FAMØS

FAMØS marts 2012
Fagblad for Aktuar, Matematik,
-Økonomi og Statistik ved Københavns Universitet

Tegnere:
Maria Bekker-Nielsen Dunbar (forside)
Kristian Knudsen Olesen (side 31)

Deadline for næste nummer:
20. maj 2012

Indlæg modtages gerne og bedes sendt
til famos@math.ku.dk – gerne i LaTeX
og gerne baseret på skabelonen
som kan hentes på hjemmesiden.

FAMØS er et internt fagblad.
Eftertryk tilladt med kildeangivelse.

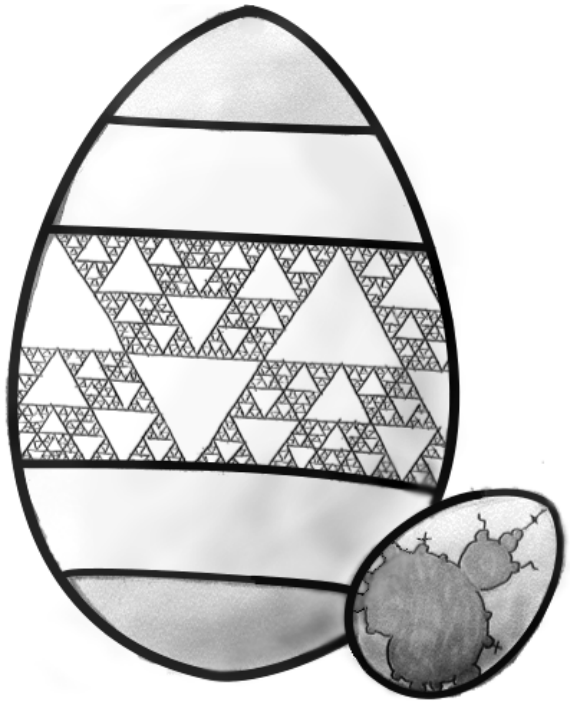
Fagbladet FAMØS
c/o Institut for Matematiske Fag
Matematisk Afdeling
Universitetsparken 5
2100 København Ø
http://www.math.ku.dk/famos/

Oplag: 400 stk.
ISSN: 1903-2227

21. årgang, nr. 3, marts 2012

FAMØS

Fagblad for Aktuar, Matematik, -Økonomi og Statistik
21. årgang, nr. 3, marts 2012



Mit lemma står med prikker: ... .

Redaktion

⋆ Bo 'Maling' Malling Christensen,
⋆ Frederik Möllerström Lauridsen,
⋆ Jens Siegstad,
⋆ Jingyu She,
⋆ Kristian Knudsen Olesen,
⋆ Kristian Peter Poulsen,
⋆ Maria Bekker-Nielsen Dunbar,
⋆ Martin Patrick Speirs,
⋆ Søren Knudby,
⋆ Søren Wengel Mogensen

This page is not not intentionally left blank.

Hilsen L. E. J. Brouwer

Indhold

21. årgang, nr. 3

Sådan smager dit nærmiljø

– Vi afprøver diverse caféer og madsteder i nærheden af HCØ, så du tør tage chancen og prøve noget nyt

Rie Jensen og Katrine Gravesen

Nørrebros hjerte, Runddelen byder på alt hvad hjertet begærer. Denne udgave af FAMØS' egen gastronomiske inspiration tager dig en tur til dette velkendte og befolkede sted. Her tilbydes både lidt til den sunde og den søde tand, og vi guider dig gennem nogle af Runddelens muligheder.

Det Grønne Køkken, ★★★★☆☆

Efter flæskesteg og risengrød (hos GrødGutterne) er slankesæsonen nu gået i gang. Bikinen skal snart frem fra skabet, og måske vil du gerne lige tabe et par kilo. Desværre er salaten dyr i kantinen og du orker ikke selv at snitte og hakke. Derfor skal du besøge *Det Grønne Køkken* på Nørrebrogade 140. Her er der salat for alle pengene og mere til. I montren ved indgangen findes et udvalg af mellem 15 og 20 forskellige salater. Afhængigt af hvor sulten og nysgerrig man er, kan man vælge at blande forskellige antal af salater og der er også mulighed for at få dem med i en praktisk plastikbakke. Dette koster ikke ekstra og er velegnet til studerende med en travl kalender og sulten mave. Stedet er meget populært omkring frokosttid, men betjeningen er hurtig og høflig. Vi fik forskellige salater heriblandt broccolisalat, tunmousse, græsk fetasalat og bulgursalat, som alle var lækre og meget smagfulde. Til salaten får man tilbudt brød. I menuen står der, at dette koster 2 kr., men vi fik brødet med gratis. At blande tre salater koster 49 kr. og en menu med hotwings og to salater fås til 59 kr. Vi fik meget for pengene og blev meget mætte (og følte os virkelig sunde!) efter besøget. Til sin menu kan man også vælge frikadeller eller kyllingefileter. Derudover kan man købe bagels og

betingelsen.

Problemet er, at den bagvedliggende kvotient for Misère spil ikke er den samme for alle spil, strukturen er en monoid, altså en gruppe uden invers, og den kan ikke findes ved ækvivalens over alle spil.

Men lige netop for *Misère Nim* findes der en enkel metode, som Bouton faktisk fandt: *Spil, som du ville spille Nim, med mindre du efterlader lutter stakke á 1 pind. I den givne situation: sørg for at efterlade et ulige antal stakke á 1 pind.* Metoden kan benyttes på flere Misère spil.

Hvis den metode virker, kaldes spillet for et *tamt* Misère spil.

De forsøg på at finde kvotienten, som blev gjort før år 2000, prøvede at finde en ækvivalens under alle spil. Desuden har det sandsynligvis været svært at acceptere den manglende invers. Løsningen kom omkring år 2005 og blev givet af T. E. Plambeck og A. N. Siegel.
Det er spændende læsning med en algebraoplysende bivirkning.

Introduktion til kombinatorisk spilteori fås i bogen Lessons in Play (A. K. Peters, 2007).

side 4, der svarer til: $(\ldots, 0, 1, 1) + (\ldots, 0, 0, 1) = (\ldots, 0, 1, 0)$.

Piet Heins kompenserede sit tab af Nim var ved at udvikle et nyt kombinatorisk spil, Nimbi, der ikke så let lod sig løse. I Nimbi kan additionen først benyttes relativt sent i spillet, hvilket gør det besværligt at reducere.

En miserabel situation

Kender du „Sidste år i Marienbad“ godt, vil du måske indvende, at der gjaldt det jo om at ikke tage den sidste pind, hvilket også er den traditionelle måde at spille på.

Vinderbetingelsen er altså vendt om — Kaldet *Misère*. Bouton mål var faktisk at løse denne type *Nim*, men det er mere besværligt, for hvor alle upartiske spil kan relateres til en Nim-stak, via en Nimværdi, så er det ikke tilfældet, når vinderbetingelsen vendes.

For at eksemplificere problemet, tag spillet, G, som er 2 stakke á 2 pinde, for nemheds skyld skrevet, $G = (2, 2)$. Det er en taberposition, uanset hvilken vinderbetingelse man benytter. Under den almindelige vinderbetingelse er Nimværdien 0. Hvilken Nimværdi bør den have under Misère?

Nimværdien 0 er en dårlig kandidat, da spillet H, som er stakken bestående af 0 pinde, er en vinderposition under Misère. Altså er $o(H + 0) \neq o(G + 0)$ — Tilsvarende argument gælder for $H = (2), \ldots, H = (n)$. Tilbage er $H = (1)$, stakken bestående af 1 pind: Problemet med den er, at $o(G + G) \neq o(H + G)$.

Kompleksiteten under den nye vinder betingelse synliggøres ved at se på antallet af spil af en given længde: Der er op til isomorfi ved nimværdier (ækvivalens) kun 6 almindelige spil af længde maks 5: stakkene 0 til 5, mens der er over 4 millioner under Misère

sandwich, som begge ser meget lækre (og sunde!) ud. Alt i alt er maden god, men stedet er ikke velegent til lange frokoster. Tag derfor maden med dig og nyd det nye sunde (!) liv.

Cortado Kaffebar ★★☆☆☆☆

Er du træt af at høre om slanketips og salat? Og har du mere lyst til kage og forkælelse? Dette findes også ved Runddelen. *Cortado* ligger ved siden af den gamle McDonalds (Nørrebrogade 122), som nu er blevet til Lagkagehuset. Indretningen på caféen er meget lig den på *Kaffekilden*, som den flittige læser kender fra sidste nummer af FAMØS. Der er også fri adgang til internettet, spil og forskellige blade. Dog følger stemningen ikke helt med på samme niveau. Der er højt til loftet, men dette gør desværre, at hyggen forsvinder en smule. Ligeledes er standarden på *Cortado* ikke så høj. Vi smagte en mørk drømmekage, som mildt sagt ikke smagte af noget som helst. De 30 kr. ville være givet bedre ud til en pulverblanding af Guf-kage fra Netto. Til kagen fik vi iskaffe og islatte. Disse var betydelig bedre end kagen og havde været en bedre oplevelse alene. Til en pris på 40 kr., og heraf trækkes 15% i studierabat, er dette et udmærket køb og absolut at anbefale. Desværre blev oplevelsen og stemningen bare aldrig rigtig hyggelig, og vi forlod derfor caféen rimelig hurtigt. Er du derfor på jagt efter god kaffe, så er stedet værd at overveje, men trænger du til et sukkerchok og lidt til sidebenene, så skulle du måske hellere overveje, at kigge på kagerne i Lagkagehusets vindue lige ved siden af.

Studieordningen til revision?

Matias Lolk Andersen

Matematikstuderende er ikke vanvittigt engagerede i studenterpolitik – det er et faktum, der understøttes af vores stadigt ikkeeksisterende fagråd. Alligevel er det mit håb, at nærværende artikel kan rejse en række spørgsmål om matematikstudiets nuværende opbygning, som læserne af dette blad vil debattere aktivt med deres medstuderende/kolleger. Inden vi når så langt, skal vi dog lige spole et par år tilbage.

I 2009 blev der foretaget markante ændringer i studieordningen for bacheloruddannelsen i matematik. Hvor det med den foregående studieordning var en nødvendighed udelukkende at følge matematikkurser på første år, blev det pludselig muligt – og tilskyndet – blot at læse matematik på halv tid, og så kunne man sideløbende klare sit obligatoriske tilvalg. Rationalet var, at matematik er et fag med en meget stejl indlæringskurve på universitetet, når man som førsteårsstuderende blot har kendskab til (den noget naive) gymnasiematematik. Ved at trække første år ud ville de studerende få en lettere start på studiet, og i sidste ende ville de få mere ud af deres kurser. Denne vurdering deler jeg ubetinget.

Planen havde imidlertid en indbygget fejl, for det var ikke alle fag, man kunne supplere med på første år. Havde man lyster, der strakte sig længere end til fysik, datalogi, kemi og mat-øk (eller var man bare snotforvirret over tilvalg), så måtte man udskyde tilvalget til et senere tidspunkt og udelukkende følge matematikkurser i starten. Det var isoleret set ikke et problem, for sådan havde betingelserne jo hidtil været for alle. Problemet bestod i, at man pludseligt havde studerende fra første og andet år, der fulgte kurser sammen. Studerende med 75 ECTS-point og en netop afsluttet An2-eksamen på bagen skulle i blok 2 have SS sammen

Men hvor Bouton „kun“ fandt en løsning for *Nim*, udviklede Sprague og Grundy uafhængigt af hinanden en samlet teori først i 1930'erne, der viste, at alle upartiske spil kan gives en Nimværdi og derfor kan lægges sammen som ovenfor beskrevet.

Sprague/Grundy-teorien skabte grundlaget for kombinatorisk spilteori, som i dag spreder sig ud over andet og mere end upartiske spil, nemlig Partizanspillene. Partizanspil, som er en matematisk talefejl for partiske spil, er meget anderledes end upartiske spil, da der er træk, som kun den ene spiller kan foretage, f. eks. må kun hvid flytte de hvide tårne i *Skak*.

Det er additionsstrukturen, der gør teorien interessant og enkel; Additionen af to spil er — som forventet — at man kan trække i enten det ene spil eller i det andet, hvorefter turen overgives til modspilleren. F. eks. betragtes hver stak i *Nim* som selvstændige spil, som adderes.
To spil, G og H, har samme Nimværdi, hvis det for alle spil, X, gælder at $o(G+X) = o(H+X)$, hvor o er udfaldsfunktionen, der angiver om næste eller foregående spiller vinder.
Ækvivalensmængden over udfaldsfunktionen udgør en gruppe, der er isomorf med

$$\bigoplus_{\mathbb{N}} \mathbb{Z}_2$$

Hvor $\bigoplus$ her betegner den direkte sum, og ikke den specielle addition, $\oplus$.

Du har lige har lært at tage elementer på ækvivalensmængden, benytte gruppeisomorfien derpå (ved at tage binærværdien af staklængden), og så benytte den specielle addition, $\oplus$, der netop svarer til additionen af 2 elementer i gruppen, $\bigoplus_{\mathbb{N}} \mathbb{Z}_2$, hvorefter du benytter den inverse gruppeisomorfi til at finde elementet i ækvivalensmængden, kaldet kvotienten. Se f. eks. beregningen øverst

Findes der en vinderstrategi, hvis stakkene er af størrelse 3, 4 og 5 eller størrelse 2, 4 og 6?

Løsningen for alle positioner i *Nim*, som Charles L. Bouton fandt, er at tage hver staks størrelse, repræsentere dem på binær form og lægge dem sammen, hvor der ses bort fra menter (!), således en stak af størrelse 3 og 1 omformes til $11 \oplus 1 = 10$. Hvis resultatet er 0, har du en tabersituation.

Figur 2 Løsning af (2, 4, 6)

	0	1	0	2
	1	0	0	4
$\oplus$	1	1	0	6
=	0	0	0	0

Altså gælder det om at fjerne pinde, så spillet får værdien 0. Beviset er at indse, at fra 0 kun kan flyttes til en *ikke-0* position og omvendt.

Eksempel 3 Så er der en vinderstrategi for spillet 3, 4 og 5? Ja; Figur 1 viser at værdien er 2.
Der er dog problemer med spillet 2, 4 og 6. Figur 2 viser at værdien er 0, og derfor efterlader alle træk en vinderposition.
Prøv selv med 6, 5, 1.

Vindertrækket findes ved at oversætte stakstørrelserne til binærværdier, reducere den længste stak, således at binærværdien sikrer et lige antal 1'ere i hver cifferposition på tværs af stakkene — Ensbetydende med at *eksklusivt eller* giver 0. Hvis det ikke er muligt, så er du fortabt.

Nuvel, der er `10` slags mennesker: Dem, der forstår binært, og dem der ikke gør... Hvis du forstod vittigheden, altså at 2 på binærform skrives `10`, så kan du trygt spille om hvem, der skal vaske op efter festen næste gang — Husk dog at vælge opstilling efter, om du skal trække først eller sidst.

med de førsteårsstuderende, der lige havde afsluttet MatIntro – og bedre blev det næppe, når de i blok 3 skulle have Alg1 sammen. Med den stejle indlæringskurve fra før in mente, er dette indlysende et problem – enten får man ikke udfordret den ene halvdel tilstrækkeligt, eller også giver man ikke den anden en levende chance.

Problemerne med studieordningen er dog større end ECTS-kløften mellem de studerende på SS, Alg1 og Geom1, for ved halveringen af matematikpensum på første år blev det besluttet, at kurset MatM (Matematisk Metode) helt skulle udgå. Centralt i MatM-pensum var prædikatlogik, bevisteknik og formulering af beviser – man lærte så at sige reglerne til det spil, som moderne matematik er. Derudover havde kurset også til formål at introducere de studerende for en lang række grundlæggende definitioner og konstruktioner som fx ækvivalens- og ordningsrelationer. Men MatM havde hjemme i blok 2, hvor der nu kun var plads til ét kursus, og den plads tilhørte LinAlg.

I stedet for blot at flytte MatM til blok 3 blev det besluttet at oprette kurset An0, der skulle forberede de studerende bedre på An1 i blok 4. An0 er i sandhed også et ambitiøst kursus, der dels formaliserer, generaliserer og videreudvikler den matematik, de studerende kender fra gymnasiet og MatIntro, dels introducerer de studerende til nye problemstillinger som fx løsning af lineære differentialligningssystemer. Langt de fleste studerende finder det ganske svært. I An0 får man dog ikke den oplæring i matematikkens spilleregler, som man tidligere modtog i MatM. Resultatet er, at de studerende på første år skal spille med i et tiltagende svært spil, som de forventes selv at gætte reglerne til – min erfaring som An0-instruktor er, at de færreste er i stand til dette. Faktisk indeholder studieordningen en erkendelse af dette problem; i blok 1 på andet år forventes de studerende nemlig at følge kurset

Dis, der i vid udstrækning behandler det gamle MatM-pensum. Det er min oplevelse, at langt de fleste finder Dis-pensum højst relevant – endelig opnår de en mere grundlæggende forståelse for strukturen af de argumenter, de mødte i løbet af første år. Omvendt undrer de sig over, hvorfor de først forventes at tillægge sig denne forståelse på så sent et tidspunkt, idet den ville være svært gavnlig at besidde på kurser som An0 og An1.

Problemet er ikke blot teoretisk; som instruktor har jeg efterhånden vænnet mig til, at de studerende ikke ved, hvad kontraposition, modstrid eller ækvivalensrelation betyder. Og hvordan skulle de så nogensinde få den ide, at et bevis lettest føres indirekte? Det er således den helt grundlæggende intuition for bevisstrategier, som mange nu misser på første år af deres studie – og det er ikke noget, jeg personligt ville bytte væk for viden om differentialligningssystemer og vektorfelter.

Er det således blot mig, der er reaktionær, eller trænger studieordningen til en revision?

andet, og derfor beskrives vinderen af et spil, som Næste eller Foregående spiller. Det kaldes udfaldet.
En option er et delspil, der er muligt at komme til ved 1 træk.

0-spillet vindes af Foregående, da det jo var sidste træk, der resulterede heri. For de øvrige spil kan man ud fra optionerne, altså trækmulighedernes resultat, afgøre udfaldet; Hvis der blandt optionerne er en med udfaldet Foregående, så har spillet selv udfaldet Næste. Ellers har spillet udfaldet Foregående.

Ved at »rulle grafen op« afgøres vinderen uden der er foretaget et fysisk træk. Og man behøver ikke en modstander, bare en startposition.

Nim er et af de enkleste af disse: Det er et spil med flere stakke bestående et af forskelligt antal pinde. Traditionelt med 3 stakke med i alt 12 pinde. Du kender det måske fra filmen „Sidste år i Marienbad“ (Alain Resnais, 1961).
2 spillere skiftes til at trække. Et træk består i at fjerne et antal pinde, dog mindst 1, fra 1 stak. Den, der tager den sidste pind, vinder.

Figur 1 Løsning af (3, 4, 5)

	0	1	1	3
	1	0	0	4
$\oplus$	1	0	1	5
$=$	0	1	0	2

Eksempel 2 Betragt situationen med 1 stak af n pinde. Det er klart, at 1 spiller altid vinder ved at rydde bordet.

En mindre triviel situation er 2 stakke med hhv. 5 og 3 pinde: Du ser nok hurtigt, at det gælder om at trække først og gøre antallet af pinde i de 2 stakke ens, for herefter at „efterabe“ den andens træk. Samtidig er det klart, at hvis der er 2 stakke med samme antal, når du skal trække, så er du i problemer.

Knuseren...

Kombinatoriske spil er f. eks. *Kryds og Bolle*, *Lejligheder*, *Kalaha*, *Skak*, *Nim*, *Go* osv. Der er stor forskel på dem: I nogle er der løkker, dvs. man kan komme tilbage til en tidligere tilstand, i nogle er samme træk ikke tilgængelig for begge spillere, sædvanligvis er den ene spiller sort og den anden hvid, i nogle har hver spiller mere end 1 træk per tur, osv.

I den traditionelle, stramme definition af kombinatoriske spil er der kun 2 spillere, da resultatet ellers kan afhænge af sympatier spillerne imellem. De 2 spillere har i hver tur kun 1 træk til rådighed. Taberen er den, der først løber tør for træk. Den anden vinder.

Det kan lyde som en stor begrænsning, men der er stadig en meget stor mængde spil at arbejde på. Desuden kan man ofte benytte teknikker herfra til at analysere de øvrige kombinatoriske spil.

Det første spil, der blev løst ved kombinatorisk spilteori, var *Nim*, som er kendt i Europa allerede i starten af det 16. århundrede. Løsningen blev fundet i 1901, og da Piet Hein opdagede resultatet, ødelagde det spillet for ham.

Hvis et spil er endeligt og uden løkker, og man sørger for, at begge spillere har samme træk til rådighed, er det klart, at man kan tegne en orienteret graf over alle trækmulighederne med udgangspunkt i spillets start. Hver trækmulighed resulterer i et delspil, hvor man kan gentage proceduren, indtil der ikke er flere trækmuligheder, 0-spillet.

Definition 1 En spillers træk er en overgang fra et spil til et

$\sqrt{2}$ er irrational

Benjamin Randeris Johannesen

Alle kender mindst et bevis for at $\sqrt{2}$ er et irrationalt tal, men de fleste kender kun det ene ældgamle bevis, man typisk bliver præsenteret for. Et andet bevis, man måske har set, udnytter, at der for enhver rational rod $\frac{p}{q}$ (lad os sige, at p og q er indbyrdes primiske!) i et polynomium

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

med $a_n \neq 0$, $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ opfylder, at $p \mid a_0$ og $q \mid a_n$. Specielt har vi, at hvis f er et monisk polynomium (dvs. $a_n = 1$), så er $q = 1$. Herfra følger det, at $\sqrt{2} \notin \mathbb{Q}$, da $\sqrt{2}$ er en rod i $g(x) = x^2 - 2$, hvorfor $\sqrt{2}$ er et helt tal eller et irrationalt tal, men det er ikke et helt tal, for 2 er ikke et kvadrattal. (Her benytter vi naturligvis bl.a. aritmetikkens fundamentalsætning). Dette bevis lader sig naturligt generalisere:

Theorem 1 *Hvis $n \in \mathbb{N}$ ikke har formen $n = k^m$, $k, m \in \mathbb{N}$, da gælder, at $\sqrt[m]{n} \notin \mathbb{Q}$.*

Bevis. Hvis $p, q, n \in \mathbb{N}$ med p og q indbyrdes primiske og $(\frac{p}{q})^m = n$, så er $q = 1$ (overvej!). □

Vi runder af med et meget charmerende bevis for at $\sqrt{2}$ er irrational, et bevis der måske er både simplere og mere elegant end de fleste andre beviser for sætningen.

Theorem 2 $\sqrt{2} \notin \mathbb{Q}$.

Bevis. Antag for modstrid, at $\sqrt{2} \in \mathbb{Q}$. Der findes da $n \in \mathbb{N}$, således at $n\sqrt{2} \in \mathbb{N}$. Vi bruger velordningsprincippet og lader $n \in$

$\mathbb{N}$ betegne det mindste naturlige tal, som opfylder at $n\sqrt{2} \in \mathbb{N}$. Bemærk, at $n > n(\sqrt{2}-1) \in \mathbb{N}$, da $2 > \sqrt{2} > 1$. Iagttag endelig blot, at $n(\sqrt{2}-1)\sqrt{2} = 2n - n\sqrt{2} \in \mathbb{N}$, hvilket er en modstrid. □

Matematik, der afgør spil

– Sandsynlighedsregning vinder ofte. Kombinatorisk spilteori sejrer hver gang

Mads Thrane

Hvis du er træt af at tabe opvasketjansen i *Sten—Saks —Papir* eller *Terning*, så skal du følge med her:

Traditionelt set har matematisk spilteori drejet sig om sandsynlighedsregning. Grundlaget for den teori blev lagt allerede i det 17. århundrede af især matematikerne Jacob Bernoulli og Laplace, og er siden blevet hvermandseje. Visse spil kan dog stadig drille en matematiker. F. eks. det såkaldte »Monty Halls paradoks«:

Du er med i et spil, hvor du skal vælge mellem 3 døre: Bag den ene er en bil og bag de øvrige geder. Når du har truffet dit valg, åbner værten en/den af de 2 andre døre, som skjuler en ged, med spørgsmålet: VIL DU SKIFTE DØR?
Sandsynligheden for gevinst fordobles, hvis du gør.

De fleste spil indeholder et element af tilfældighed, men der findes en del spil, der ikke indeholder tilfældigheder med *Skak* som en af de vigtigste repræsentanter.

Nogle af disse spil indeholder i stedet begrænset information, som f. eks. *Sten—Saks —Papir*, hvor det ikke er terninger, men modstanderens valg, der afgør spillet. Et andet kendt eksempel er *Prisoner's Dilemma*, som er beskrevet i FAMØS i marts 1996 i artiklen „At stemme eller ikke at stemme II“ — der i øvrigt er en god artikel. Overvejelserne herom kaldes strategisk spilteori, men bliver ofte bare omtalt som spilteori.

Tilbage er den mængde spil, hvor man kan sikre en sejr hver gang; De rene kombinatoriske spil.

Afgørelsen og ny præmieopgave

– Er du en vinder?

Kristian Peter Poulsen, Jingyu She og Bo Malling Christensen

Sidste bloks præmieopgave

Sidste bloks opgave gik ud på at bestemme halvdelen af gennemsnittet af de indkomne bud; hvor de tilladte bud skulle ligge i intervallet $(0, 100)$. Det ville være løgn at sige, at der blev gættet på alt mellem himmel og jord, men gættene spændte alligevel fra $0,0123456789$ til $99,9$. Gennemsnittet af samtlige bud blev $27,5107$ (afrundet), så resultatet blev $13,7553$ (afrundet).

Den, der kom tættest på det rigtige bud var Katrine Lykke Jensen, som derfor er vinder af konkurrencen. Tillykke med det, Katrine. Du vil modtage en flaske vin og et påskeæg som præmie!

Den nye præmieopgave

Udregn tværsummen af tværsummen af tværsummen af 5926^{5926}.

I denne sammenhæng er **tværsummen** defineret som summen af alle cifrene i et tal. Fx er tværsummen af 179 lig med $1+7+9 = 17$.

Vinderen af ovenstående tværsumskonkurrence vil modtage et **super-summerkit** (!) med alt hvad en lystig matematiker kunne begære i de varme sommermåneder (bl.a. badevinger og engangsgrill)!

Dollarauktion

– Hvordan man tjener 99 cent

Sune K. Jakobsen

En dollarauktion er et simpelt, men farligt spil: En auktionarius sælger en 1-dollarseddel til den højestbydende, men med en lille ekstra regel: Både den person, der byder højest, og den person, der byder næsthøjest, skal betale deres bud til auktionarius, selvom det kun er den højestbydende, der får 1-dollarsedlen. Alle bud skal være multipla af en cent. Hvad ville du gøre, hvis du sad til sådan en auktion?

Lad os se, hvad der sker, hvis man spiller dette spil med en stor gruppe personer. Det koster kun en cent at give det første bud, og der er mulighed for at tjene en dollar, så der vil formentlig være en, der byder en cent. Men to cent for en dollar er jo også en god handel, så der vil nok også være en, der byder det. Sådan kan man fortsætte i et stykke tid. Lad os sige, at Alice har budt 49 cent og Bob har budt 50 cent. Nu ville Alice tabe de 49 hvis spillet stoppede her, men hun har chancen for at vinde $100-51 = 49$ cent ved at byde 51 cent, så selvfølgelig gør hun det. Allerede her vil auktionarius komme til at vinde på at sælge sin dollar, og Alice og Bob vil altså tilsammen sætte penge til, medmindre andre deltagere er dumme nok til at give et bud. Men det fortsætter med samme tankegang som før. Hvis de når op på, at Bob har budt 98 cent, og Alice har budt 99 cent, så vil Bob tænke: *Hvis jeg stopper her, mister jeg* 98 *cent, men hvis jeg fortsætter, vil jeg komme til at betale* 100 *cent for en dollar, så det går lige op.* Derfor byder han 100 cent. Nu står Alice til at miste 99 cent, men hvis hun byder 101 cent for de 100 cent, så kan hun måske nøjes med at miste 1 cent. Det bliver skruen uden ende: Begge personer byder højere og højere i håbet om, at den anden stopper galskaben, men begge personer kommer til at sætte penge til. Der

er set eksempler på at folk på denne måde har budt 2000 $ for 20 $! [1]

Så hvad skal man gøre, hvis nogen forsøger at sælge en dollar på denne måde? En strategi ville være at lade være med at byde, men det er så kedeligt! Man kunne prøve at forklare folk problemet, derefter byde en cent og håbe på, at alle andre er kloge nok til at holde sig væk. Men hvorfor skulle de det? *Du* ved jo også, at det ender galt, så hvis de byder to cent, vil du nok bare stoppe! Man kunne i stedet vælge at lægge ud med at byde 99 cent. Så vil ingen andre kunne tjene på at overbyde dig. Der er dog to problemer med denne strategi: For det første vil du i bedste fald kun tjene en cent, og for det andet: Hvis der er en anden deltager, der hader dig, kan han få dig til at tabe 99 cent ved at byde 1 dollar. Det vil være gratis for ham, medmindre du begynder at byde over.

En sjovere strategi ville være, at du først *lover*, at du ikke vil lade andre få dollaren for mindre end $1,02$ dollar, og derefter byder du en cent. Hvis andre tror på dit løfte, vil det helt sikkert ikke kunne betale sig for dem at byde mere. Men hvorfor skulle de tro på dig? Hvis Alice nu byder 99 cent, vil det være bedst for dig at bryde dit løfte og lade være med at overbyde. Der er ikke nogen, der taber på, at du bryder dit løfte, så ingen vil blive sur på dig, og netop derfor vil du ikke have nogen grund til at holde dit løfte.

En bedre strategi vil derfor være at give Alice dette løfte: "Hvis en anden deltager får dollarsedlen for mindre end $1,02$ dollar, så skylder jeg dig 10 dollars".[1] Herefter byder du så en cent. Hvis Bob

[1]Dette er idéen i det løfte man skal give, men man bør tilføje to forbehold: Hvis man giver penge til andre som en konsekvens af aftaler lavet under auktionen, så vil man også give de 10 dollars til Alice, og Alice må ikke betale penge tilbage til dig. Det vil blive for omfattende at forklare hvorfor disse to forbehold er nødvendige, så det overlades som en sjov opgave til læseren!

kodebrydende frihedskæmpere først oprejsning mange år senere. Mange af de lokale, der boede tæt på Bletchley Park, havde endda bemærket det besynderlige i, at den slags unge, våbenføre mænd ikke var ved fronten.

Turing fortsatte sit arbejde inden for forskellige felter, men kunne ikke længere sikkerhedsgodkendes til officielle formål, da han var homoseksuel, hvilket i efterkrigstidens bornerte Storbritannien var yderst mistænkeligt i regeringens øjne. I 1952 blev han arresteret for at have et homoseksuelt forhold. Som straf blev han idømt et års østrogenbehandlinger. Disse gjorde ham både overvægtig og impotent. I 1954 spiste han af et cyanidforgiftet æble, hvilket blev hans endeligt. Hans mor mente, at det var et uheld efter et amatøragtigt kemiforsøg, der havde efterladt rester af cyanid på hans fingre. Retsmedicineren, der undersøgte ham, konkluderede, at det var selvmord.

Litteratur

[1] Andrew Hodges. *Alan Turing: the Enigma*

[2] Richard Owen. *Why the Allies Won*

[3] Andrew Williams. *Slaget om Atlanten*

[4] Simon Singh. *Kodebogen*

[5] Famøs, *10. årgang, nr. 4, maj 1997, side 9 sætningen: Ultra*

positioner. Dette nye gennembrud medførte, at de allierede igen kunne føre deres konvojer uden om de tyske u-både. Igen mente den tyske flåde, at forklaringen på de allieredes kendskab til tyske planer måtte stamme fra spionage og ikke fra udkodning af tyskernes egen kommunikation.

Indflydelsen på krigen

Hvis vi vender tilbage til vores udgangspunkt, nemlig diskussionen mellem kemikeren, fysikeren og matematikeren, så kan man med rette spørge sig selv, hvilken effekt de allieredes (amerikanere kom hen mod slutningen af krigen også ind over kryptoanalysen af tysk kommunikation) evne til at læse Værnemagtens kommunikation havde på udfaldet af krigen. Den slags kontrafaktiske overvejelser er selvfølgelig ligeså spændende, som de er spekulative. Det er blevet hævdet, at de allieredes overlegenhed på dette felt forkortede den europæiske krig med to år, da man simpelthen kunne opbygge kapacitet til invasionen af Frankrig hurtigere, når man til dels kunne føre sine konvojer uden om de glubske, tyske u-både. Det siger sig selv, at to år i bedste fald er et godt gæt og i værste fald bare et tal, men i diskussionen på Caféen, skal læseren selvfølgelig føle sig velkommen til at bruge tallet og citere FAMØS som en pålidelig kilde. Derudover skal det også med rette nævnes at selvom Rejewski, Turing og deres kolleger ydede en heroisk og imponerede indsats, ville det ikke være gået uden hjælp fra tyskerne. Gang på gang brød de med alle kryptografiens helligste principper i en blind tiltro til Enigmasystemet. Efter krigen var hele Ultraprogrammet stadig mørklagt fra den britiske regerings side og offentligheden blev først oplyst om det i 70'erne. Briterne ønskede naturligvis ikke at afsløre at de kunne læse med i det meste, herunder naboernes interne post. Derfor fik disse

overbyder dig (lad os sige han byder 99 cent), vil det nu være i din egen interesse at byde over igen. Ellers skulle du jo betale 10 dollars til Alice. Bob (og alle andre) ved derfor, at det ville være dumt at overbyde dig, og vil derfor (i teorien!) lade dig tjene de 99 cent!

Strategien er altså at love nogle penge væk under visse betingelser. Umiddelbart skulle man tro, at man kom til at stå dårligere ved at gøre dette, fordi man dermed mindsker sine muligheder. Men i spil med modstridende interesser kan det netop være en fordel at begrænse sine muligheder.[2] Hvis du spiller "Chicken" (et spil, hvor to biler kører frontalt mod hinanden, og den person, der først afviger, taber), er du næsten sikker på at vinde, hvis du inden spillet ødelægger styringen på din egen bil. Modstanderen ved, at du ikke kan afvige, og han vil derfor blive nødt til selv at afvige. Dog skal du huske at fortælle din modstander, at du har begrænsede muligheder, ellers kan det gå meget galt![3]

Litteratur

[1] Muringhan, J. Keith. "A Very Extreme Case of the Dollar Auction." *Journal of Management Education* 26, 56-69. 2002

[2] T. C. Schelling, *The strategy of conflict*, Harvard University Press, 1980.

[3] S. Kubrick, *Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb* [film], Columbia Pictures, 1964.

[4] S. Pinker, *How the mind works*, Norton, 1997.

[2] Dette er beskrevet af Nobelpris-vinderen Thomas Schelling i [2]. Se også [4, s. 408-413] for flere eksempler.

Lagrange og primtal

– Sjov med endelige grupper

Martin Patrick Speirs

I disse uger oplever mange spirende matematik-unger deres første møde med en af algebraens herligste objekter: grupper! Udover at være en fornøjelse i sig selv, så har gruppeteori et væld af anvendelser inden for en række matematiske discipliner, såvel som i naturvidenskaberne – især i fysik og kemi. Særlig smuk og dyb er konstruktionen af såkaldte symmetrigrupper som f.eks. kan hjælpe med forståelsen af både geometriske objekter og polynomier (Se artikel om Galoisteori).

I denne lille note vil jeg gengive et sjovt bevis for at der er uendeligt mange primtal. Hovedredskabet er *Lagranges sætning*! Hvis G er en (endelig) gruppe og H er en undergruppe i G, så siger Lagrange (og han har skam ret!) at ordenen af H er divisor i ordenen af G. Én måde at se dette på er ved at betragte en meget fin ækvivalensrelation på G, nemlig,

$$a \sim b \iff ab^{-1} \in H$$

(prøv at vise at det *er* en ækvivalensrelation).[3] Det vigtige ved denne ækvivalensrelation er at den giver anledning til en klassedeling af G. I dette tilfælde kan man vise (Gør det! Det er ikke svært) at hver ækvivalensklasse har samme orden som H. Altså består G af en samling ækvivalensklasser, som alle har samme orden som H. Jamen så går ordenen af H jo op i ordenen af G.

Et specialtilfælde af Lagranges sætning opstår når man har et element $g \in G$. Så frembringer g en undergruppe, kaldet $\langle g \rangle$, som altså har en orden som er en divisor i $|G|$.

[3]Der er *ikke* noget underligt ved denne relation. Den minder meget om kongruens på hele tal, altså: $a \equiv b \pmod{m} \iff a - b \in m\mathbb{Z}$

fastlægge ledningsføringen inden i denne nye scrambler. Igen var det tyske fodfejl, der gjorde det muligt. Siden 1941 havde denne fjerde scrambler nemlig siddet i en neutral position, altså uden at ændre krypteringsprocessen, i Enigmamaskinerne. I december 1941 havde en operatør ved en fejl indkodet en meddelelse med tre normale scramblere og denne fjerde scrambler, som af den ene eller anden årsag ikke havde siddet i en neutral position. Det blev opsnappet af Ultra, som jo ikke kendte til den fjerde scrambler og derfor ikke vidste, hvorfor de ikke kunne dechiffrere meddelelsen. Imidlertid indså operatøren fejlen og udsendte den præcis samme meddelelse, men nu korrekt krypteret altså uden brug af den fjerde scrambler. Denne meddelelse kunne Ultra godt dechifrere og ved at sammenligne de to meddelelser kunne Turing og hans kolleger nu fastlægge ledningsføringen i den fjerde scramber, så da den blev taget i brug, var de et skridt foran. Imidlertid gav den nye scrambler stadig 26 gange flere mulige indstillinger, som bomberne skulle kontrollere, når der var blevet gættet en crib. Det gav store problemer, da man simpelthen manglede kapacitet. Derfor blev 1942 et år med mange allierede tab i Atlanterhavet, da man ikke længere havde adgang til u-bådenes kommunikation, hvorfor man ikke kunne føre konvojerne uden om de jagende u-både. Hen mod slutningen fik den britiske kryptoanalyse dog igen vind i sejlene. Man kaprede nemlig en tysk u-båd, hvorved man fik adgang til de nye procedurer. Derudover begik tyskerne endnu en gang en fodfejl. De krypterede nemlig vejrmeldingerne med samme indstillinger som alle andre meddelelser, men med den fjerde scrambler i neutral position. Derved kunne Ultra igen finde cribs og bruge bomberne til at afprøve indstillingerne. Derefter manglede man kun at finde ud af hvordan det fjerde skulle indstilles, før man var klar til at udkode de tyske meddelelser. Dette var overkommeligt, da den fjerde scrambler kun kunne stilles i 26 forskellige

Britiske efterretninger og tyske fodfejl

I 1941 havde Turing og hans kolleger udviklet de metoder, som sammen med det opsnappede kodemateriale i perioder muliggjorde dekryptering af store dele af den tyske flådes kommunikation. I starten blev den information anvendt forholdsvis naivt. Det udmøntede sig bl.a. i sænkningen af det tyske slagskib Bismarck, som sammen med en række andre vellykkede britiske flådeoperationer fik den tyske fjende til at overveje muligheden for at Storbritannien havde adgang til hemmelige oplysninger. Heldigvis for briterne var de tyske efterretningstjenester dog lige så naive, da de fuldstændig udelukkede muligheden for, at Enigma var blevet brudt. I stedet konkluderede de, at de britiske efterretningstjenester havde infilteret centrale dele af det tyske krigsapparat, og oplysningerne altså stammede derfra. Hvis tyskerne ikke havde haft denne naive tiltro til Enigmas fortræffeligheder, ville de fx have kunnet indføre dobbeltindkodning af alle meddelser, hvilket ville havde gjort Ultras (britternes kryptoanalystiske enhed) cribstrategi ubrugelig. Hvor den britiske side straks herefter indså, at oplysninger der stammede fra dekryptering af tyskerne kommunikation skulle anvendes med meget stor varsomhed, vedblev den tyske modpart med at forholde sig naivt til Enigma og dens formåen. I løbet af krigen steg Ultras kapacitet løbende og med tiden blev puljen af kryptoanalytikere fordelt mellem forskellige tyske kodesystemer. Turing blev sat til at arbejde med kryptoanalyse af den tyske flådes kommunikation, hvilket også var en af de stærkeste. Der var imidlertid også grene af den tyske værnemagt, hvis kommunikation aldrig blev mulig at læse for Ultra. I februar 1942 forbedrede den tyske flåde Enigmasystemet ved at indføre en fjerde scrambler i maskinen. Denne scrambler var ikke udskiftelig. Det første problem for Turing og hans kolleger var at

Her er to gode eksempler på endelige grupper: $\mathbb{Z}_q$ og $\mathbb{Z}_q^*$ hvor q er et primtal. Gruppen $\mathbb{Z}_q$ er som bekendt den cykliske gruppe af orden q. Gruppen $\mathbb{Z}_q^*$ består af de elementer i $\mathbb{Z}_q$ som har en *multiplikativ* invers. Da q er et primtal er der netop $q-1$ sådanne elementer. Hvis f.eks. $q=5$ så er $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ og $\overline{2}\cdot\overline{3} = \overline{6} = \overline{1}$.

Theorem 1 *Der er uendeligt mange primtal.*

Bevis. Antag for modstrid at der er *endeligt* mange primtal og lad p være det største. Vi ser nu på tallet $2^p - 1$ (et *Mersenne* tal) og finder et primtal som er større end p. Lad q være et primtal som går op i $2^p - 1$ (husk at ethvert tal altid har primdivisorer). Vi har altså at

$$2^p - 1 \equiv 0 \pmod{q} \qquad \text{dvs.} \qquad 2^p \equiv 1 \pmod{q}$$

Vi ser nu på den multiplikative gruppe $\mathbb{Z}_q^*$. Ovenstående kongruens viser at elementet $\overline{2}$ har orden p i $\mathbb{Z}_q^*$ (her er det vigtigt at p er et primtal). Vi har nu fra Lagranges sætning at ordenen af undergruppen $\langle\overline{2}\rangle$ går op i ordenen af $\mathbb{Z}_q^*$. Dvs. $p \mid q-1$. Men så er $p < q$ og vi har altså fundet et større primtal i modstrid med antagelsen om at p var størst! □

Overstående bevis kommer fra [1] som er en herlig bog at læse i. Bogen findes både på IMF og NAT SUND bibliotekerne og sågar på nettet igennem rex.kb.dk.

God fornøjelse med grupperne!

Litteratur

[1] M. Aigner and G. Ziegler, *Proofs from the Book*, 4th ed. Springer

Blokkens blokke

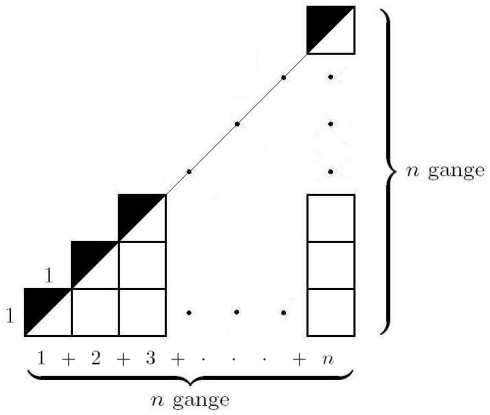
– En formel, vi alle kender

Kristian Peter Poulsen

Vi kender alle formlen, der siger, at summen af de n første tal kan skrives som $\frac{n(n+1)}{2}$. Det har jeg fundet et bevis for, som jeg ikke har set andre steder, men som sikkert er blevet lavet før.

Sætning 1

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}, \qquad n \in \mathbb{N}$$



Bevis

$$\begin{aligned}\sum_{i=1}^{n} i &= \textit{Areal}(\text{den hvide trekant}) + \textit{Areal}(\text{de } n \text{ sorte trekanter}) \\ &= \frac{1}{2}nn + n\frac{1}{2} = \frac{n(n+1)}{2}\end{aligned}$$

LR.

fremgangsmåder. En af disse fremgangsmåder var at gætte et ord i klarteksten samt dets præcise placering. På den måde kunne man afprøve hvilke indstillinger, der ville give anledning til en given indkodning af et gættet ord. Dette kunne endda afprøves mekanisk med dertil indrettede maskiner. Igen var svaret på den tyske mekanisering af kryptering en mekanisering af kodebrydningen. Den kritiske læser vil nok studse over, hvorvidt det at gætte et ord samt dets placering i klarteksten (en såkaldt crib) er en overkommelig opgave. Imidlertid var kommunikationen i de tyske væbnede styrker naturligvis underlagt visse restriktive normer, hvilket gjorde denne kommunikation meget rutinepræget. Gentagelse er kryptoanalytikerens bedste ven, og netop denne tankeløse anvendelse af Enigma muliggjorde denne fremgangsmåde. Kommunikationen, der blev opsnappet, blev udsendt over radio, hvorfor den var let for de britiske lyttestationer at få fingre i. På den måde kunne briterne fx hver morgen opsnappe vejrmeldinger fra tyskerne. Igen vil den kritiske læser nok fare op af stolen og hævde, at briterne ville kunne kigge ud af vinduet, hvis de var interesseret i vejret. Imidlertid viste det sig at fx vejrmeldingerne var meget rutineprægede og ord som Wetter (tysk: vejr) indgik som oftest. Dermed kunne briterne bruge denne viden til at finde frem til dagskoden som senere kunne anvendes til at dekryptere mere interessant information. Turing og hans kolleger videreudviklede bomberne, så man mekanisk kunne finde frem til hvilke indstillinger meddelsen var indkodet med givet en crib. Hele fremgangsmåden var dybt afhængig af operativ efterretningsindhentning. Man havde simpelthen brug for at kende tyskernes procedurer så præcist som muligt. Man havde heldigvis succes med dristige operationer, hvor britiske flådefartøjer kaprede tyske skibe og u-både og fik fat i kodemateriale, inden skibene blev sænket.

Biuro Szyfróws arbejde senere lagde grund for de britiske kryptoanalytikeres forsøg på at bryde Enigmakoden. Rejewskis anstrengelser betød desværre ikke meget for det praktiske forløb af Hitlers invasion af Polen. I 1938 fik alle Enigmaoperatører nemlig to nye scramblere. Nu skulle der pludselig bruges 60 bomber til at tjekke indstillingerne (nemlig (5*4*3)). Man indførte også fire ledninger mere i plugboardet så antallet af ombyttede bogstaver nu steg til hele 20. Den elegante polske fremgangsmåde var fuldstændig afhængig af den faktiske ledningsføring i Enigmamaskinerne, hvorfor selv små ændringer i anvendelsen eller opbygning af det tyske kodesystem betød, at de polske kryptoanalytikere var tilbage på bar bund. Desværre modtog Biuro Szyfrów nu heller ikke længere dagskoderne fra den fransk spion. Hele den tyske Blitzkrieg var ellers dybt afhængig af kommunikation for at koordinere de store og voldsomme angreb, men nu kunne polakkerne ikke længere følge med i denne kommunikation. Major Langer ville ikke lade sine folks arbejde gå til spilde, hvorfor han i 1939 inviterede franske og britiske kolleger til Polen, hvor han overdrog arbejdstegningerne til bomberne samt to Enigmamaskiner til dem. Kort efter blev Polen invaderet.

Kampen flyttes til de britiske øer

I Storbritannien var det Government Code and Cypher School i Bletchley Park, der havde forsøgt at dekryptere tyskernes kommunikation. Inden kontakten med de polske kolleger uden stor succes. Briterne byggede dog videre på de polske fremskridt, men med den indsigt, at kodebrydningen ideelt set ikke skulle afhænge af lavpraktiske omstændigheder som tyskernes indkodningsprocedurer samt ændringer i ledningsføring og lignende. Kodebrydningen skulle derimod afhænge af mere generelt anvendelige

Polynomier med sælsomme egenskaber modulo p

Bo Vagner Hansen

Reduceres koefficienterne i et normeret heltalspolynomium modulo et primtal, opstår et nyt polynomium over restklasseringen. Både ringen af polynomier med heltalskoefficienter og ringen af polynomier med koefficienter i $\mathbb{Z}/p$ har, ligesom de hele tal, entydig primfaktorisering, og primelementerne er netop de irreducible polynomier. Det er ofte nyttigt at kunne bestemme sådanne primfaktoriseringer, eller i første omgang blot afgøre, om polynomiet er irreducibelt, eller tillader yderligere faktorisering, samt hvilke typer af faktoriseringer der i givet fald kan forekomme. Artiklen undersøger hvad vi kan sige om faktoriseringen af det reducerede polynomium ud fra egenskaber ved det oprindelige polynomium. Specifikt skal vi se, at Galoisgruppen for polynomiet kan fortælle os en del om, hvorledes det reducerede polynomium faktoriserer, og vi giver derfor en ikke-alt-for-teknisk introduktion til Galoisgrupper. Undervejs støder vi på flere spøjse og overraskende resultater, og vi bliver blandt andet i stand til at karakterisere primtallene ud fra eksistensen af polynomier med særlige egenskaber.

Reduktion modulo p

Vi betragter gennemgående i artiklen et normeret polynomium $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ med koefficienter i ringen $\mathbb{Z}$ og grad $n \geq 1$. For et primtal p haves en kanonisk homomorfi $\varphi\colon \mathbb{Z} \to \mathbb{F}_p$, der afbilder et helt tal i den tilsvarende restklasse modulo p (her og nedenfor betegner $\mathbb{F}_p$ restklasseringen $\mathbb{Z}/p$, der som bekendt udgør et legeme). Billedet af $b \in \mathbb{Z}$ under φ betegnes $\overline{b}$. Denne afbildning inducerer en homomorfi $\Phi\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ mellem

polynomiumsringene ved at erstatte koefficienterne til $f \in \mathbb{Z}[x]$ med deres restklasser modulo p. Lad os betegne billedet af f under Φ med $\overline{f}$. Vi skal i det efterfølgende interessere os for, hvorledes polynomiet $\overline{f}$ faktoriserer i $\mathbb{F}_p[x]$.

Et normeret polynomium kaldes som bekendt irreducibelt, hvis det ikke kan skrives som et produkt af to polynomier med positiv grad. Hvis der for et polynomium f gælder, at $\overline{f}$ er irreducibelt i $\mathbb{F}_p[x]$, så følger det automatisk, at f er irreducibelt i $\mathbb{Z}[x]$. Alternativt ville vi nemlig have en ikke-triviel faktorisering $f(x) = f_1(x)f_2(x)$, hvilket under homomorfien Φ ville give en faktorisering $\Phi(f_1)\Phi(f_2)$ af $\overline{f} = \Phi(f)$, i modstrid med, at $\overline{f}$ er irreducibelt. Det er altså tilstrækkeligt at finde et primtal p, for hvilket $\overline{f}$ er irreducibelt i $\mathbb{F}_p[x]$, for at vise, at f er irreducibelt.

I almindelighed gælder ikke, at $\overline{f}$ også vil være irreducibelt, hvis blot f er det. Vi kan nemlig finde et primtal p og en rod $\overline{b} \in \mathbb{F}_p$ for $\overline{f}$ som følger: Da f er et polynomium, kan f kun antage værdierne ± 1 endeligt mange gange. Der findes altså $b \in \mathbb{Z}$, så $f(b)$ har en primdivisor p, og dermed er $f(b) \equiv 0 \pmod{p}$, eller med andre ord, $\overline{b}$ er rod i $\overline{f} \in \mathbb{F}_p[x]$. Faktisk kan vi altid finde uendeligt mange primtal p, så $\overline{f}$ har en rod i $\mathbb{F}_p$. Antag nemlig induktivt, at $\overline{f}$ har en rod modulo $p_1, \ldots, p_k$. Sæt $d = p_1 \cdots p_k$ og betragt

$$f(da_n x) = a_n(a_n^{n-1}d^n x^n + a_1 a_n^{n-2} d^{n-1} x^{n-1} + \cdots + a_{n-1}dx + 1)$$

Betegn med udtrykket i parentesen med $\hat{f}(x)$. Som før indses, at der findes $c \in \mathbb{Z}$, så $\hat{f}(c)$ har en primdivisor p. Dermed gælder

$$f(da_n c) \equiv \hat{f}(c) \equiv 0 \pmod{p} \quad \text{og} \quad \hat{f}(c) \equiv 1 \pmod{d}\ .$$

Specielt er p ikke divisor i d, så vi har fundet et primtal, som ikke allerede var på vores liste, og hvor $\overline{f}$ har en rod.

slå op i kataloget, hvilke indstillinger, der giver netop sådan en cykeltype. Dette blev gjort for både 1. og 4., 2. og 5. samt 3. og 6. bogstav. Hermed var arbejdet ikke færdigt. Scramblerindstillinger kunne findes på denne måde, men man havde jo stadig set bort fra plugboardet, der jo byttede parvist om på et antal bogstaver. Inden krigen var dette antal 12, altså seks par. Biuro Szyfrów havde imidlertid også et svar på dette. De indstillede simpelthen en kopi af en Enigmamaskine med de fundne indstillinger. Derefter begyndte de at udkode teksten. Det blev for det meste noget volapyk, men indimellem kunne man genkende brudstykker af forståelig tekst. Disse brudstykker gav et fingerpeg om, hvilke bogstaver der var byttet om, og hvilke der ikke var. Ved på denne måde prøve sig lidt frem kunne polakker nå helt i mål, og de blev altså de første, der brød Enigma. Senere lavede Rejewski en mekanisering af processen med at finde scramblerindstillinger. Der var seks forskellige scramblerrækkefølger (3!), hvorfor seks maskiner blev opstillet til mekanisk at afprøve de 17.576 (26^3) forskellige scramblerindstillinger givet en rækkefølge af scramblerne. Disse maskiner blev kaldt bomber.

Invasionen af Polen

Polakkerne lagde en stor mængde arbejde for dagen af nødvendighed, kan man hævde. Krigstruslen var da også til at tage og føle på for polakkerne, men faktisk havde chefen for Biuro Szyfrów hele tiden haft de tyske dagskoder liggende på sit kontor, da en fransk spion havde været i stand til løbende at få fat på dem. Chefen for Biuro Szyfrów, major Langer, havde dog ment, at hans folk skulle trænes til den dag, hvor krigen brød ud, og det ikke længere ville være muligt at få fat i koderne. Set i det helt store historiske perspektiv må man sige, at det nok har været en god disposition, da

Denne startindstilling foreskrev altså, hvordan scramblerne skulle indstilles, scramblernes rækkefølge og hvilke bogstaver, der parvist skulle ombyttes. Tyskerne ønskede dog ikke at give deres fjender for mange beskeder, der var krypteret med samme nøgle, hvorfor de tyske operatører kun brugte dagsnøglen til at kryptere seks bogstaver i starten af hver besked. Disse seks bogstaver var faktisk de nye scramblerindstillinger, som resten af beskeden var indkodet med. Scramblerindstillinger udgjorde kun tre bogstaver, men for at sikre sig mod slåfejl valgte tyskerne at lade deres operatører gentage de tre bogstaver. Det var en fejl. Det var netop denne form for systematik og gentagelse, som Marian Rejewski og hans kolleger havde brug for. Når tyskerne fx startede en besked med PKHJOK vidste de polske kodebrydere, at 1. og 4., 2. og 5. samt 3. og 6 parvist var indkodninger af samme bogstav. Det er umiddelbart ikke meget at arbejde med, men polakkerne var ikke færdige med at få gode idéer. Nu begyndte et møjsommeligt arbejde. Hvis nemlig polakkerne havde nok beskeder fra samme dag (altså hvor de første seks bogstaver var indkodet med samme dagskode) kunne de betragte 1. og 4. bogstav i beskederne, hvor bogstaverne i 4. position var en permutation af bogstaverne i 1. position. Polakkerne brugte nu et år på at kortlægge, hvilke initialindstillinger af scramblerne (rækkefølge og orientering), der gav hvilke cykeltyper i disse permutationer. Der var 105.456 indstillinger, der skulle tjekkes. Til hvilken nytte, kunne man spørge. Hvordan skulle dette give dagskoden? Polakkerne lader til fuldstændig at have glemt, at der også er et plugboard, som bytter om på bogstaverne. Imidlertid ændrer disse ombytninger ikke cykeltypen af en given permutation. Denne erkendelse var et gennembrud. Nu kunne polakkerne med deres dugfriske katalog over hvilke scramblerindstillinger, der giver hvilke cykeltyper simpelthen analysere en given dagskode, finde dens cykeltype og derefter

Det følger af Frobenius' Densitetssætning nedenfor, at der sågar findes uendeligt mange primtal p, så $\overline{f}$ har alle sine n rødder i $\mathbb{F}_p$.

Vi har altså set, at selvom f er irreducibelt, findes uendeligt mange primtal p, så $\overline{f}$ har en rod i $\mathbb{F}_p$, og specielt kan $\overline{f}$ ikke være irreducibelt, medmindre f er et førstegradspolynomium. Man kunne så forvente, at $\overline{f}$ i det mindste vil være irreducibelt for en delmængde af primtallene, men selv dette viser sig ikke at holde stik. Vi skal således i det følgende bl.a. vise, at polynomiet $g(x) = x^4 + 1$ er irreducibelt i $\mathbb{Z}[x]$, men reducibelt modulo ethvert primtal. Første del kan vi indse allerede nu, f.eks. ved at bruge Eisensteins kriterium på $g(x+1)$, eller ved direkte at verificere, at ingen ikke-trivielle faktoriseringer er mulige. Beviset for anden del beror på en sætning af Dedekind, samt kendskab til Galoisgruppen for polynomiet g. Herfor en kort introduktion til begrebet Galoisgrupper.

Galoisgrupper

Vi betragter fortsat et polynomium f af grad n. Som følge af Algebraens Fundamentalsætning har f nøjagtig n rødder $u_1, \ldots, u_n$ indenfor de komplekse tal, talt med multiplicitet. Vi skal i det følgende antage, at alle rødderne er simple (dvs. de er alle forskellige). Vi associerer en gruppe G til polynomiet f, bestående af de permutationer af rødderne u_i, der bevarer de indbyrdes rationale relationer mellem rødderne: Hvis rødderne opfylder en relation $\psi(u_1, \ldots, u_n) = 0$ for et polynomium $\psi \in \mathbb{Q}[x_1, \ldots, x_n]$ i n variable, da skal de permuterede rødder også opfylde relationen. For $\sigma \in G$ skal der altså gælde

$$\psi(\sigma(u_1), \ldots, \sigma(u_n)) = 0 \ .$$

Ved at identificere en rod u_i med dens indeks i, kan vi opfatte G som en undergruppe i den symmetriske gruppe S_n. Permutationen der ombytter rødderne u_1 og u_2 og fikserer de øvrige, bliver således repræsenteret ved transpositionen (12), osv.. Det ses straks, at identitetsafbildningen er i G, at kompositionen af to elementer fra G igen er i G, og hvis $\sigma \in G$ er σ^{-1} en potens af σ, eftersom S_n er en endelig gruppe, og dermed er $\sigma^{-1} \in G$. Altså er G vitterligt en gruppe. Gruppen G kaldes Galoisgruppen for polynomiet f.

Lad os bestemme Galoisgruppen for $g(x) = x^4+1$. Rødderne i g er de primitive 8. enhedsrødder: $v_1 = e^{\pi i/4}, v_2 = e^{3\pi i/4}, v_3 = e^{5\pi i/4}$ og $v_4 = e^{7\pi i/4}$. Bemærk, at der er oplagte rationale relationer mellem rødderne. Det er således muligt at udtrykke samtlige rødder ved hjælp af blot den ene. F.eks. har vi $v_2 = v_1^3$, $v_3 = v_1^5$ og $v_4 = v_1^7$. Dette sætter begrænsninger på de mulige permutationer i G. Betragter vi f.eks. en permutation σ, der sender v_1 til v_2, følger det, da σ skal bevare relationerne mellem rødderne, at $\sigma(v_2) = \sigma(v_1)^3$ og heraf $\sigma(v_2) = v_1^9 = v_1$. Tilsvarende finder vi $\sigma(v_3) = v_1^{15} = v_4$ og $\sigma(v_4) = v_1^{21} = v_3$. Læseren kan videre overbevise sig om, at hvis vi betragter permutationer τ og μ, der sender v_1 til v_3 resp. v_4, følger det, at $\tau(v_2) = v_4, \tau(v_3) = v_1, \tau(v_4) = v_2$ og $\mu(v_2) = v_3, \mu(v_3) = v_2, \mu(v_4) = v_1$. I alle tilfælde er permutationen altså fuldstændig fastlagt ved værdien i v_1. Der er således kun 3 mulige permutationer af rødderne i dette tilfælde, udover den trivielle permutation (identiteten). Samtidig er det klart, at disse permutationer bevarer enhver relation mellem rødderne: Hvis vi har en relation

$$\psi(v_1, v_2, v_3, v_4) = \psi(v_1, v_1^3, v_1^5, v_1^7) = 0 \ , \qquad (*)$$

betyder det nemlig, at v_1 er rod i et polynomium $\theta \in \mathbb{Q}[x]$. Da g er irreducibelt, er $x^4 + 1$ det normerede polynomium i $\mathbb{Q}[x]$ af

der er blev indkodet som hvad. Dette kan klart nok kun gøres, når man ved, at alle bogstaver, man betragter, er indkodet med samme substitutionsalfabet, hvorfor man først ville skulle opdele kodeteksten i 17.576 samlinger af bogstaver. Nu kan man jo så overveje, om Famøs har brudt Enigma på en halv side, men tyskerne var jo ikke dummere end som så, så det var vanskeligere, end det er blevet gjort her. Plugboardets effekt er nemlig blevet glemt i det ovenstående. Plugboardet havde et hul til hvert bogstav og et antal kabler, som kunne forbinde disse huller. Dermed kunne der foretages et antal parvise ombytninger af bogstaver. I starten blev der anvendt seks kabler og dermed seks parvise ombytninger af bogstaver. For den overambitiøse Famøs-redaktør er det et alvorligt problem, da vores fremgangsmåde med at betragte Enigma som en polyalfabetisk substitutionskode nu er mere eller mindre nytteløs. I stedet for at forsøge selv at arbejde videre med Enigma, så lad os se på, hvad andre kloge hoveder har gjort tidligere.

Polsk opfindsomhed og tysk naivitet

Den store udfordring for Biuro Szyfrów i tiden op til 2. verdenskrig var at adskille de forskellige komponenters virkning, som det også blev antydet herover. Hvis man kunne isolere plugboardets virkning, ville man faktisk bare have med parvise ombytninger af bogstaver at gøre. Hvis man kunne isolere scramblernes virkning, ville det være en svær, men overkommelig opgave at bryde koden. Marian Rejewski og hans kolleger begyndte derfor at studere strukturen i maskinens ind- og udkodning.

Tyskerne havde imidlertid selv indlagt en svaghed i deres brug af Enigma. Hver måned blev der til Enigmaoperatørerne distribueret en kodebog indeholdende en startindstilling for hver dag.

(det polske cifferbureau) til at satse på bl.a. matematikere, som kryptoanalytikere. Især den unge matematiker Marian Rejewski udviste stort talent for disciplinen. Hvor franskmændende havde opgivet at bryde koderne, havde polakkerne stadig truslen om et tysk angreb hængende over hovedet, hvilket motiverede dem til at forsøge at bryde Enigmakoden. Enigma var kort fortalt en mekanisering af ind- og udkodning af beskeder. Den bestod af et tastatur, et antal scramblere (tre i den oprindelige militære udgave af Enigma), en reflektor, et plugboard og en lampe for hvert bogstav. Hvis operatøren ville kode fx A, trykkede han på A-knappen, hvorefter der blev skabt forbindelse gennem plugboardet, ledningerne på scramblerne, hen til reflektoren, tilbage gennem scramblerne og hen til plugboard og op til en lampe, hvor operatøren kunne aflæse, hvad A skulle indkodes som. Ind- og udkodning var fuldstændig symmetriske processer, så når operatøren modtog et A og ville udkode det, trykkede han ligeledes på A. Hele pointen var, at man skulle kende de præcise indstillinger for at kunne udkode korrekt. Scramblerne var bevægelige og for hvert ind- eller udkodet bogstav rykkede den yderste sig ét hak. Når den yderste havde bevæget sig en hel omgang, rykkede den næste ét hak og så fremdeles. Dermed gav scramblerne i sig selv en polyalfabetisk substitutionskode med en periode på 17.576 (26^3), da der er 26 bogstaver i det tyske alfabet. Det vil kort sagt sige, at hvert 17.576. bogstav blev indkodet med samme ombytninger af bogstaver og derfor ville man kunne, hvis man havde nok materiale, samle de bogstaver der var indkodet med samme ombytning af bogstaver og anvende frekvensanalyse på hver af disse ombytninger af bogstaver. Frekvensanalyse er en metode, hvor man kigger på hvilke bogstaver (i kodeteksten) der fremgår flest gange og så anvender statistik over anvendelse af bogstaver i fx det tyske sprog for at gætte sig frem til, hvilke bogstaver

lavest positiv grad, der har $v_1 = e^{i\pi/4}$ som rod. Sætningen om division med rest giver

$$\theta(x) = (x^4 + 1)q(x) + r(x) \ ,$$

for polynomier r, q hvor $\text{grad}(r) < 4$. Da

$$0 = \theta(v_1) = (v_1^4 + 1)q(v_1) + r(v_1) = r(v_1)$$

følger det, at v_1 er rod i $r(x)$ og dermed, at r må være nulpolynomiet. Af fremstillingen $\theta(x) = (x^4 + 1)q(x)$ ses derfor, at også v_2, v_3, v_4 er rødder i θ. Dermed vil relationen $(*)$ også være opfyldt, hvis v_1 erstattes af v_2, v_3 eller v_4. Vi kan således konkludere, at Galoisgruppen G for g består af fire elementer, hvoraf de tre har orden 2, og G er således isomorf med Kleins Vierergruppe. I cykelnotation kan vi skrive

$$G = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \ .$$

Klassisk benyttes Galoisgruppen for et polynomium til at afgøre, hvornår det er muligt at 'finde en formel' for rødderne i polynomiet. Det berømte resultat, at det generelle polynomium af grad større end eller lig fem ikke kan løses ved roduddragning, og som normalt tilskrives Abel og Ruffini, kan således henføres til egenskaber ved den symmetriske gruppe S_n for $n \geq 5$. Galois var den første til at relatere løsbarheden af polynomiumsligninger til egenskaber ved den tilhørende permutationsgruppe på rødderne. De dybsindige iagttagelser, som han herved gjorde, har haft vidtrækkende konsekvenser for matematikkens udvikling sidenhen.

Et vilkårligt polynomium har en naturlig tilbøjelighed til at have en stor Galoisgruppe G, dvs. indeks $[S_n : G]$ er lille (se [4] for et præcist udsagn). Statistisk set har de fleste polynomier

derfor den fulde symmetriske gruppe som Galoisgruppe. En lille Galoisgruppe er således tegn på en form for anomali eller asymmetri i polynomiet, der giver det nogle særlige egenskaber, såsom muligheden for at finde formler for rødderne i polynomiet, eller begrænsede faktoriseringsmuligheder modulo et primtal. Vi skal nu, som lovet, se nærmere på nogle af disse afvigere.

En sætning af Dedekind

Vi betragter som nævnt et heltalspolynomium f med lutter simple rødder. Sætningen vi skal formulere forudsætter endvidere, at det koefficientvist reducerede polynomium $\overline{f}$ også har lutter simple rødder. Heldigvis er det ligetil at sikre dette ud fra egenskaber ved f. Hertil har vi brug for diskriminanten. Hvis f har rødder $u_1, \ldots, u_n$ defineres diskriminanten som

$$\operatorname{disk}(f) = \prod_{1 \le i < j \le n} (u_j - u_i)^2 \ .$$

Diskriminanten for $\overline{f}$ er det tilsvarende produkt af kvadratet på differenserne mellem de n rødder i $\overline{f}$ (i et passende udvidelseslegeme). Af definitionen fremgår umiddelbart, at et polynomium har multiple rødder, hvis og kun hvis diskriminanten er nul.

Det er muligt at udtrykke diskriminanten for f alene ved summer og produkter af koefficienterne til f. Da reduktion modulo p er en ringhomomorfi, fremgår heraf formlen

$$\operatorname{disk}(\overline{f}) = \overline{\operatorname{disk}(f)} \ .$$

Heraf ses, at $\overline{f} \in \mathbb{F}_p[x]$ har multiple rødder, hvis og kun hvis diskriminanten for f er delelig med p. Ved at betragte primtal hvor $p \nmid \operatorname{disk}(f)$, sikrer vi os således, at både f og $\overline{f}$ har lutter simple rødder.

at have afgørende indflydelse på Turings liv. Scherbius og Ritter forsøgte sig med alt fra turbiner til opvarmede puder, men af eftertiden blev de især husket for Enigma, krypteringssystemet, som Turing skulle spille en prominent rolle i kampen mod. Selvom Alan Turing fortjent har fået meget af æren for at bryde den tyske Enigmakode, må det nævnes, at en bedrift af den kaliber sjældent kommer fra ét menneske alene. Allerede i 20'erne begyndte den proces, der skulle muliggøre det, som tyskerne troede umuligt, nemlig at Turing og hans hold under 2. verdenskrig formåede at udkode dele af tyskernes krypterede kommunikation. Allerede i mellemkrigstiden havde tyskerne verdens mest sikre, bredt anvendelige krypteringssystem i Enigma. Tidens teknologi muliggjorde en stærkere kryptering, ligesom man også dengang kunne anvende teknikker, der praktisk talt gjorde en tredjeparts dekryptering umulig, men ingen systemer kombinerede kommunikationssikkerhed og anvendelighed, som Enigma gjorde det. Især polakkerne var meget bekymrede over dette, da retorikken fra det tyske nationalsocialistiske parti var skarp over for især Polen. Frankrig og England følte sig derimod godt tilpas som Europas stærkeste nationer efter sejren i 1. verdenskrig og følte derfor ikke noget behov for at læse, hvad tyskerne skrev til hinanden. En fransk spion fik ved lidt af et tilfælde fat i håndbogen til Enigma, ud fra hvilken det var muligt at lave en præcis kopi af maskinen. Franskmændene brugte ikke ressourcer på at prøve at bryde tyskernes koder, men overgav derimod håndbogen til polakkerne, som gerne ville forberede sig på en fremtidig krig.

En hård nød

Historisk set havde kryptografi og kryptoanalyse været udført af sprogkyndige, men den øgede mekanisering fik Biuro Szyfrów

Knæk koden, Alan!

– En fortælling om matematikere og verdenshistorien

Søren Wengel Mogensen

Når en kemiker, en fysiker og en matematiker sidder på Caféen? og diskuterer emner af akut vigtighed, som fx deres respektive fags indflydelse på verdenshistoriens gang, vil kemikeren vel med rette kunne hævde at 1. verdenskrig i høj grad var kemiens krig med den ukritiske anvendelse af kemiske våben som verden for første gang stiftede bekendtskab med. Fysikeren vil nok fremhæve, igen med en vis berettigelse, 2. verdenskrig og Manhattanprojektet, som satte et effektivt punktum for den amerikansk-japanske del af 2. verdenskrig. Matematikeren vil naturligvis som en standardrefleks påpege, at matematikken jo netop er grundlaget for mange andre videnskaber. Imidlertid skal en stolt matematiker heller ikke glemme, at verdenshistorien faktisk rummer tilfælde, hvor matematikken, eller i hvert fald matematikere, var i forreste linje og ikke gemt bag fysiske love, kemiske forbindelser eller lignende. 2. verdenskrig og de allieredes kamp for at bryde de tyske koder er netop et af de tilfælde, hvor matematikere viste sig mere nyttige for krigsindsatsen som skrivebordskrigere end som fodsoldater. Disse matematikere blev naturligvis til en vis grad misforstået af deres samtid, men det skal jo ikke forhindre Famøs i at se tilbage på en stor fortælling om matematik, liv og død.

Enigma

Når talen falder på kodebrydning og 2. verdenskrig, dukker briten Alan Turings navn op i manges hoveder. Turing blev født i 1912 og få år efter grundlagde tyskerne Arthur Scherbius og Richard Ritter en virksomhed, hvis mest kendte produkt skulle vise sig

Sætning 1 (Dedekind) *Lad f være et normeret heltalspolynomium og p et primtal så $p \nmid disk(f)$. Hvis det koefficientvist reducerede polynomium $\overline{f} \in \mathbb{F}_p[x]$ har (den entydige) faktorisering $\tilde{f}_1 \cdots \tilde{f}_r$, med hvert $\tilde{f}_i$ irreducibelt af grad l_i, da indeholder Galoisgruppen for f en permutation som er et produkt af disjunkte cykler $\gamma_1 \cdots \gamma_r$, hvor γ_i har længde $l_i = grad(\tilde{f}_i)$ og $l_1 + \cdots + l_r = grad(f)$.*

Se [2] for nærmere detaljer.

Specielt interesserer vi os for sætningen i den kontraponerede form: Hvis Galoisgruppen for f ikke indeholder nogen permutationer med en bestemt cykeltype $l_1 \dots l_r$, da kan $\overline{f}$ ikke faktorisere som et produkt af irreducible polynomier med graderne $l_1, \dots, l_r$.

Med ovenstående resultat i baghånden er tiden hermed kommet, hvor vi kan demonstrere vores forehavende.

Sætning 2 *Polynomiet $g(x) = x^4 + 1$ er irreducibelt i $\mathbb{Z}[x]$, men reducibelt modulo ethvert primtal.*

Bevis. Som vi har set, har polynomiet $g(x) = x^4 + 1$ Galoisgruppen

$$G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \ .$$

Specielt indeholder G ikke nogen 4-cykel. For et primtal p så $p \nmid \mathrm{disk}(g)$, følger det af Dedekinds sætning, at fjerdegradspolynomiet $\overline{g}$ ikke kan være et produkt af en enkelt irreducibel fjerdegradsfaktor, eller med andre ord, at $\overline{g}$ er reducibelt.

Indsættes rødderne for g i definitionen på diskriminanten ovenfor, kan man beregne $\mathrm{disk}(g) = 2^8$. Vi mangler altså blot at checke primtallet $p = 2$, og modulo 2 finder vi $x^4 + 1 \equiv (x+1)^4 \pmod 2$, altså er $\overline{g}$ også reducibelt modulo 2. □

Endvidere står det klart, ud fra formen på permutationerne i G, at de eneste mulige faktoriseringer af $\overline{g}$, er som et produkt af to andengradsfaktorer eller fire førstegradsfaktorer. Da

$$x^4+1 \equiv (x^2+2)(x^2+3) \pmod 5 ,$$
$$x^4+1 \equiv (x+2)(x+8)(x+9)(x+15) \pmod{17}$$

ses, at begge muligheder forekommer for primtal p, der ikke går op i diskriminanten. Som vi skal se nedenfor, er dette ikke nogen tilfældighed.

Lad os snuppe endnu et eksempel. Polynomiet

$$h(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

har rødderne $w_k = e^{2\pi ik/11} + e^{-2\pi ik/11} = 2\cos(2\pi k/11)$ for $k = 1, \ldots, 5$. Som før eksisterer der relationer mellem rødderne, idet vi har $w_{k+1} = w_k w_1 - w_{k-1}$. Læseren kan selv overbevise sig om, at en permutation σ i Galoisgruppen H for h er entydigt fastlagt ved værdien i w_1. Vælges f.eks. $\sigma(w_1) = w_2$, følger det automatisk, at $\sigma(w_2) = w_4$, $\sigma(w_4) = w_3$, $\sigma(w_3) = w_5$ og $\sigma(w_5) = w_1$. Dermed bliver $\sigma = (12435)$ en 5-cykel, og potenserne af σ vil generere hele Galoisgruppen, altså har vi $H = \langle\sigma\rangle$ og H er cyklisk af orden 5.

Vi er således i en position, hvor vi kan anvende Dedekinds sætning til at udtale os om de mulige faktoriseringer af $\overline{h}$. Hvis $p \nmid \mathrm{disk}(h)$ er der som før kun to muligheder for faktoriseringen af $\overline{h}$. Enten svarer p til den trivielle permutation i Galoisgruppen, og så spalter $\overline{h}$ til bunds som et produkt af fem førstegradsfaktorer, eller også svarer p til en 5-cykel, og da vil $\overline{h}$ være irreducibelt. Beregner man diskriminanten, finder man $\mathrm{disk}(h) = 11^4$ (det bliver en længere udregning). For $p = 11$ er det ikke svært at indse, under brug af binomialformlen, at $h(x) \equiv (x-2)^5 \pmod{11}$. Vi

træk idet spiller B kun kan returnere med at fjerne netop ét af de resterende felter.

Til 3×2 er situationen som følger: Hvis A starter med at fjerne felt nr. 1, så kan (skal) B fjerne felt nr. 3, og dermed tvinge et nederlag til A. Hvis A starter med at fjerne felt nr. 2, så er situationen med 2×2 tilbage, som jo var en vindende position for spilleren der lagde ud, i dette tilfælde B. Altså taber A igen. Fjerner A først felt nr. 3, så kan B fjerne felt nr. 1 – og derved tvinge et nederlag til A igen. Starter A med at fjerne felt nr. 4, så kan B returnere ved at fjerne felt nr. 2 og som før, sikre sig sejren. Den eneste mulighed for A er derfor at starte med at fjerne felt nr. 5. Hvis vi antager A gør dette, så kan spillet fortsætte på følgende måde:

— Hvis B fjerner felt nr. 1, så skal A fjerne felt nr. 3 og dermed vinde.
— Hvis B fjerner felt nr. 2, så er vi i 2×2-situationen igen, hvorved A kan vinde.
— Hvis B fjerner felt nr. 3, så kan A fjerne felt nr. 1 og vinde.

Hvis B fjerner felt nr. 4, så er der tre tilfælde tilbage:

- Hvis A fjerner felt nr. 1, så kan B vinde ved at fjerne felt nr. 3.
- Hvis A fjerner felt nr. 3, så kan B vinde ved at fjerne felt nr. 1.
- Hvis A fjerner felt nr. 2, så har B tabt.

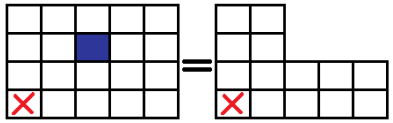
Konklusionen på denne analyse er:
Hvis A fjerner felt nr. 5 først, så har han en mulig vinderstrategi. Kan du finde en generel vindende strategi?

– GOD SPILLELYST!

Blokkens spil
– Chomp

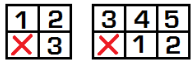
Bo 'Maling' Malling

I denne udgave af blokkens spil ser vi på spillet *Chomp*. Chomp kan altid spilles når der er en plade chokolade til rådighed og dét er også grunden til spillets lidt mærkelige navn.



Figur 1 Her foretages der et træk af spiller A i et spil Chomp med størrelse 5×4.

Chomp kræver 2 spillere (A og B), samt en $m \times n$ spilleplade. Hver spiller skiftes til at vælge et felt, hvorefter alle felterne til højre og ovenfor fjernes. Den der spiser det sidste stykke chokolade taber spillet[4]. Se figur 1.



Figur 2 Et spil 2×2 og et spil 3×2 Chomp.

Bemærk at hvis man spiller på en $n \times 1$ plade, så er det muligt for spiller A ved sit første træk at fjerne $n - 1$ felter, og dermed tvinge en sejr i land. Dette gælder også for $1 \times n$. Ser vi i stedet for på 2×2, som illustreret herover, så vil felt nr. 2 være et vindende

[4]Enten fordi det stykke chokolade er giftigt eller ved brug af princippet om at den der tager det sidste stykke giver næste gang.

kan heraf samlet konkludere, at h har den usædvanlige egenskab, at for ethvert primtal p er $\overline{h} \in \mathbb{F}_p[x]$ enten irreducibelt eller et produkt af fem førstegradsfaktorer.

Ovenstående resultat kan anvendes til let at afgøre, om $\overline{h}$ er irreducibelt. Der gælder nemlig for $p \neq 11$, at $\overline{h}$ er reducibelt hvis og kun hvis $\overline{h}$ har alle sine fem rødder i $\mathbb{F}_p$. Da $\mathbb{F}_2$ og $\mathbb{F}_3$ indeholder færre end fem elementer, kan $\overline{h}$ ikke have fem forskellige rødder modulo 2 eller 3, så i disse tilfælde bliver $\overline{h}$ automatisk irreducibelt. Videre ses med et halvt øje, at $\overline{h}$ er irreducibelt modulo 5 og 7. I første tilfælde er det nemlig nok at indse, at 0 ikke er rod, og i andet tilfælde skal det endvidere checkes, at f.eks. ± 1 ikke er rødder. Det første tilfælde hvor $\overline{h}$ har fem forskellige rødder i $\mathbb{F}_p$, indtræffer for $p = 23$.

Frobenius' Densitetssætning

Vi har set, at de irreducible faktoriseringer af $\overline{f}$, medfører eksistensen af hertil svarende permutationer i Galoisgruppen for f. Frobenius' Densitetssætning garanterer omvendt, at der til givne permutationer i Galoisgruppen, altid findes uendeligt mange primtal, så $\overline{f}$ har en faktorisering svarende til cykeltypen for permutationen. Da enhver gruppe indeholder den trivielle permutation, indebærer dette specielt, at der for et vilkårligt polynomium f, altid findes uendeligt mange primtal, så $\overline{f}$ spalter til bunds i førstegradsfaktorer.

Sætning 3 (Frobenius) *Lad f være et normeret heltalspolynomium uden multiple rødder. Antag at Galoisgruppen for f indeholder en permutation, der er et produkt af disjunkte cykler $\gamma_1 \cdots \gamma_r$, hvor γ_k er en cykel af længde l_k for $k = 1, \ldots, r$. Da findes uendeligt mange primtal p, så $\overline{f} \in \mathbb{F}_p[x]$ faktoriserer som et produkt af irre-*

ducible faktorer med graderne $l_1, \ldots, l_r$. Ydermere er tætheden af sådanne primtal givet ved kvotienten $N/|G|$, hvor N er antallet af permutationer i G med cykeltype $\gamma_1 \cdots \gamma_r$.

Med tætheden mener vi: Hvis P_n er antallet af primtal mindre end n og Q_n er antallet af primtal mindre end n der giver anledning til en faktorisering svarende til permutationen $\gamma_1 \cdots \gamma_r$, da er tætheden givet ved

$$\lim_{n\to\infty} \frac{Q_n}{P_n} = \frac{N}{|G|} .$$

Vi ser således, at det ikke var noget tilfælde, da vi ovenfor kunne finde primtal p, så polynomierne $g(x)$ og $h(x)$ havde en faktorisering svarende til hver type permutation i Galoisgruppen. Yderligere kan vi ud fra sætningen bestemme, hvor ofte hver type faktorisering gennemsnitligt vil forekomme. For tilfældet $g(x) = x^4 + 1$ vil således i gennemsnit hvert fjerde primtal resultere i en faktorisering af $\overline{g}$ som et produkt af fire førstegradsfaktorer, mens de øvrige tre fjerdedele af primtallene vil give en faktorisering af $\overline{g}$ som et produkt af to andengradsfaktorer. Tilsvarende gælder for $h(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$, at for fire femtedele af primtallene vil $\overline{h}$ være irreducibelt, mens $\overline{h}$ for de resterende primtal p, vil have alle sine rødder i $\mathbb{F}_p$.

Det er naturligt at spørge, for hvilke primtal de forskellige faktoriseringer indtræffer. For tilfældet $g(x) = x^4 + 1$ kan man vise, vha. basale resultater om kvadratisk reciprocitet, at $\overline{g}$ faktoriserer som et produkt af fire førstegradsfaktorer når $p \equiv 1 \pmod 8$, og som et produkt af to andengradsfaktorer når $p \not\equiv 1 \pmod 8$. Dette resultat indebærer jævnfør ovenstående, at tætheden af primtallene, der er kongruente med 1 modulo 8, er 1/4. Som tilføjelse hertil kan nævnes, at dette er i overensstemmelse med Dirichlets sætning om primtal i aritmetisk progression, der netop

Alle kender dem:
Ernsts kassogrammer

1. år

MatIntro	LinAlg	An 0	An 1
Dis	SS	Alg 1	Geom 1

men kun få er klar over at de er 3-dimensionelle

1. år

Litteratur

[1] R. Guralnick, M. Schacher and J. Sonn, *Irreducible polynomials which are locally reducible everywhere*, Proceedings of the AMS Vol. 133 (2005), no. 11, p. 3171-3177.

[2] C. U. Jensen, *Matematik 4AL*, Matematisk Afdeling KU.

[3] P. Stevenhagen & H. W. Lenstra, *Chebotarëv and his density theorem*, The Mathematical Intelligencer Vol 18. No. 2, 1996.

[4] B. L. van der Waerden *Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt*, Monatsh. Math. 43 (1936), 137-147.

angiver tætheden af primtal kongruent med 1 modulo 8 til at være $1/\varphi(8) = 1/4$ (φ er Eulerfunktionen). For nærmere detaljer om relationen mellem sætningerne af Dirichlet og Frobenius, samt et bevis for Chebotarëv's Densitetssætning, som generaliserer dem begge, se [3].

En karakterisering af primtallene

Vi har set, at polynomiet x^4+1 er irreducibelt i $\mathbb{Z}[x]$, men reducibelt modulo ethvert primtal p. Med hjælp fra Frobenius' Densitetssætning kan vi nu vise, at eksistensen af et polynomium med denne egenskab ikke er helt triviel, idet et polynomium med primtalsgrad ikke kan have selvsamme egenskab.

Sætning 4 *Lad q være et primtal og $f \in \mathbb{Z}[x]$ et normeret irreducibelt polynomium af grad q. Da findes uendeligt mange primtal p, for hvilke $\overline{f} \in \mathbb{F}_p[x]$ er irreducibelt.*

Bevis. Det er velkendt, at et irreducibelt polynomium over $\mathbb{Z}$ ikke kan have multiple rødder. Ideen er derfor at vise, at Galoisgruppen G for f indeholder en q-cykel, thi da følger eksistensen af primtallene p fra Frobenius' Densitetssætning. Det er et generelt resultat, at Galoisgruppen for et irreducibelt polynomium endvidere bliver transitiv, altså at der til to vilkårlige rødder i f, findes en permutation i G, der sender den ene rod til den anden. Betragt derfor undergruppen

$$G^1 = \{\sigma \in G \mid \sigma(1) = 1\} \ .$$

To permutationer $\sigma, \tau \in G$ er ækvivalente modulo G^1 hvis og kun hvis $\sigma^{-1}\tau$ tilhører G^1, som sker hvis og kun hvis $\sigma(1) = \tau(1)$. Da G er transitiv forekommer samtlige værdier $1, \ldots, q$ som værdi i

1 for permutationer i G. Der er altså q sideklasser modulo G^1. Lagranges Indekssætning giver derfor, at $[G : G^1] = q$ er divisor i $|G|$. Da G endvidere er en undergruppe i S_q, der har orden $q!$, må $|G| = qm$ hvor q og m er primiske. Det følger nu direkte af Sylows Første Sætning, at G har en undergruppe af orden q, og specielt altså indeholder en q-cykel. □

Specielt er fire den laveste grad, for hvilken noget irreducibelt polynomium kan være reducibelt modulo ethvert primtal. Videre kan man spørge sig selv, hvorvidt der findes et sjettegradspolynomium med samme egenskab, eller mere generelt et polynomium af grad n for et vilkårligt sammensat tal n. Det viser sig faktisk, at primtalsgraden er den eneste forhindring for, at polynomiet kan have den omtalte egenskab, og der findes således irreducible polynomier af enhver sammensat grad, der er reducible modulo ethvert primtal. Beviset herfor er dog ikke trivielt, se f.eks. [1]. Dette giver os følgende karakterisering af primtallene:

Sætning 5 *Et naturligt tal $n \neq 1$ er et primtal hvis og kun hvis der* ***ikke*** *findes et irreducibelt polynomium f af grad n, så $\overline{f}$ er reducibelt modulo ethvert primtal p.*

Selvom der altså findes irreducible polynomier af enhver sammensat grad, der er reducible modulo ethvert primtal, og selvom der altid findes uendeligt mange primtal, for hvilke et givent polynomium spalter til bunds i førstegradsfaktorer, er der alligevel en grænse for, hvor tosset et irreducibelt polynomium kan te sig modulo p. En elementær sætning af Burnside udsiger nemlig, at en transitiv undergruppe af S_n for $n \geq 2$ altid vil indeholde en permutation uden fikspunkter. Anvendt på Galoisgruppen for et irreducibelt polynomium f af grad mindst 2, følger det af Frobenius' Densitetssætning, at der findes uendeligt mange primtal p, for hvilke $\overline{f}$ ikke har en rod i $\mathbb{F}_p$.

Afrunding

Læseren kan nu selv tage sin yndlingsgruppe og fundere over, hvilke sjove egenskaber et polynomium med denne gruppe som Galoisgruppe kan have. Som følge af Cayleys Sætning kan enhver endelig gruppe nemlig opfattes som en permutationsgruppe, idet en gruppe af orden n kan indlejres som en transitiv undergruppe i den symmetriske gruppe S_n. Desværre er det sjældent nogen let opgave at bestemme et polynomium med en given gruppe som Galoisgruppe, ja faktisk er det et endnu uløst problem, kendt som Galoisteoriens omvendingsproblem, at afgøre hvorvidt enhver endelig gruppe kan realiseres som Galoisgruppe for et polynomium med koefficienter i $\mathbb{Q}$ (eller ækvivalent hermed, for et normeret polynomium med heltalskoefficienter). Her 180 år efter Évariste Galois' død (i øvrigt i en alder af kun 20 år, som følge af sår tildraget i en duel!), fortsætter den eponyme matematiske disciplin således med at rejse ubesvarede spørgsmål, generere overraskende resultater og give inspiration til matematikere i alle aldre.

Galois skrev aftenen før den fatale duel: 'Der er endnu noget at eftervise. Jeg har ikke tid.' Heldigivs har mange sidenhen haft tid til at udvikle hans originale ideer, således at de tanker Galois oprindeligt satte i verden, i dag kan bibringe anvendelser langt ud over, hvad Galois selv kunne have forestillet sig.