{E}^* S(t) = \mathrm{e}^{rt} S(0)$. Risikoneutralitet er ikke en typisk situation i den virkelige verden: Hvis f.ex. et forsikringsselskab er stillet overfor at skulle forsikre to skader X, Y med $\mathbb{E}X = \mathbb{E}Y$, vil selskabet normalt kræve mere i præmie for X hvis variansen er større for X end for Y (selskabet er *risikoaverst*). Omvendt kan man argumentere for at en køber af en lottokupon betaler en merpris for den enorme variabilitet der er mellem en indskud og potentielt udbytte (han er risikosøgende).

Den risikoneutrale verden kommer man frem til udfra en række økonomiske aksiomer, der bl.a. indvolverer at finansielle markeder må være fri for *arbitrage*. Her defineres en arbitragemulighed (også kaldet *free lunch*) som en handel hvis endelige udbytte X tilfredstiller $X \ge 0$ men $\mathbb{P}(X > 0) > 0$. Filosofien bag dette aksiom er at virkelighedens markeder sætter sine priser således at der ikke er arbitragemuligheder — ellers har nogen snydt sig selv ved at sætte enten købs- eller salgspris.

For at illustrere tankegangen der fører frem til risikoneutral prissætning ser vi på det måske simplest mulige eksempel, en *en-periodes binomialmodel*, som udsiger at der er to grundlæggende aktiver, en bankkonto og en aktiekurs. Vi kan uden tab af generalitet antage at værdierne til tid 0 er $B(0) = S(0) = 1$. Til tid 1 har vi så $B(1) = \mathrm{e}^r$ hvor r er renten, medens der for aktiekursen antages kun to muligheder $S(1) = u$ (up) eller $S(1) = d$ (down) med sandsynligheder hhv. p og $1-p$ (her antages $d < u$). For at markedet skal være arbitragefrit er det nødvendigt at $d \le \mathrm{e}^r \le u$. Hvis nemlig f.ex. $\mathrm{e}^r < d$, kan man låne 1 KR i banken til tid 0 og købe en aktie for pengene. Til tid 1 skylder man så banken e^r, men kan sælge aktien for mindst d. Da begge er $d > \mathrm{e}^r$, er dette en arbitragemulighed. Tilfældet $\mathrm{e}^r > u$ behandles ved at bytte fortegnet, hvad der kaldes at tage en *kort position* i aktien.

For at illustrere prissætningen ser vi på et finansielt produkt, en option som udbetaler $\Phi\big(S(1)\big) \ge 0$ til tid 1, hvor $\Phi(u), \Phi(d)$ begge er ≥ 0 og mindst én er > 0. Et standardeksempel er en *Europæisk option*, som udbetaler $S(1) - K$ KR hvis aktieprisen $S(1)$ er over et givet niveau $K \in (u, d)$ og ingenting ellers. D.v.s. $\Phi\big(S(1)\big) = \big(S(1) - K\big)^+$ (positiv del), og man kan tænke på optionen som en forsikring der garanterer at kunne købe en aktie til tid 1 til pris højst K (optionen vil jo dække en eventuel merpris; udover aktiepriser er oplagte fortolkninger af $S(1)$ olieprisen, vekselkursen USD/DKK etc.). Hvad er prisen Π for at købe en sådan option?

For at udregne Π, viser vi først at optionen kan *repliceres*, d.v.s. at afkastet $\Phi\big(S(1)\big)$ til tid 1 er det samme som $w(1)$, afkastet af en mere traditionel portefølje sammensat af bank- og aktieinvestering. Dette betyder at man låner a KR i banken og køber b aktier til tid 0 (korte positioner er tilladt), så man skal betale $w(0) = a + b$ for porteføljen. Til tid 1 har man så $w(1) = a\mathrm{e}^r + bS(1)$ KR. Sættes dette lig optionsudbetalingen $\Phi(S(1))$ har vi de to muligheder u eller d, og skrives $V_u = \Phi\big(u\big)$, $V_d = \Phi\big(d\big)$, giver dette $V_u = a\mathrm{e}^r + bu$, $V_d = a\mathrm{e}^r + bd$. Dette er to ligninger med to ubekendte a, b, og løsningen er

$$a = \frac{uV_d - dV_u}{(u-d)\mathrm{e}^r}\,, \quad b = \frac{V_u - V_d}{u-d}\,.$$

Hvis nu $\Pi < w(0)$, har vi en arbitragemulighed til tid 1, nemlig at tage en kort position i porteføljen til tid 0 og købe $w(0)/\Pi$ optioner. Dette er gratis. Til tid 1 er vores afkast så

$$-w(1) + \frac{w(0)}{\Pi}\Phi\big(S(1)\big) \;=\; \Big(\frac{w(0)}{\Pi} - 1\Big)\Phi\big(S(1)\big)\,,$$

som iflg. antagelsen om Φ er er ikke-negativt og positivt hvis enten $S(1) = u$ eller $S(1) = d$ (eller evt. i begge tilfælde). Da markedet antages frit for arbitrage, er altså $\Pi \ge w(0)$. Den modsatte ulighed fås ved at ombytte korte og lange positioner, så det ønskede resultat er

$$\Pi \;=\; w(0) \;=\; a + b\,. \tag{7}$$

Hvis vi sætter $p^* = (\mathrm{e}^r - d)/(u-d)$, $q^* = 1 - p^* = (u - \mathrm{e}^r)/(u-d)$, er $0 \le p^* \le 1$ fordi $d \le \mathrm{e}^r \le u$ i et arbitrage-frit marked, og det ses let at (7) kan skrives

$$\begin{aligned} \Pi \;=\; w(0) \;&=\; \mathrm{e}^{-r}\big[p^*V_u + q^*V_d\big] \\ &=\; \mathbb{E}^*\big[\mathrm{e}^{-r}\Phi\big(S(1)\big)\big], \end{aligned} \tag{8}$$

hvor $\mathbb{E}^*$ står for middelværdi med p erstattet af p^*. D.v.s. prisen har samme form som det naive gæt $\mathbb{E}\big[\mathrm{e}^{-r}\Phi\big(S(1)\big)\big]$, men med et andet p. Man viser også let den ovenfor givne definition af risikoneutralitet, $\mathbb{E}^*\big[\mathrm{e}^{-r}S(1)\big] = 1$

En særdeles overraskende, for ikke at sige paradoksal, konsekvens af denne beregning er at Π ikke afhænger af p. Hvis man uden nøjere overvejelse skal gætte på ordningen af priserne Π', Π'' af to Europæiske optioner med samme K og baserede på to aktier med $p' > p''$, vil man jo umiddelbart tro at $\Pi' > \Pi''$ — det forventede afkast er større. Men både de økonomiske aksiomer og de matematiske beregninger er svære at gennemhulle!

4 Panjer's rekursion

Som sidste eksempel vil jeg se på beregningen af sandsynligheden for en stor totalskade i et år for et forsikringsselskab.

Det antages at totalskaden har formen $A = V_1 + \cdots + V_N$, hvor de enkelte skadebeløb $V_1, V_2, \ldots$ er uafhængige med fælles fordeling F, og at N (skadeantallet) er en uafhængig heltallig stokastisk variabel med $p_n = \mathbb{P}(N = n)$, $n \in \mathbb{N}$. Vi antager at F er koncentreret på $h, 2h, 3h, \ldots$ (dette kan altid bruges som approksimation for et generelt F ved at tage h lille nok) og skriver $\mathbb{P}(V_i = hj) = f_j$. Da er også $A \in \{0, h, 2h, 3h, \ldots\}$ og vi skriver $g_j = \mathbb{P}(A = hj)$. Vi er interessede i $\mathbb{P}(A > ha) = 1 - g_0 - g_1 - \cdots - g_a$ for et stort a. Vi kan antage $h = 1$ og behøver at beregne $g_1, \ldots, g_a$.

Den naive metode er som følger. Først betinges med $N = n$, hvad der giver $g_0 = p_0$ og

$$g_j \;=\; \sum_{n=1}^{j} p_n f_j^{*n}\,, \quad j = 1, 2, \ldots\,, \tag{9}$$

hvor $f_j^{*n} = \mathbb{P}(V_1 + \cdots + V_n = j)$; $A = j$ kan ikke indtræffe for $n > j$ fordi alle $V_i \ge 1$. Disse størrelser kan beregnes rekursivt ved $f_j^{*1} = f_j$,

$$f_j^{*n} \;=\; \sum_{k=n-1}^{j-1} f_k^{*(n-1)} f_{j-k}\,. \tag{10}$$

Dette giver kompleksiteten (antal arithmetiske operationer) $\mathrm{O}(a^3)$ for at udføre (9), (10) for $a = 0, \ldots, j$. Panjer's rekursion er en algoritme med den væsentlig mindre kompleksitet $\mathrm{O}(a^2)$, og udledningen indeholder desuden et (ihvertfald for en sandsynlighedsteoretiker) lækkeri, nemlig et ombyttelighedsargument (der som andre anvendelser f.ex. har martingalbeviset

Vi behøver at specialisere vores N noget ved at antage at der findes a, b med

$$p_n \;=\; \left(a + \frac{b}{n}\right) p_{n-1}, \quad n = 1, 2, \ldots. \tag{11}$$

For eksempel gælder dette med $a = 0$, $b = \lambda$ for Poissonfordelingen med parameter λ (et særdeles velmotiveret eksempel p.gr.a. binomialapproksimationen) fordi

$$p_n \;=\; \mathrm{e}^{-\lambda}\frac{\lambda^n}{n!} \;=\; \frac{\lambda}{n}\mathrm{e}^{-\lambda}\frac{\lambda^{n-1}}{(n-1)!} \;=\; \frac{\lambda}{n}p_{n-1}.$$

Panjer's rekursion er

$$g_0 = p_0,\; g_j \;=\; \sum_{k=1}^{j}\left(a + b\frac{k}{j}\right) f_k g_{j-k}\,, \quad j = 1, 2, \ldots. \tag{12}$$

Bevis. Idet $V_i > 0$, kan $A = 0$ kan kun indtræffe hvis $N = 0$, og dette giver umiddelbart begyndelsesbetingelsen $g_0 = p_0$. Ombyttelighedsargumentet i rekursionen er nu at bemærke at da $V_1, \ldots, V_n$ indgår symmetrisk, kan

$$\mathbb{E}\left[a + b\frac{V_i}{j} \;\middle|\; \sum_{i=1}^{n} V_i = j\right] \tag{13}$$

ikke afhænge af $i = 1, \ldots, n$. Men summeres (13) over i, fås $na + b$, så værdien af (13) er derfor $a + b/n$.

$$\begin{aligned}
g_j &= \sum_{n=1}\Big(a + \frac{\cdot}{n}\Big)\, p_{n-1} f_j^{*n} \\
&= \sum_{n=1}^{\infty}\mathbb{E}\left[a + b\frac{V_1}{j} \;\middle|\; \sum_{i=1}^{n} V_i = j\right] p_{n-1} f_j^{*n} \\
&= \sum_{n=1}^{\infty}\mathbb{E}\left[a + b\frac{V_1}{j}\,;\, \sum_{i=1}^{n} V_i = j\right] p_{n-1} \\
&= \sum_{n=1}^{\infty}\sum_{k=1}^{j}\left(a + b\frac{k}{j}\right) f_k f_{j-k}^{*(n-1)} p_{n-1} \\
&= \sum_{k=1}^{j}\left(a + b\frac{k}{j}\right) f_k \sum_{n=0}^{\infty} f_{j-k}^{*n} p_n \\
&= \sum_{k=1}^{j}\left(a + b\frac{k}{j}\right) f_k g_{j-k}
\end{aligned}$$

(den næstsidste ulighed vises ved at betinge med $\sum_2^n V_i = j - k$), så (12) er vist. □

5 Afsluttende beærkninger

Metodikken illustreret i løsningen af de Moivre's ruinproblem har et noget videre sigte. En teoretisk matematiker vil nok først og fremmest tænke på forbindelserne mellem Brownsk bevægelse (BM) og analyse. Udviklingen af en Brownsk bevægelse $\{B(t)\}_{t\geq 0}$ er beskrevet ved differentialoperatoren $\mathcal{A}f = \mu f' + \sigma^2 f''/2$ i den forstand at $\mathbb{E}_u f\big(B(h)\big) = f(u) + h\mathcal{A}f(u) + \mathrm{o}(h)$ hvor $\mathbb{E}_u$ refererer til begyndelsbetingelsen $B(0) = u$. Hvis man tager $f(u) = \psi_v(u)$ som ovenfor (sandsynligheden for at den Brownske bevægelse rammer 0 før v hvis man starter fra $u \in (0, v)$) giver dette en differenetialligning (ODE) $0 = \mu f' + \sigma^2 f''/2$, og med randbetingelserne $f(0) = 1$, $f(v) = 0$ ved vi jo alle hvordan denne ODE kan løses.

Denne udregning er en anvendelse af ODE'er på BM, men anvendelser af BM på ODE'er og PDE'er er mindst lige så vigtige. Et grundlæggende eksempel er PDE'en $F_t + \mu F_x + \frac{1}{2}\sigma^2 F_{xx} = 0$ (med passende randbetingelser) for en funktion $F(t, x)$, hvis løsning har en *Feynman-Kac repræsentation* som en middelværdi i BM. Mere generelt kan μ, σ^2 tillades også at afhænge af t, x, og BM skal da erstattes af løsningen X af den stokastiske differentialligning (SDE)

$$\mathrm{d}X(t) \;=\; \mu\big(t, X(t)\big)\,\mathrm{d}t \;+\; \sigma\big(t, X(t)\big)\,\mathrm{d}B(t).$$

Der er imidlertid også en anden udvidelse af de Moivre's beregning som har et bredere anvendelsessigte. Denne går i retningen Markovkæder. Lad $X_0, X_1, \ldots$ være en Markovkæde med endeligt tilstandsrum E dekomponeret som disjunkt forening af E_+, E_-, E^*. For $i \in E^*$, hvad er sandsynligheden $f(i)$ for at ramme E_+ før E_- givet $X_0 = i$? Løsning: hvis p_{ij} er sandsynligheden for at gå fra i til j i et skridt, fås ved at betinge med $X_1 = j$ at for $i \in E^*$ er

$$f(i) \;=\; \sum_{j\in E} p_{ij} f(j)\,,$$

så vi skal bare løse lineære ligninger hvor vi bruger randbetingelserne $f(i) = 1$ for $i \in E_+$ og $f(i) = 0$ for $i \in E_-$

En typisk anvendelse af dette er risikoberegninger for fly, atomkraftværker etc. En tilstand i kan her have formen $i = i_1 i_2 \ldots i_M \in \{0, 1\}^M$ hvor M er

antallet af relevante komponenter og $i_m = 1$ betyder at komponent m fungerer, $i_m = 0$ at den ikke gør. E_+ er så de kombinationer af 0'er eller 1'er hvor hele systemet ikke fungerer, $E_- = \{11 \ldots 1\}$ den tilstand hvor alt er perfekt, f.ex. lige efter et serviceeftersyn.

Markovkædesynspunktet giver et yderligere perspektiv, idet det nemlig kan vises at i denne rammer er tidspunktet indtil E_+ rammes (altså ikke bare før E_-) asymptotisk eksponentialfordelt. Når man siger at et fly forulykker en gang pr. 2.000.000 flytimer, kan dette altså normalt fortolkes som at tiden til ulykken er omtrentligt eksponentialfordelt med middelværdi 2.000.000.

Til slut lad os bemærke nogle væsentlige begrænsninger ved risikoberegninger af den type vi har set på her:

Det er umuligt at lave en matematisk model der indkorporerer alle risikofaktorer. Erfaring viser at uønskede hændelser ofte indtræffer af årsager som er uforudsete, d.v.s. ikke tidligere sete i den givne sammenhæng.

De sandsynligheder man er interesseret i er ofte meget små, og bliver derfor typiskt meget følsomme over modellen. Et problem er mange gange at der reelt er afhængighed (f.e.x. mellem fejl af forskellige komponenter) hvor man i mangel af præcis viden om denne vil antage uafhængighed.

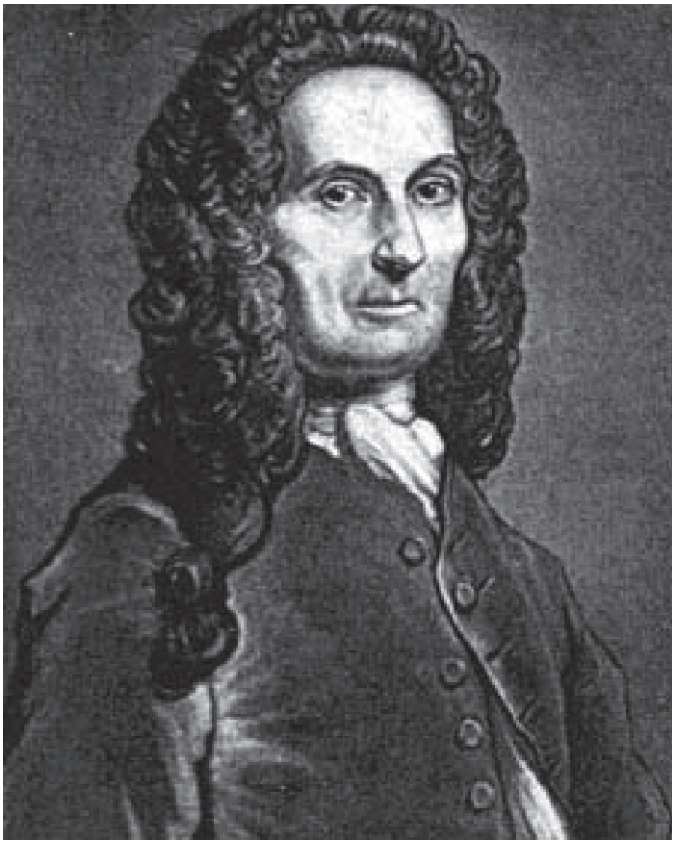
Rimeligheden af en model og indgående parameterværdier kan testes udfra data i normale sammenhænge. Men sjældne hændelser indtræffer ikke i normale sammenhænge, så der er sjældent data til at teste om modellen kan ekstrapoleres til ekstreme sammenhænge.

S. Asmussen (2000) *Ruin Probabilities.* World Scientific, Singapore.

S. Asmussen (2009) Ruin theory. *Encyclopedia of Quantitative Finance* (redaktører R. Cont & P. Tankov). Wiley, Chichester.
Tilgængelig som `http://home.imf.au.dk/asmus/eqfruin`

T. Björk (2004) *Arbitrage Theory in Continuous Time.* Oxford University Press

J.L. Doob (1984) *Classical Potential Theory and Its Probabilistic Counterpart.* Springer-Verlag.



Abraham de Moivre

Playing a trick on uncertainty

F. Thomas Bruss (Bruxelles)

If you have to decide between two alternatives without knowing which one is more favourable, then you may quite as well flip a coin - Right?

No, you can do better.

You want to sell your house. Your ad "Sell for the best offer above 800.000 Euro" has been running for weeks already in the newspaper. But now, next Sunday is the deadline.

Two potential buyers have announced their definite interest. Mr. X from Paris called, saying that he will make an offer exceeding 800.000 Euro but that he would like to see the house again next Saturday before finalizing his exact offer. And then there is Mrs. Y who called from London to say essentially the same, except that she can come next Sunday only. Both Mr. X and Mrs. Y insisted that they would need your irrevocable Yes or No on the very day of their visit.

You would have liked so much to find out more! If you only had been able to obtain an indication of what limit Mr. X and Mrs. Y were prepared to pay!

However, all you got on the phone was a short laugh and something like "Please let me see the house again." True business people, both of them! You also have made already your inquiries: Both are serious and reliable, and both have the necessary funds. But then, it seems hard to guess who of the two could be expected to be the more interested one.

It is time to analyse the exact circumstances of your situation. Clearly, you will have again the opportunity to point out the splendid features of your house. However, this will not change your dilemma: If you accept the offer of Mr. X you will lose the one of Mrs. Y, and if you want to wait for the offer of Mrs. Y you lose the one of Mr. X. This seems like gambling! You will lose the better of the two offers with probability 1/2, won't you?

Another idea comes to your mind. Paris….London ..., it is not likely that Mr. X and Mrs. Y know each other. Should you perhaps try to push up the price by telling each of them how much interested the other one is? Perhaps trying with Mr. X first? - But No, you dismiss this idea, a man like Mr .X would hardly be impressed by this - rather on the contrary. Trying with Mrs. Y perhaps? But then, the day she comes, Mr. X is already out of the game and can no longer serve as a means of pressure.

And again you arrive at the same conclusion as before: You may as well flip a coin in order to decide. Perhaps you should simply make the deal with Mr. X to have at least your Sunday free!

Game with two cards

Such situations in real life occur in many different variations. A special offer in the supermarket, a nice apartment, an attractive job offer, or even the woman or man for life: One must so often decide without knowing whether something better is still to come.

To clear the view for the problem, we summarize the essence in terms of a little game: You ask your son and your daughter to write, each one secretly, and not consulting each other either, one arbitrary number on his/her card. You point out that "arbitrary" means really as they want: Large, small, negative, decimal point, everything is allowed. Then they place their cards, face down, on the table. You can now turn over the card of your son, inspect the number, and then decide whether you accept it. If you refuse it, then you receive automatically your daughter's card. Now both numbers are compared. If you have chosen the larger number you win, otherwise you lose.

The difference between these numbers is now without importance you just want to win. If the numbers happened to be the same, the game would be repeated, but this case is improbable. Further, if you think you may have some advantage from knowing your children well, you can imagine them being replaced by others. Alternatively, one person may also fill in both cards.

This really looks now like a purified game of chance with win probability 1/2.

But now the surprise: There is a strategy with which you can increase your win probability above 1/2. It is based on an idea of Professor Thomas Cover (Stanford University). Let X and Y be the two different numbers on the cards.

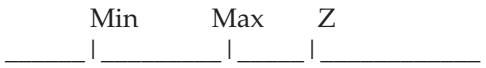
Strategy: Think of an arbitrary number Z. Now uncover the first number, X, and choose this number if it is larger than Z, otherwise choose Y.

Why should this strange strategy be better than choosing X or Y at random?

Here is the proof:

Recall X is the first number, Y the second. Let Min=min{X, Y} be the smaller and Max=max{X,Y} the larger one. There are exactly three possibilities:

(A) Both numbers X and Y are not larger than Z,



(B) Z lies between X and Y (possibly coinciding with the smaller one),

(C) Both X and Y exceed Z.

According to the strategy, you choose the number Y in case (A) and the number X in case (C). In these two cases you end up with a random choice between the larger and the smaller number, hence you win with probability 1/2. In case (B), however, you win with certainty, because if X is the larger of the two numbers you accept it, but if it is the smaller one, you refuse it. Thus your total win probability is now

$$w = a/2 + c/2 + b,$$

where a, b, and c denote the unknown probabilities of the events (A), (B) and (C) respectively. One of these events is bound to happen, of course, that is $a+b+c=1$, and hence

$$w = (a+b+c)/2 + b/2 = 1/2 + b/2.$$

Thus the win probability exceeds equal chance by $b/2 > 0$, because (B) can occur.

[Remark: To make this precise it suffices to choose Z according to any density that is strictly positive everywhere on the real line.]

How can you apply this strategy most skilfully? Evidently you should try to make the case (B) as probable as possible. This means you should choose Z such that it has the largest possible probability of falling between X and Y. Since these two numbers are unknown, no general recommendation can be made. In concrete cases, however, one may quite well have some ideas.

Optimal choice of a threshold

Our house-selling problem is such a concrete case. On the first card is the offer of Mr. X and you will not know the number on the other card, the offer of Mrs. Y, when you must say Yes or No to Mr. X. The first difference to the card game with arbitrary numbers is that you know that both X and Y are above 800.000. The second difference is that the amount $|X-Y|$ is now of real interest to you.

An offer of 900.000 Euro or more would be nice, but is not very likely. On the other hand, if you accepted Mr. X's offer of 801.000 Euro, say, then you would not suffer much regret if Mrs. Y would offer 802.000 Euro. There is no point in trying to hedge against a loss of too modest a magnitude. Therefore it may be best to choose Z clearly above 800.000 Euro, but then again not too large. If you asked me what I would do: I would toss a die and, for each eye of my result, add 5.000 Euro to the amount 800.500 Euro. So, for instance, if I obtained 3, I would choose Z=815.500. But, by all means, there is nothing special about this suggestion and you may be much happier with your own idea.

Why toss a die? Why not simply fix Z=820.000, say, if we feel this should be more or less in the right order of magnitude? Apart from our probability argument there is another reason: In such a game-theoretical situation, it is often better to be unpredictable. If we act in a predictable way, the other player may adjust his behaviour. Hence the introduction of a random component.

What is our strategy worth? - Definitely more than the random choice, as we have seen. We cannot really quantify the advantage compared with a random choice, but some additional 10.000 Euro or so may quite well be in it (in expectation.)

Let us go a step further and look again into our two-card game. Now you and I play the game. Suppose you are the one who writes the two numbers on the two cards and it is I who has to choose one. As before, I win if I choose the larger one. Suppose you would like to decrease my win probability. What should you do?

The answer is simple. You just choose two numbers that are very close to each other. Take 6.123455 and 6.123456, say. My advantage of using a Z-strategy is now hardly worth talking about because my chosen Z will have little chance of falling between these two numbers.

In real-world problems, things are often different, however. Real-world strategies are developed by one party and typically not communicated to the other party. What difference does this make?

To find this out, I made, several years ago, a test with Vesalius College business students. Everybody in the audience received two cards to write down his or her numbers, and then I passed from one to the other to make my choice. I had not mentioned Z-strategies before.

My score was 32 successes for 41 or 42 participants. With a random choice we would expect some 21, and some three or four more with a bit of luck. 32 however should not be explained by pure luck alone, as they knew. Even the best students were puzzled. It is difficult to see what one does not expect. But you, dear reader, you probably guess correctly: I had applied a Z-strategy, even a particularly naive one. I had chosen Z = 0.

Why was this so successful? – I think it was because I could prepare the field for the strategy: My remark "The numbers may also be negative had seemingly succeeded in being sufficiently casual. The fact is that numerous students made use of negative numbers, and all those who had written down just one negative number made me automatically a winner.

This experiment shows that strategic thinking has no simple rules Some people preach that the key to success in strategic behaviour is always narrowing down the adversary's field of action. However, this is not true. If we believe that our adversary does not expect our strategy it can be unwise to narrow down the set of his or her options. The less one can do, the more one thinks about each step. Indeed, in our experiment, by allowing negative numbers

we did not narrow down but actually enlarged the set of options for the students. This probably helped to distract from paying attention.

A few words about mathematics

You have just learned to know a little problem in a field of mathematics, which, compared to other fields, is still in its infancy: strategic thinking, as a part of probability theory. Even at this introductory level several questions are still open. For instance, does there exist a strategy for the two card game which is generally more efficient than a Z-strategy? - The proof of existence or non-existence would already be a true progress. However, at the current state of knowledge, I see no sufficiently safe foundation to attack such a proof, not even to make this question sufficiently precise.

Is it not truly surprising that nobody can optimise, in a strict mathematical meaning, the sale of a house to two potential buyers? Given that we see so many impressive things mathematics has achieved in our world, we would agree that it is, wouldn't we? Think of other optimisation problems from modern airplane engineering, for instance. Compared to such problems, our little problem seems ridiculously simple. However, this is not true. Airplane engineers have a huge time advantage: They can work, routinely, with many methods for which the mathematical foundations have been well established for two to three centuries. This is not the case for our little problem.

Such contrasts do exist in many fields of mathematics.

Is this a symptom of the eternal youth of a discipline?

Yes, I think it is.

Footnote:

This is the author's English translation of his article Der Ungewissheit ein Schnippchen schlagen published in Spektrum der Wissenschaft (= German Edition of Scientific American). The latter was based on the author's Unerwartete Strategien published in Mitteilungen der Deutschen Mathematikervereinigung (German Mathematical Society.) The idea was instigated by Cover's Problem. (References below.)

Acknowledgement . The author would like to thank Professor Lundsgaard Hansen for his comments on the English version.

References

F. Thomas Bruss, Unerwartete Strategien, Mitteilungen der Deutschen Mathematikervereinigung, Heft 3 (1998), 6-8.

F. Thomas Bruss, Der Ungewissheit ein Schnippchen schlagen, Spektrum der Wissenschaft, Juni Heft (2000), 106-107.

Thomas M. Cover, Problem 2.5 : Pick the largest number. In: Open Problems in Communication and Computation, Springer Verlag, New York. (1987).

:

F. Thomas Bruss [tbruss@ulb.ac.be] studied Mathematics in Saarbrücken (FRG), Cambridge, and Sheffield (UK). He started his career as assistent and first assistant in Namur (B) from where he moved on to the United States, where he was Visiting Associate Professor at UC Santa Barbara, U of Arizona, and UCLA, successively. In 1990 he was appointed Professor at Vesalius College of the Vrije Universiteit Brussels. Since 1993 he is Professor of Mathematics and Statistics at the Université Libre de Bruxelles. His research is in probability: limit theorems, branching processes, probabilistic models, and optimal stopping. He is fellow of the Institute of Mathematical Statistics and Feodor-Lynen-fellow of the von-Humboldt Foundation.

The Theorem of Green–Tao

af Valentin Blomer (Toronto, Canada)

"Prime numbers were invented to multiply them, not to add" – Gelfand attributes this famous quote to Russian physicist Lev Landau. Nonetheless, the additive properties of the primes have been a fascinating subject for generations of professional (and lay) mathematicians, and by now there is an ample supply of powerful and flexible methods to attack classical problems.

Ben Green (left) and Terence Tao

A remarkable breakthrough was achieved in the joint work of Ben Green and Fields Medalist Terence Tao. Ben Green completed his thesis in 2002 under the supervision of Tim Gowers and is a professor at Cambridge, UK. Terence Tao was a student of Elias Stein (Princeton) and is currently at the University of California in Los Angelos. He is known for fundamental contributions to an impressive range of mathematical disciplines including harmonic analysis, partial differential equations, signal analysis, operator theory, combinatorial and algebraic geometry and additive number theory. In 2004, Green and Tao announced the following result:

Theorem 1 (Green-Tao [6])**.** *The set of prime numbers contains arbitrarily long arithmetic progressions; in other words, for every integer $k \geq 3$ there is a sequence of primes $p_1, \dots, p_k$ such that $p_2 - p_1 = p_3 - p_2 = \dots = p_k - p_{k-1}$. More precisely, there is a constant $\delta_k > 0$ such that*

$$\#\{(n,d) \in [1,N]^2 \mid n, n+d, \dots, n+(k-1)d \text{ prime}\} \geq \delta_k \frac{N^2}{(\log N)^k}.$$

For example, $7, 37, 67, 97, 127, 157$ is an arithmetic progression of length $k = 6$ consisting only of primes. In 2004, Frind, Underwood and Jobling found a progression of length 23 with first element of size $\approx 5.6 \times 10^{13}$ but of course the existence of such a progression could be a sporadic freak of nature. Notice that the theorem guarantees arbitrarily long progressions of primes but infinitely long progressions do not exist: $n + jd$ is certainly not prime if $j = n$.

This note presents some of the ideas and techniques that go into the proof of the theorem. There are other surveys, for instance [5, 11, 14, 15].

Heuristic approaches

Why could one reasonably expect the theorem of Green-Tao to be true? Prime numbers do not seem to follow any pattern but tend to be distributed rather randomly. This suggests a probabilistic approach: by the prime number theorem

$$\pi(x) := \{p \leq x \mid p \text{ prime}\} \sim \frac{x}{\log x}, \tag{1}$$

the probability that a randomly chosen number n is prime is about $1/\log n$. Let us now draw randomly the first element $n \leq N$ and the difference $d \leq N$ of our progression. Then the probability that the k numbers $n, n+d, n+2d, \dots, n+(k-1)d$ are all prime is about $1/(\log N)^k$, so there ought to be about $N^2/(\log N)^k$ progressions of length k with first element and difference at most N. Here we have tacitly assumed that the events "n prime" and "$n+d$ prime" are independent. This is obviously wrong, as one can see for $d = 1$: if $n > 2$ is prime, then $n+1$ is never prime. Conversely, if $d = 2$ and n is prime, then the (conditional) probability that $n+2$ is prime increases to $2/\log N$, because we know already that $n+2$ is odd. These effects, however, can easily be controlled. They come from obvious divisibility and congruence conditions or, put into more formal language, from p-adic obstructions of the various non-archimedean completions $\mathbb{Q}_p$ of $\mathbb{Q}$. For each prime p we obtain a correction factor so that we arrive at the following conjecture:

Conjecture. For fixed $k \geq 3$ one has

$$\#\{(n,d) \in [1,N]^2 \mid n, n+d, \dots, n+(k-1)d \text{ prime}\} \sim \gamma_k \frac{N^2}{(\log N)^k} \tag{2}$$

for $N \to \infty$, where $\gamma_k = \prod_p \alpha_p(k)$ is an explicitly given, absolutely convergent product over primes satisfying $\gamma_k = \exp((1+o(1))k \log\log k)$ as $k \to \infty$.

If this conjecture was true, then it is obvious that for every fixed $k \geq 3$ there are (in fact, very many) arithmetic progressions of length k if only one takes N sufficiently large, $N = k^k$ say. In particular, up to the constant, the theorem of Green-Tao yields the conjectured order of magnitude for the number of the progressions in question.

In addition to probabilistic considerations, the conjecture is supported by a method of Hardy and Littlewood, the so-called circle method. Developed around 1920, it has been substantially extended and refined and is by now one of the most powerful tools in additive number theory. For $k = 3$, for instance, one could argue as follows. For $\alpha \in \mathbb{R}$, let

$$f(\alpha) := \sum_{\substack{p \leq N \\ p \text{ prime}}} e^{2\pi i p \alpha}$$

be a finite exponential sum over prime numbers.[1] Then one

has

$$\begin{aligned} I &:= \int_0^\infty f(\alpha)^2 f(-2\alpha)d\alpha \\ &= \sum_{p_1,p_2,p_3\le N} \int_0^1 \exp(2\pi i(p_1+p_2-2p_3)\alpha)\,d\alpha \\ &= \#\big\{(p_1,p_2,p_3)\in[1,N]^3 \mid p_1-p_3 \\ &= p_2-p_3, \text{ all } p_j \text{ prime}\big\}, \end{aligned}$$

since the integrand vanishes unless $p_1+p_2-2p_3=0$. The right hand side is essentially the quantity that we want to count, so we have to calculate or estimate the integral I. We observe that f can be easily evaluated at $\alpha=0$; one simply has $f(0)=\pi(N)$. Similarly one finds[2]

$$\begin{aligned} f(1/3) = 1 &+ e^{2\pi i/3}\#\{p\le N \mid p \text{ prime}, p\equiv 1 \,(\mathrm{mod}\, 3)\} \\ &+ e^{4\pi i/3}\#\{p\le N \mid p \text{ prime}, p\equiv 2 \,(\mathrm{mod}\, 3)\}. \end{aligned}$$

In general, the integrand of I can be approximated reasonably well at rational numbers p/q with denominator q not too large, if one has some knowledge on the distribution of primes in residue classes modulo q. By continuity one can extend this approximation to a small neighbourhood of these rationals. The integral over this part of the unit interval yields the main term, up to a small error. If one could control the integrand slightly off rational points by other techniques, the remaining portion of the integral can be identified as an error term and (2) is proved. For $k=3$ this is indeed possible and was carried out by van der Corput [1] in 1939.

Another approach to (2) is to detect the primality condition by combinatorial means using the inclusion-exclusion principle, or the sieve of Erathostenes: in order to count primes in a set $\mathscr{S}\subseteq[1,N]$ one subtracts from the total count the multiples of 2, then the multiples of 3 (but adds the doubly subtracted multiples of 6) and so forth up to the largest prime number below $\sqrt{N}$.[3] This yields a sum of $2^{\pi(\sqrt{N})}$ terms with alternating signs that cannot be controlled satisfactorily. Sieve theory provides combinatorial means that in many situations make it possible to carry out a similar procedure ("sieve") at least up to N^δ for some (small but fixed) $\delta>0$. A number $s\in\mathscr{S}$ that is only divisible by primes $p>N^\delta$ has at most $1/\delta$ prime factors; hence we can detect "almost primes" in $\mathscr{S}$ having only a fixed number of prime factors. More generally, a sieve can be applied to k-tuples of numbers, say arithmetic progressions of length k. E. Grosswald [9] showed in 1980 that there are arbitrarily long progressions in almost primes. More precisely, for each k there is a number $A=A(k)$ such that there are (many) arithmetic progressions of length k consisting of numbers with at most A prime factors. The circle method and the sieve method can be coupled: Heath-Brown [10] proved in 1981 that there are infinitely many progressions of four numbers, three of which are prime and one of which has at most two prime factors.

Finally one could hope that no arithmetic properties of the primes are necessary to prove (2) but that the density (1) given by the prime number theorem would suffice to guarantee arbitrarily long arithmetic progressions. This has been a folklore conjecture but it has resisted any proof so far. A famous theorem of van der Waerden [18] (1927) states that for each disjoint partition $\mathbb{N}=\bigcup_{j=1}^n S_j$ of $\mathbb{N}$ into finitely many subsets S_j at least one of them contains arbitrarily long arithmetic progressions. By an ingenious application of the circle method, Fields medalist Klaus Roth [12] showed in 1956 that for some constant $c>0$ every set $\mathscr{S}\subseteq[1,N]$ of cardinality $\#\mathscr{S}\ge cN/\log\log N$ contains an arithmetic progression of length 3. One of the most important theorems in this context is Szemerédi's theorem [13] (1975): for $\mathscr{S}\subseteq\mathbb{N}$ let $d^*(\mathscr{S}):=\limsup\#(\mathscr{S}\cap[1,N])/N$ be the upper density. If $d^*(\mathscr{S})\ge c>0$, then $\mathscr{S}$ contains arbitrarily long progressions. The proof uses, among other things, van der Waerden's theorem. Subsequently, a number of other proofs of Szemerédi's theorem have been found, for example by Furstenberg [2] (1977) and by Gowers [4] (2001) who proved the following stronger result. There are constants $c_k,d_k>0$ such that every subset $\mathscr{S}\subseteq\mathbb{N}$ satisfying $\#(\mathscr{S}\cap[1,N])\ge c_kN(\log\log N)^{-d_k}$ contains an arithmetic progression of length k. Unfortunately, by (1) this is not yet enough for the prime numbers. In 1936, Erdős and Turan conjectured more generally that every subset $\{a_1,a_2,\ldots\}\subseteq\mathbb{N}$ contains arbitrarily long progressions providing that $\sum 1/a_j$ diverges (this would be the case for the primes). This conjecture is still open; it is not even known if such a set contains a progression of length 3.

Ideas of the proof

None of the heuristic approaches presented so far can prove (2) but they all play a fundamental role in the proof of the theorem of Green-Tao. The basic idea is to distinguish between sets that behave like random sets (pseudo random sets) and sets that carry a certain structure. For pseudo random sets one can argue probabilistically, whilst otherwise one can exploit the particular structure. One could hope to decompose arbitrary sets into a random and a structured part, and in either case one has a method to detect progressions. Of course, the difficulty is to make this idea precise.

If one searches for arithmetic progressions in the primes, there are obvious effects coming from the distribution of primes modulo "small" numbers; for instance there are no such progressions having difference $d=1$. These effects are responsible for the main term in the circle method and, more or less equivalently, for the correction factor γ_k in the probabilistic approach. For technical reasons, we remove these properties from the primes: while almost all primes are odd, the sequence $(p-1)/2$, $p\ge3$, is essentially equidistributed modulo 2, since there are about as many primes congruent 1 modulo 4 as primes congruent 3 modulo 4. By further scaling, the sequence of primes can be modified such that it becomes equidistributed in residue classes $p\le P$. Let $W:=\prod_{p\le P}p$ and define a number $\tilde{p}$ to be a "modified prime" if $W\tilde{p}+1$ is prime. In order to prove (2), two goals need to be achieved: the notion of "structure" versus "pseudo random set" has to be made precise and we need to study the influence of this structure in the case of the primes. Both questions are, in general, very hard.

To get started, let us regard subsets $\mathscr{S}\subseteq[1,N]$ as a subset of $\mathbb{Z}/N\mathbb{Z}$ and let us consider the Fourier coefficients of the characteristic function $\mathbf{1}_{\mathscr{S}}(x)$. Thus we look at exponential sums of the form

$$\sum_{s\in\mathbb{Z}/N\mathbb{Z}} e^{2\pi isr/N}\mathbf{1}_{\mathscr{S}}(s) = \sum_{s\in\mathscr{S}} e^{2\pi isr/N}, \quad r\in\mathbb{Z}/N\mathbb{Z}. \qquad (3)$$

We compare these with the Fourier coefficients of the expected value

$$\sum_{s\in\mathbb{Z}/N\mathbb{Z}} e^{2\pi isr/N}(\#\mathscr{S}/N), \quad r\in\mathbb{Z}/N\mathbb{Z}. \tag{4}$$

If the difference of (3) and (4) is small for all $r\in\mathbb{Z}/N\mathbb{Z}$ then this might indicate that $\mathscr{S}$ behaves like a random set. Indeed, this approach suffices for progressions of length 3, which is why van der Corput could successfully complete the case $k=3$. In general, however, the definition of a pseudo random set depends on the objects being considered. If one counts longer progressions, the definition of a pseudo random set becomes much harder. Here one also has to sum the characteristic function of $\mathscr{S}$ against quadratic exponentials such as $e^{2\pi is^2/N}$, or even more complicated terms of the type $e^{2\pi is\sqrt{2}\{s\sqrt{3}\}}$.[4] The precise description of the right set of test functions is very hard as is the proof that the characteristic function on the modified primes does not correlate with these test functions. With hindsight, Green and Tao worked this out in [7, 8] for $k=4$. In general, however, this is in some sense harder than the (still unsolved) twin prime problem. Therefore, Green and Tao use a slightly different approach.

By (1), the prime numbers are too thin to apply Szemerédi's theorem, even in Gowers' quantitative form. The idea of Green-Tao is to embed the prime numbers into a suitable, sufficiently manageable and not much larger set $\mathscr{P}'$ with the aim of proving a version of Szemerédi's theorem: every sufficiently large subset of $\mathscr{P}'$ contains arbitrarily long arithmetic progressions. In particular, this would imply the stronger statement that every not too thin subset of the primes contains arbitrarily long arithmetic progressions, for example, the set of all primes $\equiv 1 \pmod 6$. "Sufficiently manageable" means that $\mathscr{P}'$ behaves in some precise sense like a random set. Roughly, one can imagine $\mathscr{P}'$ to be the set of almost primes. More precisely, the set is constructed by applying Selberg's sieve and it is possible (but not easy) to check the required properties of $\mathscr{P}'$ by classical techniques.

This version of Szemerédi's theorem is at the heart of the theorem of Green-Tao. For a rigorous realization a complicated and in part newly developed machinery is necessary. For technical reasons it is convenient to replace sets by their characteristic functions and to work generally with nonnegative functions instead of sets. Thus we can reformulate Szemerédi's theorem as follows. If $f:\mathbb{Z}/N\mathbb{Z}$ is a nonnegative, bounded function satisfying $\sum_{n=1}^N f(n)\geq \delta N$ for some $\delta>0$ then

$$\sum_{n\in\mathbb{Z}/N\mathbb{Z}}\sum_{d\in\mathbb{Z}/N\mathbb{Z}} f(n)f(n+d)\cdot\ldots\cdot f\big(n+(k-1)d\big) \geq c(k,\delta)N^2+o(N^2) \tag{5}$$

for some positive constant $c(k,\delta)$. In particular, if f is the characteristic function of a set then the left hand side counts the number of arithmetic progressions. The methods developed in Furstenberg's and Gowers' proof of Szemerédi's theorem now play an important role.

Let us consider the following situation. Let $(X,\mathscr{X}\subseteq\mathscr{P}(X),\mu)$ be a probability space, $T:X\to X$ a measurable map with $\mu(A)=\mu(T^{-1}A)$ for all $A\in\mathscr{X}$, and let $k\geq 1$ be an integer. If $E\in\mathscr{X}$ has positive measure, then Furstenberg [2] showed the existence of $n\in\mathbb{N}$ such that $\bigcap_{j=0}^{k-1}T^{-jn}E$ has positive measure. Moreover, he proved the following combinatorial correspondence. If the upper density of $d^*(A)$ of A is positive then there is a quintuple $(X,\mathscr{X},\mu,T,E)$ as above such that $\mu(E)=d^*(A)$ and

$$d^*\big(A\cap(A+m_1)\cap\ldots\cap(A+m_{k-1})\big) \geq \mu(E\cap T^{-m_1}E\cap\ldots\cap T^{-m_{k-1}}E)$$

for all $m_1,\ldots,m_{k-1}$. Putting $m_j=jn$, we recover Szemerédi's theorem. The important novelty of this proof is the introduction of ergodic theory into the discussion that inspired many ideas of Green and Tao.

Gowers' proof uses harmonic analysis. An important construction is the U^d-norm of a function $f:\mathbb{Z}/N\mathbb{Z}\to\mathbb{C}$, defined by

$$\|f\|_{U^d}:=\left(\frac{1}{N^{d+1}}\sum_{x\in\mathbb{Z}/N\mathbb{Z}}\sum_{\mathbf{h}\in(\mathbb{Z}/N\mathbb{Z})^d}\prod_{\omega\in\{0,1\}^d} f(x+\omega\cdot\mathbf{h})\right)^{1/2^d}$$

with the usual inner product $\omega\cdot\mathbf{h}$ in $\mathbb{R}^d$. These norms are used to measure the distance of a function f from its expected value, i.e. from the constant function $N^{-1}\sum_{n=1}^N f(n)$. As in (3) and (4), for the characteristic functions of a pseudo random set $\mathscr{S}$ this distance is small in all norms U^d for $d\leq k-1$.[5]

The proof of the theorem of Green-Tao rests on the following method. The characteristic function on the modified primes is normalized by multiplication with $\log N$, such that the new function f has expected value 1. Using the above mentioned Selberg sieve, one constructs a majorant g that is well-behaved as it comes from a pseudo random set (almost primes). Szemerédi's theorem is not applicable for f, since f is not bounded, but Green and Tao show that f can be decomposed essentially into two parts. The first part is close to its expected value with respect to the Gowers-norm U^{k-1} and hence manageable. The second part is majorized by the corresponding portion of g. Using properties of almost primes, one can show that this part of g is bounded. A fortiori, the considered part of f is bounded and the original version (5) of Szemerédi's theorem completes the proof.

The full proof contains an impressive combination of number theory, ergodic theory, harmonic analysis and combinatorics and the techniques are also applicable in other situations. For example, Tao and Ziegler prove in [17] that more generally primes contain arbitrarily long polynomial progressions: if $q_1,\ldots,q_k\in\mathbb{Z}[x]$ are arbitrary polynomials with $q_1(0)=\ldots=q_k(0)=0$ then there are infinitely many $n,d\in\mathbb{N}$ such that $n+q_1(d),n+q_2(d),\ldots,n+q_k(d)$ are simultaneously prime. Similar results are possible, for example for Gaussian primes [16]. Using the methods of Green and Tao it is proved in [3] that every set $\mathscr{S}\subseteq\mathbb{N}$ with positive upper density contains infinitely many progressions of length 4, such that the common difference is of the form $p+1$ (p prime). It is clear that the methods developed by Green and Tao have opened many new doors for arithmetic combinatorics.

Notes

1. Since f is a 1-periodic function, it can be regarded as a function on S^1. This is where the name circle method comes from.
2. The first term 1 comes from the prime 3.

3. This excludes, of course, the primes between 1 and $\sqrt{N}$ but their number should be small compared to all primes in $\mathscr{S} \cap [1,N]$.
4. As usual, we denote by $\{x\} = x - [x]$ the fractional part of x.
5. Recall that the definition of a pseudo random set depends on k.

References

[1] J. G. van der Corput, *Über Summen von Primzahlen and Primzahlquadraten*, Math. Ann. **116** (1939), 1–50.

[2] H. Furstenberg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256.

[3] N. Frantzikinakis, B. Host and B. Kra, *Multiple recurrence and convergence for sequences related to the prime numbers*, J. Reine Angew. Math. **611** (2007), 131–144.

[4] W. T. Gowers, *A new proof of Szemerédis theorem*, GAFA **11** (2001), 465-588.

[5] B. J. Green, *Long arithmetic progressions of primes*, in: Analytic Number Theory: A tribute to Gauss and Dirichlet, W. Duke and Y. Tschinkel (eds.), Amer. Math. Soc., Providence, RI, 2007.

[6] B. J. Green and T. C. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math., to appear.

[7] B. J. Green and T. C. Tao, *Quadratic uniformity of the Möbius function*, Annales de'l Institut Fourier, to appear.

[8] B. J. Green and T. C. Tao, *Linear equations in primes*, Annals of Math., to appear.

[9] E. Grosswald, *Arithmetic progressions of arbitrary length and consisting only of primes and almost primes*, J. Reine Angew. Math. **317** (1980), 200–208.

[10] D. R. Heath–Brown, *Three primes and an almost prime in arithmetic progression*, J. Lond. Math. Soc. **23** (1981), 396–414.

[11] B. Kra, *The Green-Tao Theorem on arithmetic progressions – an ergodic point of view*, Bull. Amer. Math. Soc. **43** (2006), 3–23.

[12] K. F. Roth, *On certain sets of integers*, J. Lond. Math. Soc. **28** (1953), 245-252.

[13] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245.

[14] T. C. Tao, *Long arithmetic progressions in the primes*, http://www.math.ucla.edu/~tao/preprints/acnt.html.

[15] T. C. Tao, *Arithmetic progressions and the primes*, Collect. Math. **2006**, Vol. Extra, 37–88.

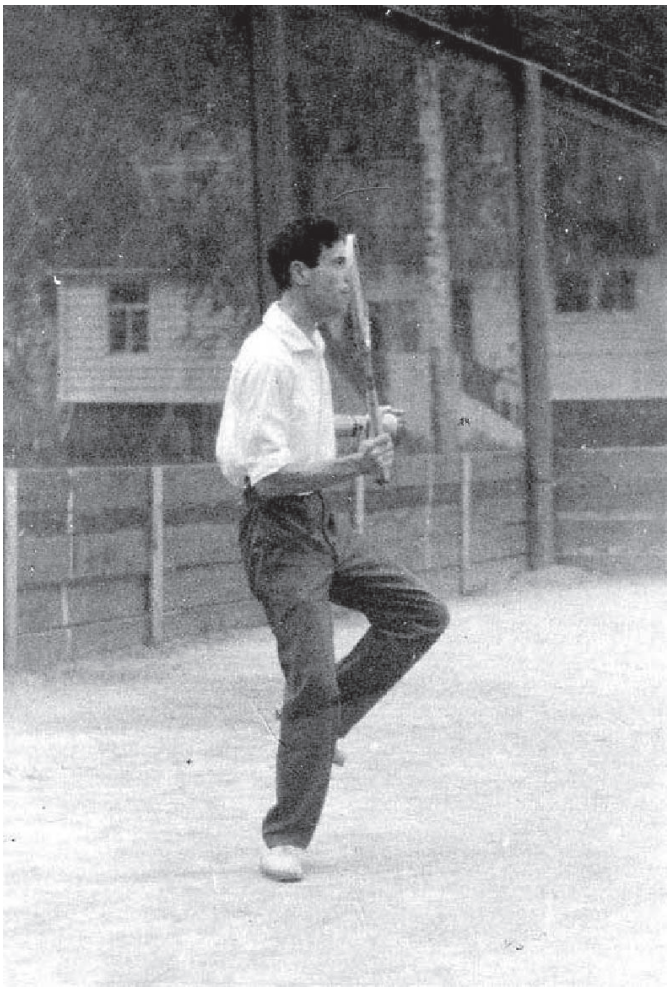
[16] T. C. Tao, *The Gaussian primes contain arbitrarily shaped constellations*, J. Analyse Math. **99** (2006), 109–176.

[17] T. C. Tao and T. Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta. Math., to appear.

[18] B. L. van der Waerden, *Ein Satz über die Klasseneinteilung von endlichen Mengen*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 185–187.

*This article appeared originally in German in Mitteilungen der DMV **15**, no. 3 (2007), 160–164. The Newsletter thanks the editor for the permission to print the author's translation into English.*

Valentin Blomer [vblomer@math.toronto.edu] received his PhD from the University of Stuttgart (supervisor Jörg Brüdern) in 2002 and is currently an assistant professor at the University of Toronto. For his research in analytic number theory he has been awarded the Heinz Maier-Leibnitz Prize of the German Research Council. He is a graduate in piano performance of the Hochschule für Musik, Frankfurt. Valentin is married and has one daughter.



Lev Landau
"Prime numbers were invented to multiply them, not to add" – Gelfand attributes this famous quote to Russian physicist Lev Landau

Kære medlemmer

Der er godt dansk nyt fra rådsmødet i den Europæiske Matematiske Forening (»EMS Council Meeting«), der blev afholdt i Utrecht, 12-13. juli, 2008. De to danske delegerede til rådsmødet i Utrecht var Martin Raussen fra Ålborg Universitet, og Bjarne Toft fra Syddansk Universitet.

Ved rådsmødet blev Martin Raussen valgt som medlem af »EMS executive committee« med det højeste stemmetal blandt alle kandidater. Stort tillykke til Martin med dette valg til en vigtig post i matematisk sammenhæng på europæisk plan.

Samtidig vil jeg benytte lejligheden til på Dansk Matematisk Forenings vegne, at udtrykke min varmeste tak til Martin Raussen for det særdeles flotte stykke arbejde han har udført som hovedredaktør af »Newsletter of the European Mathematical Society« fra efteråret 2003 til juni 2008, hvor han blev afløst af Vicente Muñoz fra Spanien. I løbet af Martins tid som hovedredaktør, har EMS Newsletter udviklet sig til et yderst interessant tidsskrift, som alle medlemmer af Dansk Matematisk Forening kan få glæde af ved at melde sig ind i European Mathematical Society.

European Mathematical Society udfører et stort og vigtigt arbejde for matematikken i Europa, og øger til stadighed sine aktiviteter. De nationale foreninger, herunder Dansk Matematisk Forening, har modtaget følgende brev fra EMS, som jeg herved bringer videre til foreningens medlemmer.

Med venlig hilsen

Vagn Lundsgaard Hansen,
V.L.Hansen@mat.dtu.dk>
formand

European Mathematical Society

European Mathematical Society

The European Mathematical Society is increasing its activities and its membership. We are working harder than ever to make sure that mathematics is represented properly when funding decisions are taken at a European level, and this is beginning to bear fruit. An example is the recent call by the European Science Foundation for proposals for research conferences in mathematics

http://www.esf.org/index.php?id=4602

Also, we now have 56 national member societies from all over Europe, which brings huge opportunities for collaborative work of all kinds.

We would like to increase our individual membership, which now comes with free access to Zentralblatt

http://www.zentralblatt-math.org/portal/en/

as well as our superb Newsletter

http://www.ems-ph.org/journals/journal.php?jrn=newsand many other benefits, as you can see from our new web site

http://www.euro-math-soc.eu/

Membership is not expensive, and joining is easy: you can do it either through the Danish Mathematical Society or on the EMS web page.

Ari Laptev, President
Pavel Exner, Vice-President
Helge Holden, Vice-President
Stephen Huggett, Secretary

PS (Additional remark from Ari Laptev):
I would also like to use this opportunity to remind you
that the European Science Foundation has advertised
the ESF Research Conferences to be held in 2009 and 2010 at one of ERCOM centres http://www.esf.org/index.php?id=4602. The deadline for applications is September 15, 2008. Please make sure that members of your society know about it.

Interview with Alain Connes, part II

The interview was conducted by Catherine Goldstein and George Skandalis, Paris. The first part appeared in Matilde 32. The interview has also appeared in the EMS newsletter.

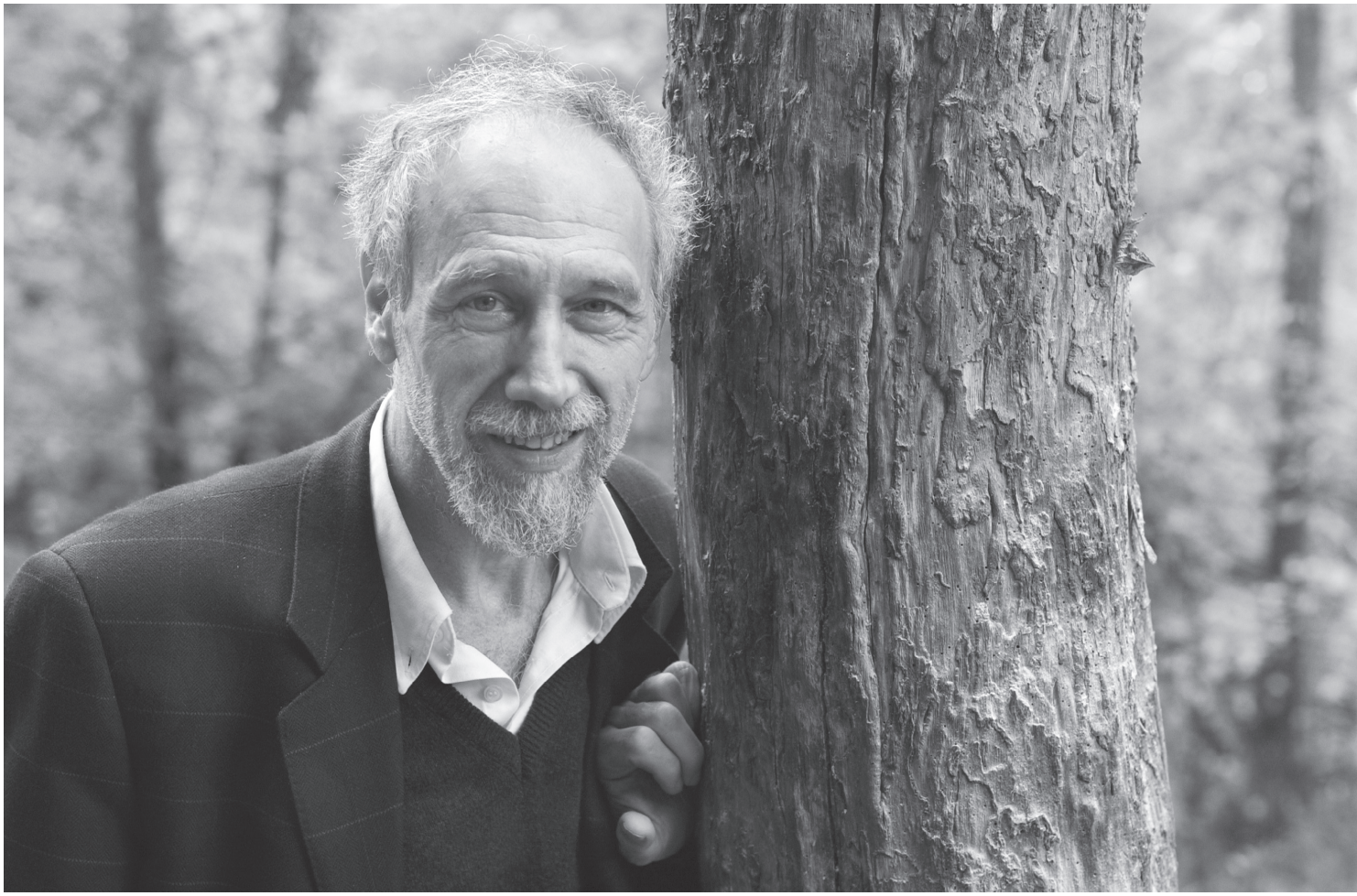
Catherine Goldstein and George Skandalis

Among the results you have obtained, is there one you are most proud of?
Being a scientist is (as far as I am concerned) a pretty humbling activity and I am not keen on showing any pride for any result. I tend to be suspicious of arrogant people. In fact what really matters to me is the pleasure of the discovery as opposed to the appreciation of the result by the community. The amount of joy one gets, the "kick" is of course quite variable and for instance, just to try to answer your question, the link between renormalization and the Birkhoff decomposition, that we found in 99 in our joint work with Dirk Kreimer gave me a great kick that lasted over a full week. I used to behave in a proud manner as a kid till I reached the age of ten, when I was sent to the scouts by my parents. I landed among a tough group and they taught me, one day, by a "group mockery" of myself that they did not buy my proud attitude. Since then I have, like the bulls in the corrida after the session with the picadors, always stood with a slightly bent back.

Following your mathematical quest since the Seventies, one has the impression that you have always been fascinated by physics - and the zeta function.
Absolutely. My fascination for the Riemann zeta function comes from reading Weil's work on his reformulation in terms of idèles of the explicit formulas of Riemann which relate the zeros of the zeta function with the distribution of primes. There is a striking analogy between the "prime number" side of this formula and the fixed point contributions in a Lefschetz formula and the first problem is to find a space X on which the idèles are acting so that the Riemann-Weil explicit formula becomes a trace formula. At some point, after reading a paper of Victor Guillemin on foliations and the Selberg trace formula I realized that the space X should be a space of leaves of a foliation and hence a noncommutative space. I remained fascinated by this idea for ten years until after going to a conference in Seattle on the Riemann zeta function, I realized that the space X was already present in my work on quantum statistical mechanics with Bost, and is simply the adèle class space: the quotient of the space of adèles by the action of the multiplicative group of the field. This gives the interpretation of the Riemann-Weil explicit formulas of number theory as a trace formula and the spectral realization of the zeros as an absorption spectrum.

It is still quite far from giving the relevant information on the location of the zeros but it gives a geometric framework in which one can start to transpose the proof of Weil for the case of global fields of positive characteristic. In our joint work with Katia Consani and Matilde Marcolli we have now shown how to understand the spectral realization from a cohomological point of view, compatible with Galois theory. What emerges in particular is that while, as I explained in the first part of the interview, noncommutative spaces generate their own time, this new dynamical feature enables one to cool them down and obtain in this way, when the temperature goes to zero, a set of classical points. Moreover one can refine this thermodynamical procedure and get the analogue of the points over the algebraic extensions of the residue field, and these are organised in the same way as the points of a curve under the action of the Frobenius when dealing with the case of positive characteristic. It is a great challenge for noncommutative geometry now to develop the general conceptual tools allowing to transpose Weil's proof from algebraic geometry to our analytic framework.

My fascination for physics comes from quantum mechanics which, with the discovery of Heisenberg, is at the origin of noncommutative geometry. I have always admired the sophisticated computations physicists do, more specifically those which are motivated by experiment. It is a great motivation to discover that, hidden behind these recipes that physicists are finding from their physics motivation, there are marvellous mathematics. In these recent years the earlier work with Kreimer on renormalization and the Birkhoff decomposition has been pursued further in my collaboration with Marcolli. We discovered a universal group, obtained from a Riemann-Hilbert correspondence, which plays the role of the "cosmic Galois group" that Pierre Cartier had conjectured a few years ago. Indeed it is a universal symmetry group of all renormalizable quantum field theories. It contains the renormalization group of physicists as a one parameter subgroup but has a much richer structure. We have not been able to understand completely its relation with the motivic Galois groups, and in that sense it does not yet



Alain Connes

fully implement the dream of Cartier but deep work of Bloch, Esnault and Kreimer will surely shed more light on that aspect.

For the Standard Model, this work started a few years ago with Ali Chamseddine and it has been pushed further on in my recent collaboration with Chamseddine and Marcolli. It turns out that the incredibly complicated Lagrangian of gravity coupled with the Standard Model is obtained just as pure gravity (of the simplest form, just counting the eigenvalues of the line element) for a spacetime which has a fine structure. Namely it is described not as ordinary 4-dimensional continuum but as the product of an ordinary continuum by a finite noncommutative space of the simplest kind whose effect is to correct the dimension modulo 8 coming from K-theory. It is clear that these are interesting ideas but, so far, they have not passed the experimental test and thus still belong to the realm of pure mathematics.

You have spoken of the relation between mathematics and physics. Could you say something about the relationship between mathematicians and physicists, which is not the same thing?
Yes. It is normal for the true physicist not to worry too much about mathematical rigor. And why? Because one will have a test at the end of the day which is the confrontation with experiment. This does not mean that sloppiness is admissible: an experimentalist once told me that they check their computations ten times more than the theoreticians! However it's normal not to be too formalist. This goes with a certain attitude of physicists towards mathematics: loosely speaking, they treat mathematics as a kind of prostitute. They use it in an absolutely free and shameless manner, taking any subject or part of a subject, without having the attitude of the mathematician who will only use something after some real understanding.

After the heroic period that culminated in the elaboration of the Standard Model, and renormalization of gauge theories, an entire generation of physicists drifted away from the contact with experimental physics in search for a theory that would not only "explain" the Standard Model but also unify it with gravity. And pursuing the idea called string theory, these physicists became mathematicians and had a great impact on mathematics. The objects they manipulate are Riemann surfaces, Calabi-Yau manifolds: and they do mathematics, real sophisticated mathematics. But so far there is no physical test showing any relation between these ideas and the real world. Moreover, because of their origin from physics, the way they proceed is totally different from that of mathematicians.

This is true in particular at the sociological level: they work in huge groups and the amount of time they spend on a given topic is quite short. At a given time t, most of them are going to be working on the same problem, and the preprints which will appear on the web are going to have more or less the same introduction. There is a given theme, and a large number of articles are variations on that theme, but it does not last long. This happened in particular in the relation between string theory and

noncommutative geometry. A herd of people tried to do field theory on a noncommutative space at the beginning of the years 2000, and after a relatively short time, they concluded that field theory on a noncommutative space was not renormalizable, because of the phenomenon of mixing between infrared and ultraviolet frequencies.

This conclusion remained in force for two or three years, but after the pack had moved to another topic, a completely different, very small group of people showed that in fact, the theory was renormalizable, provided one added a missing term in the Lagrangian. This required tremendous insight on the part of the main actors Wulkenhaar and Grosse, and then with Rivasseau, Vignes-Tourneret, Gurau etc... they developed the general theory which is now in a remarkable state, closing on the first effective construction in 4 dimensions. The pack never came back, and continued to move on from one topic to the next.

The sociology of science was deeply traumatized by the disappearance of the Soviet Union and of the scientific counterweight that it created with respect to the overwhelming power of the US. What I have observed during the last two decades since the fall of the USSR and the emigration of their scientific elite to the States is that there is no longer a counterweight. At this point, if you take young physicists in the US, they know that, at some point, they will need a recommendation written by one of the big shots in the country, and this means that if one of them wants to work outside string theory he (or she) won't find a job. In this way there is just one dominant theory and it attracts all the best students.

I heard some string theorists say: "if some other theory works we will call it string theory", which shows they have won the sociological war. The ridiculous recent episode of the "exceptionally simple theory of everything" has shown that there is no credibility in the opponents of string theory in the US. Earlier with the Soviet Union, there was resistance. If Europe were stronger, it could resist. Unfortunately there is a latent herd instinct of Europeans, particularly in theoretical physics. Many European universities, at least in France or England, instead of developing original domains as opposed to those dominant in the United States, simply want to follow and call the big shots in the US to decide whom to hire. It is not by lack of original minds such as my friend and collaborator Dirk Kreimer. But it is a lack of self-confidence of Europe, which means that we are not capable of doing what needs to be done, of resisting and safeguarding this diversity at any price. I don't think that we see similar things in mathematics, so there is a fundamental sociological difference between mathematics and physics. Mathematicians seem very resistant to loosing their identity and following fashion.

In your conversations with Changeux you discussed mathematics and reality. Have you advanced in your thinking about this?

I have no doubt that mathematical reality is something which exists, that it exists independently of my own brain trying to see it, and has exactly the same properties of resistance as external reality. When you want to prove something, or when you examine if a proof is correct or not, you feel the same anguish, the same external resistance as you do with external reality. Some people will tell you that this reality does not exist because it is not "localized" somewhere in space and time. I just find this absurd and I adopt a diametrically opposed point of view: for me even a human being is better described by an abstract scheme than by a material collection of cells – which in any case are totally renewed and replaced over a relatively short period of time and hence possess less meaning or permanence than the scheme itself, which might eventually be reproduced in several identical copies...

If one wants to reduce everything to "matter localized somewhere" one soon meets a wall which comes from quantum mechanics and one finds that this reduction of the outer reality to matter is an illusion that only makes sense at intermediate scales but by no means at a fundamental level. Thus I have no doubt on the subtleness and existence of a reality which can be neither reduced to "matter" nor "localized". Now the question of whether mathematical reality is something created or something pre-existing is much easier to discuss if one uses the distinction which appears in Gödel's theorem between "truth" and "provability" of a mathematical statement. I discussed this in details in my book "Triangle of thoughts" with Lichnerowicz and Schultzenberger and I refer to that book for the detailed argument which is rather involved. I was a bit frustrated after the book "Matière à Pensée" with Changeux, by the lack of an effective communication, and I made a point of writing another book where I could explain better the input coming from Gödel's theorem. There is a fundamental mathematical reality out there, and the mathematician creates tools to understand it.

The relation between the deductions of the mathematician (which –great recent discovery– take place in his brain) and that reality is similar to the relation between the deductions performed in a court as opposed to what actually happens in the real world. It hinges on a fine grammatical distinction between mathematical statements at the level of quantifiers– some are provable if they are true etc... This analogy with the court hall as opposed to external world is perfectly explained in the book of J.Y. Girard on Gödel's theorem. It allows one, after some real work, to get a clear mental picture of the distinction between the role of the mathematician (creating tools to uncover a piece of this reality) and the reality itself.

You have mentioned originality and fashion in mathematicians. Do you have an example?

I had just arrived as a newcomer in IHES [Institut des hautes études scientifiques, in Bures-sur-Yvette, near Paris] in 1976. The first people I met were talking about stuff I just didn't know. I was in the cafeteria and they would discuss "étale cohomology", all kinds of things like that, which, with my culture coming from functional analysis and operator algebras, I didn't know at all.

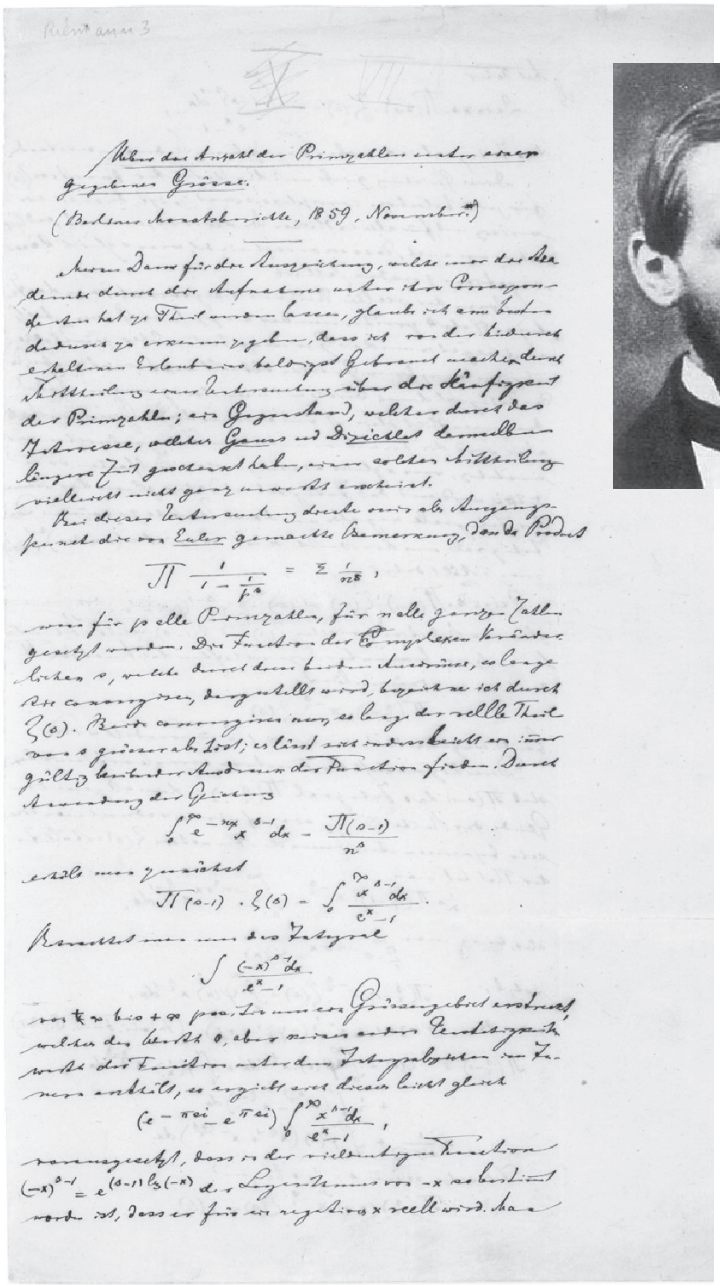
Fortunately, I soon ran into Dennis Sullivan who, as long as he was in Bures, used to go up to any newcomers, whatever their field or personality, and ask them questions. He asked questions that you could, superficially, think off as idiotic. But when you started thinking about them, you would soon realize that your answers showed you did not really understand what you were talking about. He has a kind of Socratic power which would push people into a corner, in order to try to understand what

they were doing, and so unmask the misunderstandings everyone has. Because everyone talks about things without necessarily having cleaned out all the hidden corners. He has another remarkable quality; he can explain things you don't know in an incredibly clear and lucid manner. It's by discussing with Dennis that I learnt many of the concepts of differential geometry. He explained them by gestures, without a single formula. I was tremendously lucky to meet him, it forced me to realize that the field I was working in was limited, at least when you see it as tightly closed off. These discussions with Dennis pushed me outside my field, through a visual, oral dialogue. And not at all through reading texts.

You have talked about the importance of diversity, that people should have different backgrounds. But do you have some ideas about what sort of mathematical common ground everyone should share?

It is a bit subtle. I mentioned the vibrant heart of mathematics. You could say: Why not teach this to everyone? But this would result in a disaster! Because people would end up knowing Riemann surfaces, modular forms, etc, but they would be ignorant of large parts of mathematics, like Hopf algebras or other subjects that might look more esoteric. So, I don't know. I have the impression there should be a minimal common background - fundamental notions of differential and algebraic geometry, algebraic structures, real and complex analysis. Topology, basic number theory ... are all needed. You can't avoid it. People must know that much.

After that, when you want to enter into more elaborate subjects, diversity should be the rule. We have to cultivate original people, as I explained in the first part of the interview, who are able to provide students with a totally original background with respect to this common knowledge. This will give young mathematicians keys, completely personal keys, which will allow them to open their own worlds. If they are lucky, they will be interested by many different things, because it is important for them to be able to flip from one thing to another for a while at



Riemann's paper on zeta

... These works, the ones with this absolute perfection, give you momentum. They give you something which is not only a feeling; they give you an extraordinary power, a force, which allows you to carry on further. It passes something on to you. I have this impression with some papers in mathematics or in physics. Riemann's paper on zeta, Einstein's article on relativity for instance…

the very beginning, until they find a subject that will really inspire them. I think it is important not to go beyond a certain limit for this common background. Then you should find and follow your own line, with an advisor who will allow you to strengthen your own originality. But of course there is no general recipe.

But would you really recommend that a young mathematician learns a lot of mathematics without being a specialist in something?
For a young mathematician, it is absolutely crucial to prove first that he or she is a mathematician. And that means to become a specialist in a topic and prove that you are able to do something very difficult. And this is not compatible with the dream of learning a bit about everything at the same time. Thus after finding the topic that you find enticing it is mandatory to concentrate, perhaps for a number of years, till you make a real dent. Afterwards, of course, once you've succeeded, once you have your passport to do mathematics, it's wonderful if you succeed in enlarging your spectrum to avoid remaining a specialist of a narrow discipline for the rest of your life. But it's very difficult to be a generalist. Because there is the danger of not doing real stuff in mathematics any more.

Do you have some ideas about the way mathematics should be taught?
We must absolutely train very young people to do mathematical exercises, in particular geometry exercises — this is very good training. I find it awful when I see that, in school, kids are taught recipes, just recipes, and aren't encouraged to think. When I was at school, I remember that we were given problems of solid (spatial) geometry. We went to a lot of trouble to solve them. It wasn't baby geometry. These were difficult things, with subtle proofs. And two years earlier, we were doing problems of planar geometry. We used to spend all night doing these problems. And now if you gave the same problems in an exam (the experiment was performed recently) you would be called a murderer! This is no progress. Problems in geometry are easily set, and then you have to go to a lot of trouble to find a proof.

It's a shame we don't do it anymore. I saw recent high-school problems, in which you define groups of rotations, rotations being equivalence classes... staying at a prehistorical level of sophistication just because of the heavy weight of the "formalism"... This is dreadful... Because geometry involves drawing figures, it should be directly accessible. Unfortunately, it's not impossible that this exaggerated use of mathematical formalism was inadvertently inherited from Bourbaki - who does not define real numbers until chapter 9 of Topology, long after defining uniform structures…

You mention Bourbaki. How do you judge now Bourbaki's role?
Bourbaki played a phenomenal role. You can't deny he transformed many subjects – in which the deepest obscurity reigned – into fields of an incredible clarity. There are some marvellous books by Bourbaki: Algebra Chapter III and all the volumes on Lie groups, you can only be dumfounded with admiration. Now, once all this has been done, it's done. There are still fields where something of the sort could have been done and was not done. But I don't think that doing more of it would make a big difference. All in all, Bourbaki had such a great influence in giving us a concern for clarity and rigor that the beneficial effect has already occurred. If Bourbaki hadn't been there, mathematics would have drifted towards lots of results that you could not rely on.

Do you think that it would be possible now to launch such an ambitious and unselfish project?
Unselfish to that degree now is not an obvious thing, since everybody is so busy with all sorts of "things to do". There was a marvellous spirit in the beginning of the Bourbaki group, an idea of unselfish service to the community. I participated for a short period at the end of the seventies. I wrote some drafts but what stopped me to continue was when I realized that, in a room in Ecole Normale, there were hundreds of manuscripts, 100 to 150 pages each, which would never see daylight. I found that depressing. Of course there were partial duplicates... but there was such a demand for perfection before the content would be published, that finally it was as if these texts didn't exist. Time passed, and as time passed, they became obsolete. There is this incredible dedication of Bourbaki members in writing drafts. When a manuscript is finished, it is true that you have learned a lot, you understand things better, but if the text never appears you get a real feeling of frustration. For a very long time Dieudonné was playing a key role to ensure that things would converge at some point, but after he left a lot of the efficiency left with him somehow.

What are you working on now?
Just at this time I am working on hard analysis which has to do with the spectral axioms of noncommutative geometry. This is the content of my class in College de France this year and it is a lot of technical work but also a welcome diversion. Just before this diversion I had reached, after we handed out the manuscript of our book with Matilde Marcolli, an obsessive mental state due to the inevitable risk of some mistake in such a large body of work. Of course one can check things and try to view them from all sorts of different angles, but for instance as soon as it touches physics the difficulties pile up since the accuracy of the calculations one does is not enough to ensure that they will have any "meaning" for the real world and pass the reality test. In that respect, I try to share the attitude of the great physicist Pierre-Gilles de Gennes when he said:

> *"Le vrai point d'honneur n'est pas d'être toujours dans le vrai. Il est d'oser, de proposer des idées neuves, et ensuite de les vérifier. Il est aussi, bien sûr, de savoir reconnaître publiquement ses erreurs. L'honneur du scientifique est absolument à l'opposé de l'honneur de Don Diègue. Quand on a commis une erreur, il faut accepter de perdre la face."*

What certainly matters, in what we do, is to try to constantly put one's ideas to the test and see what happens. Nothing better than waking up in the middle of the night in that respect. And one should not be afraid. Here is

what Alexandre Grothendieck writes in his unpublished book "Récoltes et Semailles" about this:

> *"Craindre l'erreur et craindre la vérité est une seule et même chose. Celui qui craint de se tromper est impuissant à découvrir. C'est quand nous craignons de nous tromper que l'erreur qui est en nous se fait immuable comme un roc. Car dans notre peur, nous nous accrochons à ce que nous avons décrété "vrai" un jour, ou à ce qui depuis toujours nous a été présenté comme tel. Quand nous sommes mûs, non par la peur de voir s'évanouir une illusoire sécurité, mais par une soif de connaître, alors l'erreur, comme la souffrance ou la tristesse, nous traverse sans se figer jamais, et la trace de son passage est une connaissance renouvelée"*

How do you read mathematics?
The only way I manage to read mathematics is extremely slow because I read a statement and then I try to think about it. I can't understand a proof if I haven't tried to prove it myself before. Once I've been stumped a long time on a result, I can understand it in seconds while scanning the proof; I see the one place where something happens and which I couldn't guess before. The problem is that this method of reading is very slow, I need an enormous amount of time to make myself familiar with the result. I am almost unable to read a mathematical book linearly. A discussion or a talk, on the contrary, allow me to go faster. But I am aware that other mathematicians function in a very different way.

Is it the same with physics?
No, it's totally different. In physics I adore reading; I spent about fifteen years studying the book of Schwinger, *Selected Papers on Quantum Electrodynamics*. He collected all the crucial articles, by Dirac, Feynman, Schwinger himself, Bethe, Lamb, Fermi, all the fundamental papers on quantum field theory, those of Heisenberg too, of course. This has been my bedside book for years and years. Because I have always been fascinated by the subject and I wanted to understand it. And that took a very long time to understand. Not so much to understand the detail of the articles, but to understand what they meant, what mathematics were behind them. In physics, then, I have a totally different reaction. I have not at all this inability to read. It's strange. I think there is a possible reason: in mathematics I need to protect myself more, in some ways. In physics, I don't feel this need.

And outside science? Would you like to speak about something else, music, art ?

These last two years, I no longer had time because I had to work harder, but before I used to take lessons in drawing and in piano. What struck me in music was to see how some composers had reached an incalculable level of perfection in their art. In studying some scores, I was struck to realise that you learn as much as in reading some mathematical papers. Simply because of the level of sophistication. This is not a question of analogy between mathematics and music. Some composers reached, by an hallucinatory work of precision, a level of perfection close to that of some of Riemann's work.

And faced with this level of perfection I react in the same way, a feeling of admiration - but an admiration which creates motion, something which is not at all static: beauty plus perfection puts thought into motion, it forces you to think. This perfection in the form of a work of art is of course very rare. To take an example, this time in literature, there is a striking difference of "form" between [Flaubert's] *Madame Bovary* and [Balzac's] *Le lys dans la vallée*. Madame Bovary is absolute perfection, a marvel of precision which is the outcome of a phenomenal amount of work, while the other is a bit botched. Le lys dans la vallée contains also marvellous stuff but there's an obvious difference in appearance.

I often have this impression when I look at mathematical papers or art works, that I feel intensely this distinction. Some pieces stand out way above the others, one gets the feeling that the author, instead of stopping at time t and saying, "fine, that will do, I'll hand in my stuff" (Balzac was forced to do that, he had a knife at his throat, he had no choice) just kept working until reaching something which is close to absolute perfection.

This is mainly what I feel about art. These works, the ones with this absolute perfection, give you momentum. They give you something which is not only a feeling; they give you an extraordinary power, a force, which allows you to carry on further. It passes something on to you. I have this impression with some papers in mathematics or in physics. Riemann's paper on zeta, Einstein's article on relativity for instance… There are few of them, very few. They put the level of writing standards so high. It's marvellous. You see something and you really understand. This is an extraordinary instrument for understanding and, beyond the clarity, you feel something which puts you in motion. It tells you: Go on.

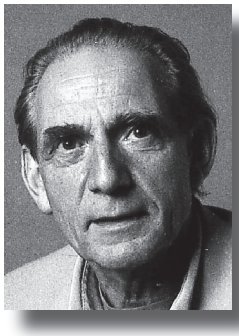
Alain Connes is a Professor at the Collège de France, IHES and Vanderbilt University. Among his awards are a Fields Medal in 1982, the Crafoord Prize in 2001 and the CNRS Gold Medal in 2004.

Catherine Goldstein [cgolds@math.jussieu.fr] is Directrice de recherches at the Institut de mathématiques de Jussieu. Her research projects lie in the history of mathematics, in particular of number theory. She recently coedited 'The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae' and currently works on the impact of World War I on mathematical sciences.

Georges Skandalis [skandal@math.jussieu.fr] is Professor at Université Paris Diderot – Paris 7 and the Institut de mathématiques de Jussieu. His main research subject is non commutative geometry. He currently studies singular foliations and the associated index theory. He is Alain Connes' former student.

MatematikerNyt

ved Mikael Rørdam



Ib Madsen bliver pr 1. september 2008 ansat som professor ved Institut for Matematiske Fag, Københavns Universitet. Ib Madsen er videre den ene af blot to danske modtagere af de meget eftertragtede European Research Chair Advanced Grants fra det europæiske forskningsråd. Han modtager herfra cirka 12 millioner til forskningsudgifter og egen løn startende i begyndelsen af 2009 i 5 år. Grantet er søgt gennem det Naturvidenskabelige Fakultet ved Københavns Universitet.

Ib Madsen er uddannet Cand. Scient. fra Københavns Universitet (1965), og PhD fra University of Chicago (1970). Siden 1971 har han været ansat først som lektor og siden som professor ved Aarhus Universitet. Hans forskning er indenfor mange forskellige områder af algebraisk topologi. I 1978 var han inviteret foredragsholder ved den internationale kongres ved Helsingfors universitet, hvor han talte om løsningen af det topologiske rumforms problem. I 2006 var han plenarforedragsholder ved den internationale kongres i Madrid hvor han talte om løsningen af Mumford formodningen.

Ib Madsen har været vejleder for et stort antal meget succesrige studerende, Erkki Laitinen, Marcel Bokstedt, Steffen Bentzen, Jan-Alve Svensson, Kenneth Hansen, Lisbeth Fajstrup, Lars Hesselholt, Christian Schlichtkrull, Kåre Nielsen, Søren Galatius og Søren Boldsen (forventet færdig 2009).

Wojciech Szymanski arrived in the beginning of August 2008 at Odense to take up a position of lektor in Mathematics/Operator Algebras at the University of Southern Denmark.

Wojciech obtained his M.Sc. degree in mathematics from Warsaw University, laura cum laude (1985) under the direction of prof. Jan Kisynski and dr. Wojciech Chojnacki. His doctoral thesis (1994) was written at the University of Cincinnati under the direction of prof. Costel Peligrad and entitled 'Hopf algebra actions on C*-algebras and von Neumann algebras'.

From 1994 until the present appointment he worked for the University of Newcastle in Australia, most recently as senior lecturer. His research interests include various aspects of theory of operator algebras and their applications to noncommutative geometry.

After work, Wojciech enjoys hiking, music, movies or a game of chess.

Jørgen Ellegaard Andersen er pr. d. 1/4 2007 ansat som professor ved Institut for Matematiske fag ved Aarhus Universitet. Jørgen er uddannet Cand. Scient. i matematik (1989) fra Syddansk Universitet og tog derefter til Oxford, studerede ved Nigel Hitchin, John Roe og Simon K. Donaldson, og blev D.Phil i 1992.

Fra Oxford blev Jørgen ansat som C.B. Morrey Jr. Assistant Professor ved UC-Berkeley og blev samtidig ansat som adjunkt ved Aarhus Universitet. Den følgende tiårige periode delte Jørgen mellem de to steder, det ene år ansat af the Clay Mathematics Institute. Ansættelsen i Aarhus overgik til en lektor ansættelse i 1997.

I 2006 blev Jørgen udnævnt til centerleder for Center for Topologien og kvantisering af Modulirum (CTQM), som blev oprettet på basis af en centerbevilling fra FNU samt bevillingen »The Niels Bohr Visiting Professorship Initiativ« fra Danmarks Grundforskningsfond for at tilknytte Professor Nicolai Reshetikhin (UC Berkeley) til centeret. Jørgen er også leder den nationale Ph.d.-skole »Geometry and Mathematical Physics School (GEOMAPS)«, med fokus på interaktioner mellem geometri og matematisk fysik, og som inkluderer forskere fra Københavns, Syddansk Universitet og Aarhus universiteter. Skolen er finansieret af Forsknings og Innovationsstyrrelsen.

Jørgens forskning er indenfor geometri og topologi med fokus på kvantisering af modulirum og med relationer til kvantefeltteori og streng teori indenfor teoretisk fysik. Specielt arbejder han med den geometriske kvantisering af modulirummet af flade konneksioner på Riemann Flader og Hitchin's konneksion, som danner den geometrisk model for Witten's og Reshetikhin-Turaev's topologiske kvantefeltteori (TQFT). Blandt hans vigtigste resultater, som har interessante konsekvenser for afbildningsklassegruppen og knudeteori, er den asymptotiske analyse af disse kvantefeltteorier ved brug af Toeplitz operator teknikker.

Jørgen er redaktør for "Journal of Knot Theory and its Ramifications" og "Geometria Dedikata".

Fritiden bruges på volleyball, tennis samt på at rejse.

Magdalena Musat took up a lektor position in the Operator Algebras group at the University of Southern Denmark on July 1, 2008. .

Magdalena got a Diploma in Mathematics in 1993 from the University of Bucharest. In 2002 she obtained her Ph.D. from the University of Illinois at Urbana-Champaign, under the supervision of Professors Donald Burkholder and Marius Junge. Her doctoral thesis was titled "On the operator space UMD property and non-commutative martingale inequalities".

After her Ph.D., Magdalena spent three years at the University of California, San Diego as a Warschawski Visiting Assistant Professor, and then joined the Mathematics Department at the University of Memphis on a tenure-track position in 2005. During the spring of 2006 and 2007 she held postdoctoral positions at the University of Southern Denmark.

Her main research interests are in the fields of non-commutative probability, von Neumann algebras and operator spaces, with a focus on non-commutative Lp-spaces and inequalities for non-commutative martingales. She has also carried out research in classical potential theory.

Referat af DMFs Generalforsamling 2008

RUC, Mandag d. 28. april 2008

1. Dirigent. Som dirigent valgtes Erik Christensen, KU. Dirigenten konstaterede at generalforsamlingen var lovligt indkaldt.

2. Formandens beretning. Den afgående formand, Søren Eilers, KU, berettede om året 2007 for Dansk Matematisk Forening. Specielt fremhævede Eilers flytningen af arkivalia fra det pladsmæssigt trængte H.C.ÿrstedinstitut til arkiver ved institutterne i Odense og ≈rhus. Det faglige møde 'Joint Mathematical Weekend' var en succes. Specialeprisen er nu en realitet, og den første specialepris skal uddeles ved årsmødet i 2008. Foreningens nyhedsbrev Matilde udkommer regelmæssigt, takket være en energisk indsats fra frivillige redaktører.

3. Regnskab. Kasseren, Carsten Lunde Pedersen, RUC, fremlagde det i årsberetningen udsendte regnskab. Foreningens økonomi er god, og årsregnskabet 2007 udviser sågar et lille overskud. Foreningen har i 2007 støttet forskellige former for ungdomsarbejde, bl.a. `Math Camp' afholdt ved SDU i Odense. Nyhedsbrevet Matilde er fortsat den store post i budgettet. Generalforsamlingen godkendte regnskabet.

4. Budget. Kasseren fremlagde et budget for 2008 som i alt væsentligt ligner budgettet for 2007. Efter en kort diskussion af medlemstallets udvikling godkendte generalforsamlingen budgettet for 2008.

5. Ny formand. Dirigenten konstaterede at revisorerne fortsatte, og gik derefter over til sammensætningen af den ny bestyrelse. Vagn Lundsgaard Hansen, DTU, blev forslået som formandskandidat, og modtog valget. Den ny bestyrelse er herefter

Vagn Lundsgaard Hansen, DTU, (Formand)
Carsten Lunde Pedersen, RUC, (Kasser)
Jørgen Ellegaard Andersen (AU)
Leif Kjær Jørgensen(AAU)
Henrik Schlichtkrull (KU)
Bjarne Toft (SDU)
Poul G. Hjorth DTU (Næstformand og Sekretær) [sidste vaglperiode]

Afgående bestyrelsmedlemmer er Søren Eilers (KU), Henrik Gordon Petersen (SDU), Johan P. Hansen (AU) og Andrew Swann (SDU).

6. Æresmedlem. Bodil Branner (DTU), tidligere formand for Dansk Matematisk Forening, blev udnævnt til æresmedlem. Bodil Branner holdt en kort takketale.

7. Eventuelt.

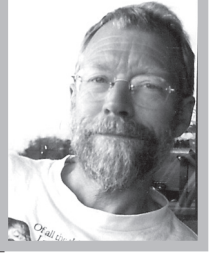
7.1.Martin Raussen (AAU) blev udpeget som foreningens repræsentant i EMS Executive Committee.

7.2 Foreningens nye bestyrelse overvejer formatet for at bidrag fra DMF til matematik i udviklingslandene.

Referent: Poul G. Hjorth, DTU

Aftermath

ved Mogens Esrom Larsen

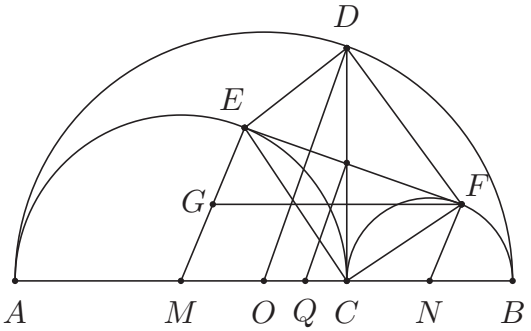


LØSNINGER

Opgaverne i sidste nr. er hentet fra Loren C. Larson, Problem–Solving Through Problems, Springer 1990. Ebbe Thue Poulsen og problemklubben "Con Amore" har indsendt løsninger.

Firkantet

Opgaven er løst af TP og CA.



Lad C være et vilkårligt punkt på liniestykket AB mellem A og B, og tegn halvcirkler til samme side over diametrene AB, AC og CB. Lad D være det punkt på halvcirklen AB, der har CD vinkelret på AB, og lad EF være fællestangenten til de to små halvcirkler.

Vis, at $ECFD$ er et rektangel.

For at bevise, at $ECFD$ er et rektangel, vil jeg bevise, at diagonalerne CD og EF er lige lange og halverer hinanden.

Af symmetrigrunde kan vi antage $R \geq r$, og da tilfældet $R = r$ er såre nemt, vil jeg nøjes med at se på tilfældet $R > r$.

Man ser, at $|MO| = (R+r)-R = r$, $|OC| = R - r$, og $|MN| = R + r$. Da radierne ME og NF er vinkelrette på fællestangenten EF, er de parallelle. Lad punktet G på ME være bestemt således, at $GF \| MN$. Så er $MNFG$ et parallelogram, og der gælder $|GF| = |MN| = R + r$, $|MG| = |NF| = r$, og altså $|GE| = R - r$.

I de retvinklede trekanter $\triangle OCD$ og $\triangle GEF$ gælder om hypotenuserne $|OD| = R + r = |GF|$, og om kateterne $|OC| = R - r = |GE|$. Altså er $\triangle OCD$ kongruent med $\triangle GEF$, og følgelig er $|CD| = |EF|$ som var den ene af de to påstande, jeg ville bevise.

Jeg skal også bevise, at CD og EF har samme midtpunkt. Lad Q være midtpunktet af OC. Den midtpunktstransversal i $\triangle OCD$, der forbinder Q med midtpunktet af CD har længde $\frac{1}{2}|OD| = (R+r)/2$, og den er parallel med OD.

Nu er Q også midtpunkt af siden MN i trapezet $MNFE$, så den midtpunktstransversal i dette trapez, der forbinder Q med midtpunktet af EF har længde $\frac{1}{2}(|ME| + |NF|) = (R+r)/2$, og den er parallel med ME og NF.

Vender vi tilbage til kongruensen mellem trekanterne $\triangle OCD$ og $\triangle GEF$, får vi, at $\angle COD = \angle EGF$, og altså, at OD er parallel med ME. Heraf ses, at de to omtalte midtpunktstransversaler er sammenfaldende, og altså, at midtpunkterne af linjestykkerne CD og EF er sammenfaldende.

Trekantet

Opgaven er løst af TP og CA.

En trekant er tegnet på ternet papir, så alle tre hjørner er i skæringspunkter (punkter med heltallige koordinater). Lad nu r være antallet af skæringspunkter på randen og i antallet af skæringspunkter i det indre af trekanten. Vis, at arealet af trekanten er

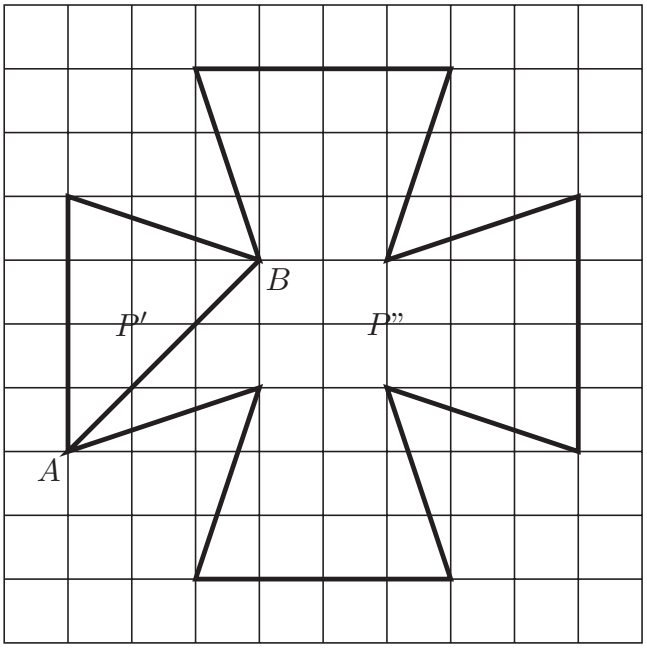
$$i + \tfrac{1}{2}r - 1$$

Jeg vil bevise, at formlen gælder ikke blot for trekanter, men for vilkårlige "gitterpolygoner", dvs polygoner med hjørner i gitterpunkterne. For en vilkårlig gitterpolygon P defineres $f(P) = i + \frac{1}{2}r - 1$, hvor i er antallet af gitterpunkter i det indre af P, og r antallet af gitterpunkter på randen.

Jeg skal bevise, at $f(P) = a(P) =$ arealet af P for enhver gitterpolygon P.

Lemma. *Hvis P er delt i to delpolygoner P' og P'' ved et linjestykke, der forbinder to gitterpunkter A og B på randen af P, så er*

$$f(P) = f(P') + f(P'')\,.$$



Bevis: Lad i, i', og i'' hhv r, r', og r'' betegne antallet af indre gitterpunkter hhv randgitterpunkter for P, P', og P'', og lad i^* betegne antallet af indre gitterpunkter i P, som tilhører linjestykket AB.

Så er

$$i = i' + i'' + i^*\,,$$

og da A og B tæller med både i r' og r'', er

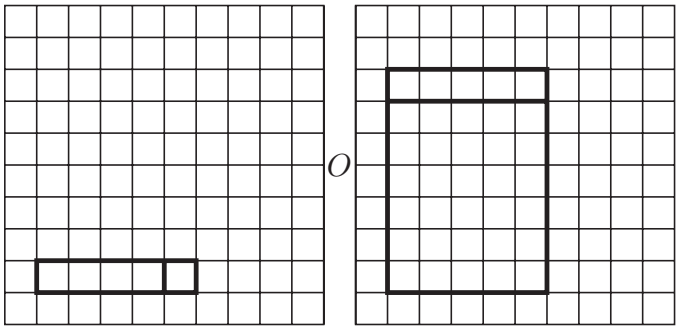
$$r = (r' - i^*) + (r'' - i^*) - 2\,,$$

og (1) følger.

Bevis for, at $f(P) = a(P)$:

(a) Hvis P er enhedskvadratet, er $f(P) = a(P)$. Bevis: $i = 0$, $r = 4$

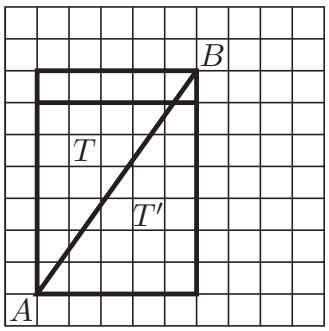
(b) Hvis P er et akseparallelt rektangel med sider m og n, er $f(P) = a(P)$.



$m = 5, \quad n = 1$ $\qquad$ $m = 5, \quad n = 7$

Bevis: Først induktion efter m med $n = 1$, derefter induktion efter n med m fast.

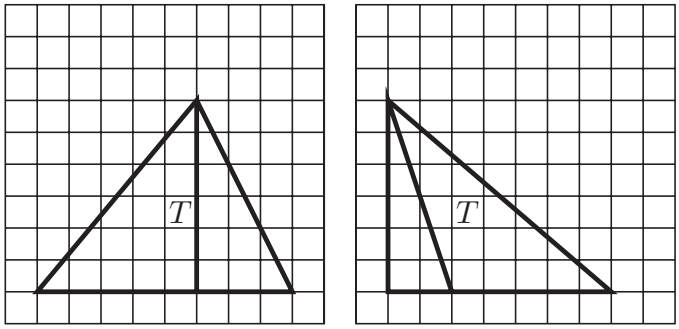
(c) Hvis T er en trekant med to akseparallelle sider, er $f(T) = a(T)$.



Bevis: Lad P være det rektangel, der fremkommer, når man tegner akseparallelle linjer gennem den tredje sides endepunkter A og B. Så deler linjestykket AB rektanglet P i to trekanter T og T'. Af symmetrigrunde er $f(T) = f(T')$ og $a(T) = a(T')$, og af (1) og (b) følger, at

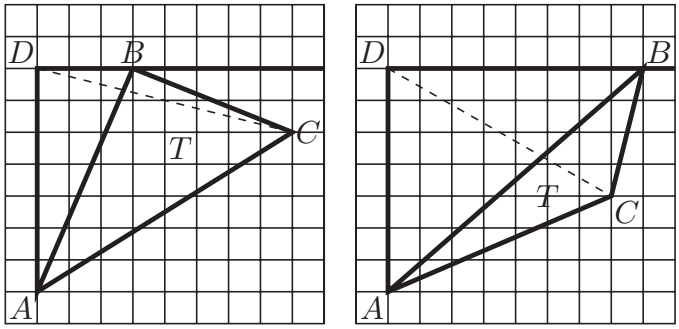
$$f(T) = \frac{f(T) + f(T')}{2} = \frac{f(P)}{2} = \frac{a(P)}{2} = a(T)\,.$$

(d) Hvis T er en trekant med én akseparallel side, er $f(T) = a(T)$.



Bevis: T er enten foreningsmængde af eller differens mellem to trekanter, der begge har to akseparallelle sider.

(e) Hvis T er en trekant uden en akseparallel side, er $f(T) = a(T)$.



Bevis: Lad R være det mindste akseparallelle rektangel, der indeholder T. Da hver af R's sider indeholder præcis n af T's vinkelspidser, er der en af T's vinkelspidser (A), der samtidig er vinkelspids i R, medens der om de to andre vinkelspidser i T gælder enten, at de ligger på hver sin af R's øvrige sider, eller, at en af dem (B) er sammenfaldende med den vinkelspids i R, der er over for A, og den anden i det indre af R.

Lad vinkelspidsen D i R være bestemt således, at $ADBC$ er en konveks firkant (se figurerne). Så er

$$\begin{aligned} f(T) &= f(ADC) + f(DBC) - f(ADB) \\ &= a(ADC) + a(DBC) - a(ADB) \\ &= a(T)\,. \end{aligned}$$

(f) Hvis P er en vilkårlig gitterpolygon, er $f(T) = a(T)$.

Bevis: P deles i trekanter.

Dette er Picks sætning (1899), Georg Alexander Pick (1859-1942).

Eksponentielt

Opgaven er løst af TP og CA.

Når man får at vide, at tallet 2^{29} er 9–cifret, og at de 9 cifre alle er forskellige, kan man så uden at udregne tallet bestemme, hvilket ciffer der mangler?

Vi har

$$2^{29} = 2^2 \times (2^3)^9 \equiv 4 \times (-1)^9 = -4 \pmod 9$$

og

$$0 + 1 + 2 + \cdots + 9 \equiv 0 \pmod 9,$$

og altså må det manglende ciffer være 4.

Kvadratisk

Opgaven er løst af TP og CA.

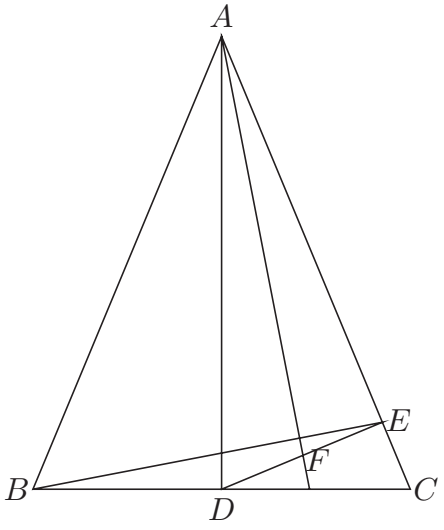
n er et helt tal, så $2n + 1$ er et kvadrattal. Vis, $n + 1$ er sum af to sukcessive kvadrattal.

Hvis det ulige tal $2n+1$ er et kvadrattal m^2, er m ulige: $m = 2k+1$, og $2n+1 = 4k^2+4k+1$, der giver

$$n + 1 = 2k^2 + 2k + 1 = k^2 + (k + 1)^2\,.$$

Trekantet

Opgaven er løst af TP og CA.



Trekanten $\triangle ABC$ er ligebenet med $AB = AC$, D er midtpunktet på BC, E på AC er det punkt, hvor ED er vinkelret på AC og F er midtpunktet af DE.

Vis, at AF står vinkelret på BE.

I trekanterne $\triangle EDA$ og $\triangle ECD$ er tilsvarende sider vinkelrette på hinanden: $ED \perp EC$, $DA \perp CD$, og $AE \perp DE$. Det følger, at trekanterne er ensvinklede og derfor ligedannede, og man ser, at en rotation omkring E med vinklen $\frac{\pi}{2}$ efterfulgt af en multiplikation i forholdet $|EC| \,/\, |ED|$ fører $\triangle EAD$ over i $\triangle EDC$. Ved denne afbildning føres ED's midtpunkt F over i EC's midtpunkt G, og AF føres over i DG.

Altså er $AF \perp DG$, og da DG som midtpunktstransversal i $\triangle BEC$ er parallel med BE, er AF vinkelret på BE, QED.

Heltalligt

Opgaven er løst af TP og CA.

Givet et naturligt tal, n, bestem antallet af firsæt, (a, b, c, d), så at $0 \leq a \leq b \leq c \leq d \leq n$.

Transformeres talsættet til $(a, b+1, c+2, d+3)$ kan spørgsmålet ændres til at bestemme antallet af firsæt, (a, b, c, d), så at $0 \leq a < b < c < d \leq n+3$. Og dette antal er $\binom{n+4}{4}$.

Polynomielt

Opgaven er løst af TP og CA.

Lad a, b og c være ulige, hele tal. Vis, at ligningen

$$ax^2 + bx + c = 0$$

ikke kan have en rational rod.

Lad $x = p/q$ være et vilkårligt rationalt tal skrevet som en uforkortelig brøk. Så er

$$ax^2 + bx + c = \frac{ap^2 + bpq + cq^2}{q^2},$$

og da p og q ikke begge kan være lige, indeholder tælleren enten 0 eller 2 lige led, dvs tælleren er ulige, og derfor $\neq 0$.

Beviset fungerer for enhver ligning af formen $ax^m + bx^n + c = 0$ med $1 \leq n < m$.

NYE OPGAVER

En tryllekunst

Tryllekunstneren og hans assistent præsenterer publikum for 8 mønter på en række. Tryllekunstneren instruerer publikum om opgaven og forlader lokalet. Publikum vælger nu for hver mønt, om den skal være krone eller plat. Derefter oplyser publikum assistenten om deres foretrukne mønt, fx nr 5 fra venstre. Nu vender assistenten én af mønterne om efter sit valg.

Tryllekunstneren kommer ind fra kulissen og udpeger den foretrukne mønt.

Hvordan bærer de sig ad? Hvad er den hemmelige kode?

En sum

I Amer. Math. Monthly April 2008 stilles som problem 11356 en opgave af Michael Poghosyan, Yerevan State University, Yerevan, Armenien.

Vis identiteten

$$\sum_{k=0}^{n} \frac{\binom{n}{k}^2}{(2k+1)\binom{2n}{2k}} = \frac{2^{4n}(n!)^4}{(2n)!(2n+1)!}$$

Sokker, der passer til hinanden

Når sandsynligheden for at få to røde sokker er $\frac{1}{2}$, når man trækker to tilfældigt ud af en sæk med røde og sorte sokker, hvor mange er der så af hver farve i sækken?

Travle duellanter

Duellerne i Travløse er sjældent fatale. Hver kombattant møder op på et tilfældigt tidspunkt mellem 5 og 6 om morgenen på den aftalte dag, venter 5 min på sin modstander, og går igen, hvis denne ikke er mødt op. Ellers slås de to.

Hvad er sandsynligheden for, at det kommer til kamp?

Ved uanbringelighed returneres bladet til afsender:

Matilde
Institut for Matematiske Fag
Aarhus Universitet
Ny Munkegade Bygning 1530
8000 Århus C

POST B
PP DANMARK