Diskret matematikk finnes ikke

D. Laksov

Matematiska Institutionen, KTH
SE–100 44 Stockholm
laksov@math.kth.se

Matematikk og anvendelser

Det skrives mye om diskret matematikk som et *nytt* område av matematikken med interessante anvendelser, fra brevutbæring til livets opprinnelse. På NV-programmet i gymnasene i Sverige har emnet *matematik diskret* blitt obligatorisk på «matematik/datalogi» grenen. Det oppsiktsvekkende med dette er at det ikke finnes noe matematisk område som heter *Diskret matematikk* og at det er både unaturlig og uinteressant å dele inn matematikken i *diskret matematikk* og *annen matematikk*. Spesielt forvirrende er det at anvendelsene som denne *diskrete* matematikken skulle gi opphav til ofte viser seg å være banale omformuleringer av matematiske begreper med ord hentet fra hverdagslivet og uten praktisk betydning. Et typisk eksempel er når man omformulerer et kjent problem av en av tidenes mest fremstående matematikere W. R. Hamilton (1805–1865) om *stier* i en *graf*, som et problem som postmenn møter når de skal dele ut post, eller som handelsreisende må løse for å besøke kunder mest effektivt. Ikke bare er anvendelsene urealistiske, men man har heller ikke bidratt noe til løsningen av problemet ved å kle det i ny språkdrakt. Vi har illustrert dette med et utførlig eksempel nedenfor.

Slike *pseudoanvendelser* trekker oppmerksomheten bort fra matematikken som et aktivt og sentralt vitenskapelig emne, med fundamentale naturvitenskapelige og tekniske anvendelser. Det er knapt noe område av et høyteknologisk samfunn som skulle fungere uten bruk av matematisk teori og matematiske formler.

Hysteriet med å fremstille deler av matematikken som «diskret» oppsto i forbindelse med datamaskinene. Intuitivt er disse «diskrete av naturen» ettersom de inneholder en endelig mengde informasjon, og alle operasjonene kan beskrives med 0-er og 1-ere. Ettersom bruken av datamaskinene fikk så stor oppmerksomhet og ble spådd en stor økonomisk betydning var det fristende å fremstille sin egen lille

spesialitet i matematikken som spesielt passende for datamaskiner, og for kommunikasjon på nettet. Dermed kunne de være med å «dele på kaken». Det er også riktig at datamaskinene skulle bli langsomme og klumpete, ja nesten ubrukelige, og at kommunikasjonen på nettet umulig, uten omfattende bruk av matematikk. For eksempel er komprimering av lyd og bilder, og lyd- og bildegjenkjennelse, som spiller en stor rolle for lagring av informasjon i datamaskiner og for kommunikasjonen av datamengder mellom dem, basert på resultater om trigonometriske funksjoner funnet av J. Fourier (1768–1830), eller på *wavelets* som ble initiert av den svenske matematikeren J. O. Strömberg for 20–30 år siden. Kryptering av informasjon på nettet, som er avgjørende for all handel på nettet, og som vi bruker hver gang vi stikker et bankkort i en automat, er basert på resultater i tallteori funnet av P. Fermat (1601–1665). Hele teorien for informasjonsoverføring, og spesielt for det mye omtalte *bredbånd*, ble utviklet av C. E. Shannon (1916–2002), og er basert på *statistisk mekanikk*, *termodynamikk* og *klassisk potensialteori* fra fysikken. Dette er bare noen eksempler som viser hvilken fundamental rolle matematikken spiller i dagens samfunn. Eksemplene viser også at det ikke er noen spesiell del av matematikken som passer bra for anvendelser på datamaskiner. Spennvidden mellom *Fourierrekker*, *Fermats lille sats* og *informasjonsteori* er enorm. Det er heller ingen av disse områdene som utmerker seg som spesielt *diskret*. At vi har en følelse av at datamaskinene virker på en «diskret måte» i noen mening, betyr selvsagt ikke at den matematikken som beskriver operasjonene i datamaskinene har noen spesiell «diskret karakter». Bredden av den matematikken som brukes i teknikk og vitenskap er imponerende. De fleste anvendelsene av matematikken er basert på en solid forståelse av matematikk, god innsikt i det praktiske problemet og ofte på geniale idéer om hvordan matematikken og anvendelsene kan kombineres. De mest overraskende matematiske resultater kommer til nytte, ofte slike som er funnet for hundretalls år siden, selvsagt uten tanke på anvendelser.

Takk til referent og redaktør. Jeg vil benytte anledningen til å takke referenten for velmotivert og konstruktiv kritikk av den første versjonen av denne artikkelen. Utformningen og innholdet i versjonen nedenfor skyldes til en stor del redaktør Marius Overholts optimistiske tolkning av referentrapporten og hans inspirerende og oppmuntrende synspunkter.

Matematikkens omfang

At det er så mange ulike deler av matematikken som har naturvitenskapelige og tekniske anvendelser reflekterer at matematikken er et gigantisk forskningsområde. Bredden av matematikken er langt større enn hva de fleste er klare over. Vi deler inn matematikken i 63 hovedområder. Hver av disse er oppdelt i underområder, som igjen er oppdelt i mindre deler. I Appendiks A har vi listet hovedklassifikasjonen av matematikken. Denne kaller vi AMS-klassifikasjonen fordi den blir utgitt av American Mathematical Society. Hele klassifikasjonen med alle underavdelingene omfatter 56 tettskrevne A4-sider. For å illustrere mangfoldet har vi i Appendiks B også gitt grovklassifikasjonen for ett av hovedområdene i matematikken, nemlig algebraisk geometri (AMS-klassifikasjon 14), og i Appendiks C har vi også alle underklassene av en av disse (AMS-klassifikasjon 14H–xx Curves). Spennvidden av

matematikken er så stor at en matematiker som arbeider på et hovedområde har like store vanskeligheter med å forstå hva en matematiker på et annet område gjør, som en ekspert på atomfysikk har for å forstå en ekspert på vulkaner.

Ingen av de 63 områdene, eller deres underområder heter *diskret matematikk*, og det tjener hverken noen hensikt, eller er spesielt påtrengende å påstå at noen delområder er mer *diskrete* enn andre. Intuitivt har vi en presis følelse av hva *diskret* betyr. For eksempel vil minuttviseren på en klokke bevege seg fra 0 til 60 i en eneste kontinuerlig bevegelse, og alle tall mellom 0 og 60 blir passert. Sekundviseren derimot hopper mellom sekundene og tar bare 60 ulike verdier. Vi oppfatter derfor bevegelsen til sekundviseren som *diskret*, mens minuttviseren beveger seg *kontinuerlig* eller i *realtid*. Prøver man å overføre denne intuisjonen til en konkret beskrivelse av hva som burde være *diskret* i matematikken får man store problemer. Oppfatter vi *kontinuerlig* som det omvendte av diskret hjelper det ikke mye. Begrepet *kontinuitet* finnes i alle deler av matematikken, selv når vi bare skal studere et endelig antall objekter. En av hensiktene med denne artikkelen er å presentere et par typiske eksempler på at begrepene *avstand* og *kontinuitet* kommer inn i de meste uventede situasjoner som vi normalt oppfatter som *diskrete*. Prøver vi isteden å holde fast på at minuttviseren passerer alle reelle tall mellom 0 og 60 så hjelper det like lite for å beskrive hva som bør være *kontinuerlig* matematikk, ettersom de reelle tallene spiller en fundamental rolle i nesten alle deler av matematikken.

Om vi istedenfor, litt naivt, antar at «Skolverket» i Sverige har løst problemet med å presisere diskret matematikk og definerer *diskret* ut fra kurset *Matematik diskret* på NV-programmet i svenske gymnaser så finner vi at *diskret matematikk* består av en liten brøkdel av de enkleste delene av områdene *Matematisk logikk* (AMS-klassifikasjon 03), *Kombinatorikk* (AMS-klassifikasjon 05), *Tallteori* (AMS-klassifikasjon 11), og *Datalogi* (AMS-klassifikasjon 68). Det kan være interessant å merke at den brøkdelen av Kombinatorikk som er med i Matematik Diskret egentlig hører hjemme i *Sannsynlighetsteorien* (AMS-klassifikasjon 60).

Resonnementer som gir seg ut for å være diskrete er ofte enkle og basert på allmenne betraktninger som man ikke behøver noen matematisk utdannelse for å utføre. Problemene har ofte karakteren av spill eller underholdningsmatematikk, og virker tilgjorte. Anvendelse er naive, på grensen til det latterlige, og er ofte rene omskrivninger av matematiske begreper i dagligspråk. De krever hverken innsikt i anvendelsene eller i matematikken. Dette kan virke lokkende på unge uerfarne personer som tror de kan drive matematikk uten en solid teoretisk bakgrunn, og som håper på å oppnå sensasjonelle anvendelser uten å ha kjennskap til området de skal bruke matematikken på. Dermed gjør de en tragisk feil fordi matematikkens skjønnhet og karakter ligger i kunnskapene om matematiske teorier og resultater og det fascinerende samspillet mellom disse. Det er også de dypere matematiske resultatene sammen med solide innsikter i praktiske problemer som leder til de epokegjørende tekniske og naturvitenskapelige anvendelsene av matematikken. Uten omfattende kunnskaper og innsikter i matematikken kan man hverken ha glede av matematikken eller anvende den til noe fornuftig.

Er endelige mengder «diskrete» eller «kontinerlige»?

Som nevnt er det vanlig å definere «diskret matematikk» som de delene av matematikken som ikke er «kontinuerlige». Begrepet kontinuerlig er velkjent fra analysen og bygger på at vi kan snakke om *avstander*, og derfor kan avgjøre når punkter ligger nære eller langt fra hverandre. Det finnes imidlertid naturlige avstandsbegreper, med store anvendelsesområder, selv på endelige mengder. Vi kan derfor resonnere geometrisk og snakke om kontinuitet på endelige mengder. Derfor er det verdiløst å forsøke å skille diskret fra kontinuerlig på denne måten.

Før vi gir et eksempel på avstandsmål på endelige mengder skal vi presisere hva vi mener med *avstand*. Vi vet at hvert reelt tall a har en absoluttverdi $|a|$. Avstanden mellom to tall a og b er absoluttverdien $|a-b|$ av differansen mellom tallene. Hele den reelle analysen med kontinuitet, deriverbarhet og integrerbarhet er bygget på denne absoluttverdien og tilsvarende avstandsmål i høyere dimensjoner. Selvsagt holder følgende tre egenskaper:

1. (Ikkedegenererthet) $|a| = 0$ hvis og bare hvis $a = 0$.
2. (Multiplikativitet) $|ab| = |a||b|$.
3. (Trekantulikheten) $|a + b| \leq |a| + |b|$.

Egenskaper (1) og (3) tilfredsstilles av absoluttverdien $|(a, b)| = \sqrt{a^2 + b^2}$ i planet, og den tilsvarende absoluttverdien $|(a_1, a_2, \ldots, a_n)| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$ i høyere-dimensjonale rom. Vi velger disse egenskapene som en modell for avstand på vilkårlige mengder. Vilkår (2) må vi, som i de høyere-dimensjonale tilfellene, ta bort ettersom vi ikke har noen naturlig multiplikasjon.

Definisjon. La S være en vilkårlig mengde. En avstand, eller som vi sier *metrikk*, på S assosierer et ikkenegativt tall $d(x, y)$ til hvert par av elementer x, y i S slik at for alle tripler av elementer x, y, z i S så vil følgende egenskaper være tilfredsstilt:

1. (Ikkedegenererthet) $d(x, y) = 0$ hvis og bare hvis $x = y$.
2. (Symmetri) $d(x, y) = d(y, x)$.
3. (Trekantulikheten) $d(x, z) \leq d(x, y) + d(y, z)$.

En mengde S med en metrikk d kaller vi et *metrisk rom*. Spesielt blir de reelle tallene $\mathbf{R}$, eller det n-dimensjonale rommet metriske rom med metrikken

$$d(x, y) = |x - y|.$$

Koder. Eksemplet vi skal gi på en endelig mengde med en avstand, det vil si en metrikk, kommer fra kodeteorien. Som alle vet kan all informasjon overføres til digital kode, det vil si, til strenger av 0-er og 1-ere. Det vanlige er at all informasjon som skal lagres eller sendes skrives som strenger av 0-er og 1-ere av en fast lengde n. Vi skal bruke en mer fantasieggende terminologi og si at informasjon er overført til *ord av lengde n med bokstaver fra alfabetet* $0, 1$. For eksempel er *byte* en vanlig enhet for informasjon, og betyr den informasjonen som rommes i de $2^8 = 256$ ordene av lengde 8 fra alfabetet $0, 1$.

Avstanden mellom to ord definerer vi som antallet posisjoner der ordene er ulike. For eksempel er avstanden $d(x, y)$ mellom ordene $x = 01100111$ og $y = 10101100$ lik 5 fordi de skiller seg i første, andre, femte, syvende og åttende posisjon. Avstanden mellom $x = 11110000$ og $y = 00001111$ er 8 ettersom x og y skiller seg i alle de 8 posisjonene. Det er en instruktiv og underholdende oppgave å vise at ordene i en byte med dette avstandsbegrepet danner et metrisk rom. Denne metrikken kalles *Hammingmetrikken* etter Richard Hamming (1915–98).

At Hammingmetrikken er både naturlig og viktig ser vi når vi bruker den på *feilrettende koder*. Anta at vi vil sende informasjon i form av ord av lengde 8 med bokstaver fra alfabetet $0, 1$ over en kanal der det forekommer støy slik at det ordet som blir mottatt kan skille seg fra det ordet vi sendte. Hva skal vi gjøre for å oppdage, eller til og med rette, feil? Den vanligste måten å oppdage feil på er ved å foreta en *paritetssjekk*, det vil si, vi lar selve meddelelsen være de første 7 bokstavene og lar den åttende bokstaven være 0 om det forekommer et like antall 1-ere blant de syv første bokstavene, og lar den være 1 om det forekommer et odde antall 1-ere. Vi kaller den åttende bokstaven for et *kontrollsiffer*. For eksempel har ordene 01100110 og 10101111 rett paritet. Sender vi ordet 01100110 og det oppstår en feil slik at vi mottar 01101110 eller 01100111 så har ordet vi mottar feil paritet og vi vet at en feil har oppstått. Derimot kan vi ikke oppdage to feil ettersom ordet 00000110 har rett paritet og forekommer fra 01100110 om vi gjør en feil i andre og tredje posisjonen. Vi kan heller ikke rette en feil fordi ordet 01101110 som har feil paritet kan fremkomme fra 01100110 og 01101100, begge med rett paritet, om vi gjør en feil.

Prisen for å oppdage en feil er at vi bare kan sende $2^7 = 128$ meddelelser, ettersom den åttende bokstaven er bestemt av de 7 første. Vil vi dessuten rette en feil er prisen mye høyere. For å se dette bruker vi Hammingmetrikken for å få et geometrisk bilde av situasjonen. Om vi skal rette en feil må avstanden mellom to kodeord være minst 3. Dette er fordi, om vi sender et kodeord x og mottar ordet x' med 1 feil, vil $d(x, x') = 1$. Om y er et annet kodeord og $d(x, y) \geq 3$ får vi av trekantulikheten at

$$3 \leq d(x, y) \leq d(x, x') + d(x', y) = 1 + d(x', y),$$

det vil si, vi har $d(x', y) \geq 2$. Med andre ord må det har forekommet minst 2 feil om vi sendte y og mottok x'. Derfor må vi ha sendt x om det bare har forekommet en feil. Vi kan formulere kravet at avstanden mellom to kodeord skal være minst 3 geometrisk ved å si at for å rette en feil må hver sfære med radius 1 omkring et kodeord, ikke inneholde noe annet kodeord.

Vi kan håpe at det rekker å bruke to kontrollsifre for å rette en feil. Faktum er at det ikke engang rekker med tre kontrollsifre. Dette er fordi en sfære med radius 1 omkring et ord x inneholder nøyaktig 9 ord, nemlig x og de 8 ordene vi får av x ved å endre på en bokstav. Om vi skal rette en feil så vi at sfærene av radius 1 om kodeordene må være disjunkte. Bruker vi 3 kontrollsifre kan vi velge de fem første sifrene fritt så vi har 2^5 kodeord og de 2^5 sfærene om disse med radius 1 må være disjunkte. Dette gir $2^5(2^3+1) = 2^8+2^5$ kodeord, som er mer enn det totale antallet 2^8 kodeord av lengde 8 med bokstaver fra alfabetet $0, 1$. Dette er umulig, så vi har vist at vi må bruke minst 4 kontrollsifre for å rette en feil. I sannhet en høy pris.

Dette forklarer hvorfor det er så viktig å finne gode koder med få kontrollsifre i forhold til antallet kodeord.

Mer generelt består en *blokk-kode* av lengde n fra et alfabet A av en undermengde C av mengden B av alle ord av lengde n med bokstaver fra alfabetet A. Elementene i C kalles *kodeord*. Hammingavstanden $d(x, y)$ er antallet posisjoner der ordene x og y er forskjellige. Som ovenfor er det en underholdende oppgave å verifisere at dette gir en metrikk på B. *Hammingdistansen* d_C for en kode C er den minste avstanden mellom to kodeord, det vil si

$$d_C = \min\{d(x, y) \colon \text{for alle distinkte punkter } x \text{ og } y \text{ i } C\}.$$

En kode med Hammingdistanse d_C kan rette $\lfloor (d_C - 1)/2 \rfloor$ feil. Dette sees som ovenfor. Om ordet x i C er et kodeord og x' et ord vi får fra x om vi gjør høyst $\lfloor (d_C - 1)/2 \rfloor$ feil så gir trekantulikheten at for hvert kodeord y så vil

$$d_C \leq d(x, y) \leq d(x, x') + d(x', y) \leq \lfloor (d_C - 1)/2 \rfloor + d(x', y) < d_C/2 + d(x', y).$$

Det vil si at $(d_C - 1)/2 < d_C/2 < d(x', y)$ så x er det eneste kodeordet som kan gi opphav til x' om vi gjør høyst $\lfloor (d_C - 1)/2 \rfloor$ feil.

Det er lett å forstå at det er vanskelig å konstruere koder med mange kodeord i forhold til kontrollsifre. Kodene skal også være lette å bruke, så det må finnes enkle regler for koding og dekoding. Noen av de beste kodene fåes ved å bruke strukturen på *elliptiske kurver*, det vil si (i alle fall om *karakteristikken* er forskjellig fra 2 og 3) løsninger til ligningen

$$y^2 = 4x^3 - g_2 x - g_3 \quad \text{med} \quad \Delta = g_2^3 - 27 g_3^2 \neq 0.$$

Det vil gå for langt å beskrive den omfattende teorien for elliptiske kurver. Studiet av elliptiske kurver tilhører området algebraisk geometri (se 14H52 i Appendiks C). Her blandes algebraiske, analytiske, tallteoretiske og geometriske metoder på en måte som gjør at alt snakk om diskret og kontinuerlig er totalt meningsløst. Som en kuriositet vil vi nevne at elliptiske kurver spilte en hovedrolle da Fermats store sats, eller som den mer korrekt ble kalt *Fermats formodning*, det vil si at ligning $x^n + y^n = z^n$ ikke har noen heltallsløsninger slik at $xyz \neq 0$ når $n > 2$, ble løst på slutten av nittenhundretallet. Det var Gerhard Frey som bemerket at det var en forbindelse mellom Fermats formodning og elliptiske kurver. Dette ledet til en enorm aktivitet blant verdens fremste eksperter på området, og til Andrew Wiles' og Richard Taylors bevis for formodningen, samt til bevis for noen av de viktigste formodningene om elliptiske kurver (se [3]). Beviset er en av de fremste matematiske innsatsene på slutten av nittenhundretallet og løste det kanskje mest kjente av alle matematiske problemer som hadde stått åpent i omtrent 350 år.

Er de hele tallene «diskrete»?

Om vi vil bruke vår intuisjon for å beskrive hva som bør være diskret matematikk ligger det nær å ta de hele tallene som et eksempel. Igjen blir vi bedratt av

intuisjonen. Det finnes uendelig mange avstandsbegrep på de hele tallene, ett for hvert primtall, som alle gir viktig informasjon om de hele tallene og som har store anvendelsesområder i og utenfor matematikken.

For å beskrive disse avstandsmålene fikserer vi et primtall p. Fra de innledende universitetskursene vet vi at hvert helt tall $n \neq 0$ kan skrive entydig på formen $n = p^k m$ der k er et ikkenegativt heltall, og m er heltall som ikke er delbart med p. Vi innfører et avstandsmål på de hele tallene $\mathbf{Z}$, eller en *p-adisk valuasjon* som det kalles mer teknisk, ved

$$|n|_p = 1/p^k.$$

For eksempel, om $p = 3$ får vi $|18|_3 = 1/3^2$ ettersom $18 = 3^2 \cdot 2$, vi har $|30|_3 = 1/3$ ettersom $30 = 3 \cdot 10$, og $|20|_3 = 1$ siden $20 = 3^0 \cdot 20$. Tallet 0 er spesielt ettersom det deles av alle potenser av p, så vi setter $|0|_p = 0$. Det er en grei og illustrativ oppgave å vise at følgende tre egenskaper holder:

1. (Ikkedegenerthet) $|n|_p = 0$ hvis og bare hvis $n = 0$.
2. (Multiplikativitet) $|mn|_p = |m|_p|n|_p$.
3. (Ikke-arkimedisk trekantulikhet) $|m + n|_p \leq \max(|m|_p, |n|_p)$.

Vi merker at trekantulikheten er sterkere enn den vi brukte tidligere ettersom vi normalt har $\max(|m|_p, |n|_p) < |m|_p + |n|_p$. Det er klart at vi får en metrikk d_p på $\mathbf{Z}$ ved å sette

$$d_p(m, n) = |m - n|_p$$

for alle hele tall m og n.

I analysen har vi sett hvordan vi fra de rasjonale tallene med den vanlige normen kan konstruere de reelle tallene. Prosessen kalles *komplettering* og kan baseres på *Cauchyfølger*. Denne konstruksjonen er tatt med i mange lærebøker. Vi minner om at en Cauchyfølge i et metrisk rom er en følge av elementer $x_1, x_2, \ldots$ fra X slik at for alle tall $\varepsilon > 0$ finnes et heltall N slik at $d(x_i, x_j) < \varepsilon$ når $i, j \geq N$. Grunnen til at vi oppfatter de hele tallene som «diskrete» er at det ikke finnes andre Cauchyfølger $n_1, n_2, \ldots$ av hele tall med den vanlige absoluttverdien enn de der $n_N = n_{N+1} = \cdots$ for en N.

Situasjonen er helt annerledes for de hele tallene med en p-adisk valuasjon. For eksempel vil følgen

$$a_1 = 1, \quad a_2 = 1 + p, \quad a_3 = 1 + p + p^2, \quad a_n = 1 + p + \cdots + p^n, \quad \cdots$$

være en Cauchyfølge for den p-adiske valuasjonen. Dette er fordi når $m < n$ vil $|a_n - a_m|_p = |p^{m+1} + p^{m+2} + \cdots + p^n|_p = 1/p^{m+1}$ som raskt går mot 0 når m vokser.

Samme konstruksjon som gir de reelle tallene $\mathbf{R}$ fra de rasjonale $\mathbf{Q}$ med absoluttverdien kan brukes på $\mathbf{Z}$ med den p-adiske valuasjonen og gir et tallområde $\mathbf{Z}_p$ med en p-adisk valuasjon der alle Cauchyfølger konvergerer. Om leseren vil ha en fullstendig analogi med konstruksjonen av $\mathbf{R}$ fra $\mathbf{Q}$, så kan man begynne med den p-adiske valuasjonen på $\mathbf{Q}$ definert ved $|m/n|_p = |m|_p/|n|_p$ for alle heltall m og $n \neq 0$, og komplettere $\mathbf{Q}$ i denne valuasjonen. Vi får da en tallkropp $\mathbf{Q}_p$ med en p-adisk

valuasjon der alle Cauchyfølger konvergerer. Vi kaller elementene i $\mathbf{Q}_p$ de *p-adiske tallene*. Kurt Hensel (1861–1941) utviklet i begynnelsen av nittenhundretallet en teori for p-adiske tall og satt disse inn i en meget bred matematisk sammenheng med forbindelser til analyse, algebra og geometri.

Hvert element i $\mathbf{Z}_p$ kan konkret beskrives som kanoniske *p-adiske uttrykk* på formen

$$n = (a_0, a_1, \dots)_p = \sum_{j=0}^{\infty} a_j p^j$$

med $0 \leq a_j < p$ som er helt analoge med desimalutviklingen av de reelle tallene. Det er like lett å regne med p-adiske utviklinger som med desimalutviklinger, for algoritmene for addisjon, subtraksjon, multiplikasjon og divisjon for desimalutviklinger kan overføres direkte til p-adiske utviklinger med ubetydelige endringer.

For å illustrere nytten av p-adiske tall skal vi vise hvordan de brukes til å løse ligninger på formen

$$f(x) \equiv 0 \pmod{m}$$

for alle tall m og heltallspolynomer $f(x)$. Slike ligninger forekommer overalt i matematikken og dens anvendelser. Vi påminner om at vi bruker Gauss' (1777–1853) geniale notasjon $n \equiv l \pmod{m}$ for å uttrykke at m deler $n - l$, og at en løsning av ligningen $f(x) \equiv 0 \pmod{m}$ er et heltall n slik at $f(n)$ er delbar med m. For eksempel er tallene $1, 2, 3, 4, 5, 6$ alle løsninger til ligningen

$$x^6 - 1 \equiv 0 \pmod{7}.$$

Dette er et spesialtilfelle av Fermats lille sats som sier at for alle primtall p er $1, 2, \dots, p-1$ løsninger til ligningen

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

Av den kinesiske restsatsen følger det at for å løse ligningen $f(x) \equiv 0 \pmod{m}$ så rekker det å løse ligningen

$$f(x) \equiv 0 \pmod{p^k}$$

for alle primtall p og alle positive heltall k. La oss se på ligningen

$$x^2 \equiv 2 \pmod{7^k}.$$

Det finnes et 7-adisk tall

$$\alpha = (3.12612124\cdots)_7 = 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \cdots$$

slik at $\alpha^2 = 2$ i $\mathbf{Z}_7$. Tallet α er altså en kvadratrot til 2 i $\mathbf{Z}_7$. Vi ser lett at de endelige 7-adiske utviklingene vi får ved å bryte av den uendelige 7-adiske utviklingen til α gir løsninger som kommer stadig nærmere tallet 2. Det vil si

$$3^2 \equiv 2 \pmod{7}, \quad (3+7)^2 \equiv 2 \pmod{7^2}, \quad (3+7+2\cdot 7^2)^2 \equiv 2 \pmod{7^3},$$
$$(3+7+2\cdot 7^2+6\cdot 7^3)^2 \equiv 2 \pmod{7^4}$$

og så videre. Med andre ord, vi har

$$|3^2-2|_7 \le 1/7, \quad |(3+7)^2-2|_7 \le 1/7^2, \quad |(3+7+2\cdot 7^2)^2-2|_7 \le 1/7^3,$$
$$|(3+7+2\cdot 7^2+6\cdot 7^3)^2-2|_7 \le 1/7^4, \quad \dots.$$

Hvis vi kjente hele den 7-adiske utviklingen til α ville vi dermed ha løst alle kongruensene $x^2 \equiv 2 \pmod{7^k}$, men vi kan like lite kjenne hele den 7-adiske utviklingen til α i $\mathbf{Z}_7$ som vi kan kjenne hele desimalutviklingen til $\sqrt{2}$ i $\mathbf{R}$.

Hensels lemma. Det finnes et enkelt og hendig kriterium, kalt Hensels lemma, som garanterer at ligningene $f(x) \equiv 0 \pmod{p^k}$ har en løsning for alle k:

Anta at vi har et heltall a_0 slik at $f(a_0) \equiv 0 \pmod p$ og $f'(a_0) \not\equiv 0 \pmod p$. Da finnes et entydig p-adisk tall $\alpha = a_0+a_1p+\cdots$ med $0 \le a_i < p$ i $\mathbf{Z}_p$ slik at $f(\alpha) = 0$ i $\mathbf{Z}_p$. Ekvivalent, vil

$$f(a_0 + a_1p + \cdots + a_mp^m) \equiv 0 \pmod{p^{m+1}} \quad \textit{for} \quad m = 0, 1, \dots.$$

Bevis. Vi bruker induksjon etter m. For $m = 0$ er lemmaet forutsetningen $f(a_0) \equiv 0 \pmod p$. Anta at vi har vist at den siste ligningen i lemmaet holder for $m-1$, det vil si, vi har $f(a_0 + a_1p + \cdots + a_{m-1}p^{m-1}) = cp^m$ og velg et vilkårlig tall a_m som vi vil bestemme. Taylors formel, som er triviell for polynomer, sier at for alle polynomer $g(t)$ med heltallskoeffisienter vil

$$g(a+h) = g(a) + hg'(a) + h^2e(h)$$

der $e(t)$ er et polynom med heltallskoeffisienter. Bruker vi først Taylors formel på $f'(t)$ med $a = a_0$ og $h = a_1p + a_2p^2 + \cdots + a_mp^m$ får vi

$$f'(a_0 + a_1p + \cdots + a_mp^m) \equiv f'(a_0) \pmod p,$$

og bruker vi den på $f(t)$ med $a = a_0 + a_1p + \cdots + a_{m-1}p^{m-1}$ og $h = a_mp^m$ får vi

$$f(a + a_mp^m) \equiv f(a) + a_mp^m f'(a) \equiv p^m\big(c + a_mf'(a_0)\big) \pmod{p^{m+1}}.$$

Ettersom $f'(a_0) \not\equiv 0 \pmod p$ ved antagelsen finnes det et entydig tall a_m slik at $0 \le a_m < p$ og $c + a_mf'(a_0) \equiv 0 \pmod p$. For dette tallet vil

$$f(a_0 + a_1p + \cdots + a_mp^m) \equiv f(a + a_mp^m) \equiv 0 \pmod{p^{m+1}},$$

og vi har vist lemmaet.

Merk. Betingelsen $f'(a_0) \not\equiv 0 \pmod p$ må være oppfylt for at vi skal være sikre på at Hensels lemma holder. For eksempel vil ligningen $x^2 \equiv 2 \pmod{2^k}$ ha løsningen $x = 0$ for $k = 1$, men ingen løsning for $k = 2$ fordi $0^2 - 2 \equiv 2 \pmod 4$, $1^2 - 2 \equiv 3 \pmod 4$, $2^2 = 2 \equiv 2 \pmod 4$ og $3^2-2 \equiv 3 \pmod 4$. I dette tilfellet er den deriverte av polynomet $x^2 - 2$ lik $2x$ som er identisk med null modulo 2.

Newtons metode. For å finne en løsning til kongruensene $f(x) \equiv 0 \pmod{p^k}$ for store k er det nok å finne tilstrekkelig gode rasjonale tilnærminger a til α i $\mathbf{Q}_7$.

Grunnen til dette er at $|\alpha - a|_7$ er liten hvis og bare hvis differensen $\alpha - a$ er delelig med en høy potens av 7. Vi trenger altså en effektiv metode for å finne rasjonale tilnærminger til en løsning til likningen $f(x) = x^2 - 2 = 0$ i $\mathbf{Q}_7$. Newtons metode egner seg utmerket til formålet. Vi setter opp iterasjonen

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} = \frac{1}{2}\Big(a_n + \frac{2}{a_n}\Big)$$

og starter den med et rasjonalt tall a_1 som ligger nær α i $\mathbf{Q}_7$. Vi kan for eksempel velge $a_1 = 3$, for dette viser seg å være nær nok til at Newton-iterasjonen konvergerer til α. I så fall får vi tilnærmingene

$$a_2 = 11/6 = (3.11111111...)_7$$

som har to korrekte 7-adiske siffer, og

$$a_3 = 193/132 = (3.12603325...)_7$$

som har fire korrekte siffer. Akkurat som når vi bruker Newtons metode i $\mathbf{R}$, kan vi regne med en dobling av antall korrekte siffer i hvert steg hvis startpunktet er nær nok til roten. Så dette er en svært effektiv algoritme for å løse $f(x) \equiv 0 \pmod{p^k}$ for store k.

Det er interessant å observere at den samme følgen $a_1 = 3$, $a_2 = 11/6$, $a_3 = 193/132, \ldots$ av rasjonale tall konvergerer til to forskjellige kvadratrøtter til 2, den ene i $\mathbf{R}$ og den andre i $\mathbf{Q}_7$. Men de to konvergensbegrepene er svært forskjellige. Dette sees for eksempel ved at følgen divergerer i $\mathbf{Q}_5$, for kongruensen $x^2 \equiv 2 \pmod 5$ har ingen løsning, og dermed kan ikke 2 ha noen kvadratrot i $\mathbf{Q}_5$.

En «naiv» anvendelse av matematikken

Vi skal i denne seksjonen illustrere hva vi mener med *banale* anvendelser av matematikken. Det vil si anvendelser som bare er omformuleringer av matematiske begreper i et dagligdags språk. Eksemplet er basert på et resultat av matematikeren P. Hall (1904–1982) som er vakkert nok, og anvendelsen er elegant. Tolkningen av setningen er imidlertid hårreisende, og anvendelsen har mer karakteren av lek eller spill enn som en påtrengende praktisk oppgave. For å markere sambandet med spill ber vi leseren tenke litt over følgende kortproblem:

Et kortproblem. Del opp en kortstokk i 13 bunter med 4 kort i hver. Vis at man kan plukke ut 13 kort av ulike valører 1, 2, ..., 10, *knekt, dronning, konge*, ett fra hver bunt.

Bemerkning. Merk først at løsningen ikke er så enkel som man først kan tro. Man kan ikke bare trekke et ess fra en bunke som har et ess i seg, deretter en toer fra en bunke som har en toer, og så videre. Om for eksempel den først bunken besto av valørene $1, 3, 3, 3$ og den andre av valørene $2, 3, 4, 5$, og vi trekker et ess fra den første bunken og en toer fra den andre er det klart at det er umulig å trekke en

treer fra noen annen bunke ettersom alle treerne befant seg i den første og andre bunken.

Ettersom kortproblemet er så enkelt kan vi ikke vente at det skal gi opphav til interessant matematikk, og det finnes selvsagt mange løsninger. Vi skal presentere en elegant løsning som følger av følgende vakre resultat:

Halls setning. *La $A_1, A_2, \ldots, A_n$ være mengder. Anta at unionen av hvert utvalg av r av disse mengdene inneholder minst r elementer for alle $r \leq n$. Da kan vi finne n ulike elementer, en fra hver av de n mengdene.*

Løsning av kortproblemet. For å se hvordan Halls setning løser kortproblemet tilordner vi til hver av de 13 buntene mengden av de 1, 2, 3 eller 4 ulike valører som forekommer for kortene i bunten. Vi får da 13 undermengder $A_1, A_2, \ldots, A_{13}$ av valørene $1, 2, \ldots, 10$, *knekt, dame, konge*, der hver av mengdene $A_1, A_2, \ldots, A_{13}$ består av $1, 2, 3$ eller 4 elementer. For eksempel om buntene ser ut som

bunt 1	bunt 2	$\cdots$	bunt 12	bunt 13
5	1	$\cdots$	4	5
6	4	$\cdots$	4	5
7	knekt	$\cdots$	4	dame
10	knekt	$\cdots$	7	dame

så vil

$$A_1 = \{5, 6, 7, 10\}, A_2 = \{1, 4, \text{knekt}\}, A_{12} = \{4, 7\}, A_{13} = \{5, \text{dame}\}.$$

I hvert utvalg $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ av k mengder blant $A_1, A_2, \ldots, A_{13}$ forekommer det minst k ulike valører ettersom kortbuntene nummer $i_1, i_2, \ldots, i_k$ tilsammen inneholder $4k$ kort. Ved Halls resultat finnes det derfor et utvalg av 13 ulike elementer, en fra hver av mengdene A_1, A_2, $\ldots$, A_{13}. Med andre ord har vi funnet 13 ulike valører, en fra hver av de 13 buntene.

Bemerkning. For å illustrere hvor useriøse anvendelser av matematikk kan være vil vi nevne at Halls setning ofte kalles *Halls ekteskapssetning*. Dette er fordi vi kan tolke setningen som at vi har n kvinner med hver sin liste $A_1, A_2, \ldots, A_n$ over menn som de kan tenke seg å gifte seg med. Om vi antar at listene til hvert utvalg av r kvinner inneholder minst r ulike menn for $r \leq n$, hvilket selvsagt er et nødvendig krav for at det skal være mulig å finne en mann til alle, så er det mulig å gifte hver av kvinnene med en mann på sin liste. Man skal lete lenge etter en så urealistisk og politisk ukorrekt situasjon, og det er plagsomt at det finnes akademikere som tar slike «anvendelser» alvorlig.

To bevis for Halls setning. For å illustrere hvor lite forkunnskaper som er nødvendig for å bedrive denne formen av matematikk gir vi to bevis for Halls setning. Det første beviset er ikke *konstruktivt*, det vil si, det sier at det finnes n elementer, men ikke hvordan de kan finnes. Det andre beviset viser hvordan vi kan finne elementene. Den eneste matematikken som inngår i bevisene er induksjonsresonnementer. Matematisk induksjon er egentlig et *aksiom* for de hele tallene, men vi bruker oftest induksjon som om den er et resultat av *sunn fornuft*.

Første bevis for Halls setning. Vi viser setningen ved induksjon etter n. Setningen holder klart for $n = 1$. Anta nu at setningen gjelder for $n = 1, 2, \ldots, k-1$. Vi skal vise at den da gjelder for $n = k$. Beviset er delt i to tilfeller.

Tilfelle 1. Anta at for hver $r < k$ vil unionene av hvert utvalg $A_{i_1}, A_{i_2}, \ldots, A_{i_r}$ av r mengder blant $A_1, A_2, \ldots, A_k$ inneholder minst $r+1$ elementer. Da vil A_1 inneholde minst to elementer. Velg en av disse elementene a_1. For $r < k$ vil da unionen av hvert utvalg av r mengder blant $A_1, A_2, \ldots, A_k$ inneholde minst r elementer forskjellige fra a_1. Det følger av induksjonsantagelsen at vi kan velge $k-1$ ulike elementer forskjellige fra a_1, en fra hver av mengdene $A_2, A_3, \ldots, A_k$. Disse $k-1$ elementene sammen med a_1 gir k ulike elementer fra mengdene $A_1, A_2, \ldots, A_k$, og vi har vist Halls setning i tilfelle 1.

Tilfelle 2. Anta at det finnes et $s < k$ slik at det finnes et utvalg $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ blant mengdene $A_1, A_2, \ldots, A_k$ hvis union har nøyaktig s elementer. Ettersom $s < k$ kan vi ved induksjonsantagelsen finne s ulike elementer $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$, en fra hver av mengdene A_{i_1}, A_{i_2}, $\ldots$, A_{i_s}.

La $j_1, j_2, \ldots, j_{k-s}$ være de tallene blant $1, 2, \ldots, k$ som er forskjellige fra tallene $i_1, i_2, \ldots, i_s$. Da vil unionen av hvert utvalg av r av mengdene A_{j_1}, A_{j_2}, $\ldots$, $A_{j_{k-s}}$ inneholde minst r elementer forskjellige fra $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$ når $r \leq k-s$. Dette er fordi, om det fantes et utvalg av r mengder blant $A_{j_1}, A_{j_2}, \ldots, A_{j_{k-2}}$ hvis union inneholdt færre enn r elementer, så ville dette utvalget av r mengder sammen med de s mengdene $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ inneholde færre enn $r+s$ elementer, hvilket er mot forutsetningen i setningen. Av induksjonshypotesen anvendt på A_{j_1}, A_{j_2}, $\ldots$, $A_{j_{k-s}}$ kan vi derfor finne $k-s$ ulike elementer forskjellige fra $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$, en fra hver av mengdene $A_{j_1}, A_{j_2}, \ldots, A_{j_{k-s}}$. Sammen med $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$ gir disse $k-s$ elementene k ulike elementer fra mengdene $A_1, A_2, \ldots, A_k$ og vi har vist Halls setning i tilfelle 2.

Andre bevis for Halls setning. Vi skal gi en metode som gjør følgende operasjon på elementer:

Om vi har funnet k ulike elementer $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$, en fra hver av mengdene $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, så kan vi finne en indeks i_{k+1} forskjellig fra $i_1, i_2, \ldots, i_k$, og et element $a_{i_{k+1}}$ forskjellig fra $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ slik at etter en eventuell omordning $j_1, j_2, \ldots, j_{k+1}$ av $i_1, i_2, \ldots, i_{k+1}$ så vil $a_{j_l} \in A_{i_l}$ for $l = 1, 2, \ldots, k+1$.

Bruker vi dette for $k = 1, 2, \ldots, n-1$ så følger Halls setning.

Ved å omnummerere mengdene $A_1, A_2, \ldots, A_n$ kan vi selvsagt oppnå at $i_1 = 1$, $i_2 = 2, \ldots, i_k = k$. Om det finnes et $i > k$ og et element a_i i A_i forskjellig fra $a_1, a_2, \ldots, a_k$, vil de k elementene $a_1, a_2, \ldots, a_k, a_i$ ha de egenskapene vi søker. Vi kan derfor anta at A_i er inneholdt i mengden $B = \{a_1, a_2, \ldots, a_k\}$ for $i = k+1$, $k+2$, $\ldots$, n. Sett $\sigma(0) = k+1$. Metoden består av å velge elementer $a_{\sigma(1)}, a_{\sigma(2)}, \ldots$ etter følgende regel:

Av antagelsen i setningen finnes det minst ett element i mengden $A_{\sigma(0)} = A_{k+1}$, og hvert element må være i B. Velg et slikt element $a_{\sigma(1)}$. Av antagelsen finnes det minst ett element i $A_{\sigma(0)} \cup A_{\sigma(1)}$ forskjellig fra $a_{\sigma(1)}$. Om det er mulig, så velg et av disse $a_{\sigma(2)}$ som ikke er i B og slutt prosessen. Om alle er i B så velg et vilkårlig $a_{\sigma(2)}$ av disse og fortsett. Av antagelsen finnes det minst ett element i $A_{\sigma(0)} \cup A_{\sigma(1)} \cup A_{\sigma(2)}$ som er forskjellig fra $a_{\sigma(1)}$ og $a_{\sigma(2)}$. Om det er mulig, så velg et av disse $a_{\sigma(3)}$ som ikke er i B og avslutt. Om ikke så velg et slikt element $a_{\sigma(3)}$ i B og fortsett. Ettersom B er endelig og forskjellig fra $A_1 \cup A_2 \cup \cdots \cup A_n$ så

slutter prosessen med et element $a_{\sigma(r)}$ som er inneholdt i $A_{\sigma(0)} \cup A_{\sigma(1)} \cup A_{\sigma(r-1)}$ og som ikke er i B. Vi har nå ulike elementer $a_{\sigma(0)}, a_{\sigma(1)}, \dots, a_{\sigma(r)}$ der de r første elementene er i B, der $a_{\sigma(r)}$ ikke er i B, og der $a_{\sigma(i)}$ er i $A_{\sigma(0)} \cup A_{\sigma(1)} \cup \cdots \cup A_{\sigma(i-1)}$ for $i = 1, 2, \dots, r$.

Nå endrer vi nummereringen til elementene som følger:

Velg $r_1 < r_0 = r$ slik at $a_{\sigma(r)} = a_{\sigma(r_0)}$ er i $A_{\sigma(r_1)}$, deretter velger vi $r_2 < r_1$ slik at $a_{\sigma(r_1)}$ er i $A_{\sigma(r_2)}$, og fortsetter til vi har en $0 < r_s$ slik at $a_{\sigma(r_s)}$ er i $A_{\sigma(0)} = A_{k+1}$. Elementene $a_1, a_2, \dots, a_k$ som er forskjellige fra $a_{\sigma(r_1)}, a_{\sigma(r_2)}, \dots, a_{\sigma(r)}$ endrer vi ikke numrene på. Vi har nå funnet $k+1$ ulike elementer, som ligger i $A_1, A_2, \dots, A_k, A_{k+1}$.

Som vi har sett følger Halls setning.

Latinske kvadrater. En noe mindre triviell anvendelse av Halls setning enn den vi gjorde på kortproblemet er forbundet med latinske kvadrater. Et *latinsk kvadrat* er et $n \times n$-rutenett der tallene $1, 2, \dots, n$ forekommer i hver rekke og i hver søyle. Når $n = 4$ har vi for eksempel

3	4	1	2
4	1	2	3
2	3	4	1
1	2	3	4

Det er rimelig å betrakte to latinske kvadrater som essensielt like om vi kan få det ene fra det andre ved å omordne tallene $1, 2, \dots, n$. Vi sier da at de er *ekvivalente*. Blant alle ekvivalente kvadrater finnes det opplagt nøyaktig ett hvis siste rad er $1, 2, \dots, n$.

Leonhard Euler (1707–83) initierte studiet av latinske kvadrater, og de har siden den gang fascinert matematikere på grunn av sine spennende, og iblant mystiske egenskaper. Det finnes fremdeles mange uløste problemer om latinske kvadrater.

En snedig anvendelse av Halls setning viser at det for hvert n finnes en mengde ikke ekvivalente latinske kvadrater. For å finne ikke ekvivalente latinske kvadrater rekker det å begynne med tallene $1, 2, \dots, n$ på siste rad, og fortsette i nest siste rad med en omordning av disse tallene som ikke holder noe tall fast. Det siste er nødvendig for å kunne få et latinsk kvadrat. Vi må vise at de resterende $n-2$ radene kan fylles med de resterende tallene slik at vi får et latinsk kvadrat. Ettersom vi skal vise nedenfor at antallet omordninger av tallene $1, 2, \dots, n$ som ikke holder noe tall fast vokser med $n!/e$, følger det da at det finnes en mengde ikke ekvivalente latinske kvadrater for store n.

Vi skal vise mer enn at vi kan komplettere kvadratet til et latinsk kvadrat når de to siste radene er gitt.

Setning. *Hvis hver rad i et rutenett med m rader og n søyler der $m < n$ inneholder tallene $1, 2, \dots, n$, og ingen søyle inneholder noe tall mer enn en gang, så kan rutenettet utvides til et latinsk kvadrat av orden n.*

Bevis. Det er nok å vise at vi kan utvide rutenettet med en enkelt rad. Anta at vi har fylt m rader. La A_j være de $n-m$ tallene som ikke forekommer i den j'te søylen. Om vi kan finne et utvalg $a_1, a_2, \dots, a_n$ av n ulike tall blant $1, 2, \dots, n$ med a_j i A_j

kan vi komplettere rutenettet med raden $a_1, a_2, \dots, a_n$ og dermed utvide rutenettet, som vi ville. La $A_{j_1}, A_{j_2}, \dots, A_{j_r}$ være et utvalg av mengdene $A_1, A_2, \dots, A_n$. Hvert av tallene $1, 2, \dots, n$ fremkommer nøyaktig en gang i hver av de m radene. Derfor forekommer hvert tall i nøyaktig $n - m$ av mengdene $A_1, A_2, \dots, A_n$. Det følger at hvert tall forekommer i høyst $n - m$ av mengdene $A_{j_1}, A_{j_2}, \dots, A_{j_r}$. Derfor må mengdene $A_{j_1}, A_{j_2}, \dots, A_{j_r}$ tilsammen inneholde minst $r(n-m)/(n-m) = r$ tall. Det følger derfor av Halls setning at det finnes n ulike tall $a_1, a_2, \dots, a_n$, en fra hver av mengdene $A_1, A_2, \dots, A_n$, presis som vi ønsket.

Vi skal gi to bevis for at antallet omordninger av tallene $1, 2, \dots, n$ som ikke holder noen av disse tallene fast vokser som $n!/e$. Det ene bruker et viktig resultat som kalles *inklusjon/eksklusjon* og det andre en snedig teknikk som kalles *genererende funksjoner*. Begge metodene er meget brukt i mange deler av matematikken. Metoden med genererende funksjoner gir dessuten en tiltrekkende algoritme for å beregne antallet eksakt.

Inklusjon/eksklusjon. *For hver mengde A betegner vi med $|A|$ antallet elementer i mengden. Videre lar vi n være et tall og betegner med J_k de $\binom{n}{k} = n!/k!(n-k)!$ delmengdene $\{j_1, j_2, \dots, j_k\}$ av $\{1, 2, \dots, n\}$ med k elementer. Da vil*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\{j_1, j_2, \dots, j_k\} \in J_k} |A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}|.$$

Bevis. For å vise formelen fikserer vi et element a som ligger i $A_1 \cup A_2 \cup \cdots \cup A_n$. Dette elementet gir et bidrag på 1 til venstre side av formelen. For å vise at det bidrar med 1 også til høyre side antar vi at a er inneholdt i mengdene $A_{i_1}, A_{i_2}, \dots, A_{i_l}$, men ikke i noen av de andre mengdene A_i. Da vil a være i like mange av snittene $A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}$ som vi kan velge ulike mengder $\{j_1, j_2, \dots, j_k\}$ blant $\{i_1, i_2, \dots, i_l\}$, det vil si, på $\binom{l}{k}$ måter. Derfor gir a et bidrag på

$$\sum_{k=1}^{l} (-1)^{k+1} \binom{l}{k} = -\left[-\binom{l}{1} + \binom{l}{2} + \cdots + (-1)^l \binom{l}{l} \right] = -\big((1-1)^l - 1\big) = 1$$

til summen til høyre. Vi har vist inklusjon/eksklusjonsformelen.

Vi bruker inklusjon/eksklusjonsformelen i tilfellet da A_i er de omordningene av tallene $1, 2, \dots, n$ som fikserer tallet i. Da består $A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}$ av de $(n-k)!$ omordningene som holder tallene $j_1, j_2, \dots, j_k$ fast, det vil si $|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}| = (n-k)!$. Derfor vil

$$\sum_{\{j_1, j_2, \dots, j_k\} \in J_k} |A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}| = (n-k)! \sum_{\{j_1, j_2, \dots, j_k\} \in J_k} 1 = (n-k)! \binom{n}{k} = \frac{n!}{k!}.$$

Ved inklusjon/eksklusjonsformelen får vi derfor

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!} = n! \Big(\frac{1}{1!} - \frac{1}{2!} + \cdots + \frac{(-1)^{n+1}}{n!} \Big).$$

Men fra analysen vet vi at $e^x = 1 + x/1! + x^2/2! + \cdots$. Setter vi $x = -1$ i denne formelen for e^x ser vi at summen $1/1! - 1/2! + \cdots + (-1)^{n+1}1/n!$ ligger veldig nære $1 - e^{-1}$ når n er stor. Derfor ligger tallet $|A_1 \cup A_2 \cup \cdots \cup A_n|$ nær $n!(1 - e^{-1})$.

Vi er interessert i antallet omordninger av tallene $1, 2, \ldots, n$ som ikke holder noen av disse tallene fast, det vil si, vi vil vite hvor mange omordninger som ikke er i mengden $A_1 \cup A_2 \cup \cdots \cup A_n$. Det er derfor omtrent $n! - n!(1 - e^{-1}) = n!/e$ slike omordninger, hvilket vi ville vise.

Genererende funksjoner. Vi betegner med c_r antallet omordninger av r elementer som ikke holder noen av disse r elementene fast. Hver permutasjon av de n elementene $0, 1, \ldots, n$ holder nøyaktig $n - r$ elementer fast, der r kan være $0, 1, \ldots, n$. For å finne alle omordninger av $1, 2, \ldots, n$ merker vi at det finnes $\binom{n}{n-r}$ muligheter for å velge de $n - r$ elementene som holdes fast. For hvert slikt valg må vi omordne de r resterende elementene slik at de ikke holder noe element fast, det vil si, de resterende elementene kan omordnes på c_r måter. Tilsammen får vi at antallet omordninger av $1, 2, \ldots, n$ kan uttrykkes som

$$n! = \sum_{r=0}^{n} \binom{n}{n-r} c_r,$$

eller ekvivalent

$$1 = \sum_{r=0}^{n} \frac{c_r}{(n-r)!r!}.$$

Vi definerer nå en *genererende funksjon*

$$f(z) = \sum_{r=0}^{\infty} \frac{c_r z^r}{r!}.$$

Da vil

$$e^z f(z) = \sum_{q=0}^{\infty} \frac{z^q}{q!} \sum_{r=0}^{\infty} \frac{c_r z^r}{r!} = \sum_{n=0}^{\infty} \sum_{r=0}^{n} \frac{c_r}{(n-r)!r!} z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}.$$

For å bestemme koeffisientene c_n rekker det derfor å regne ut koeffisientene til z^n på høyresiden i uttrykket

$$f(z) = \frac{e^{-z}}{1-z}.$$

Selvsagt finner man også lett den tilnærmede formelen for c_n som er gitt ovenfor.

Hatteproblemet. For enda en gang å vise hvor naive forkledningene av matematiske resultater i såkalt *praktiske termer* kan være vil vi nevne at problemet med å finne antallet c_n iblandt kalles *hatteproblemet*. Dette fordi, om n personer leverer inn sine hatter i en garderobe og personene glemmer nummerlappene, så er $c_n/n!$ sannsynligheten for at ingen får tilbake riktig hatt. Jeg tror dette viser hvor seriøs og nyttig den så kalte «diskrete matematikken» er. Desverre er lærebøkene på skoler og universiteter fulle av slik svindel.

Appendiks A. AMS-klassifikasjonen

00 General
01 History and biography
03 Mathematical logic
05 Combinatorics
06 Order, lattices, ordered algebraic structures
08 General algebraic systems
12 Field theory and polynomials
13 Commutative rings and algebras
14 Algebraic geometry
15 Linear and multilinear algebra; matrix theory
16 Associative rings and algebras
17 Nonassociative rings and algebras
18 Category theory, homological algebra
19 K-theory
20 Group theory and generalizations
22 Topological groups, Lie groups
26 Real functions
28 Measure and integration
30 Functions of a complex variable
31 Potential theory
32 Several complex variables and analytic spaces
33 Special functions
34 Ordinary differential equations
35 Partial differential equations
37 Dynamical systems and ergodic theory
39 Finite differences and functional equations
40 Sequences, series, summability
41 Approximations and expansions
42 Fourier analysis
43 Abstract harmonic analysis
44 Integral transforms, operational calculus
45 Integral equations
46 Functional analysis
47 Operator theory
49 Calculus of variations and optimal control
51 Geometry
52 Convex and discrete geometry
53 Differential geometry
54 General topology
55 Algebraic topology
57 Manifolds and cell complexes
58 Global analysis, analysis on manifolds
60 Probability theory and stochastic processes
62 Statistics
65 Numerical analysis
68 Computer science

70 Mechanics of particles and systems
73 Mechanics of deformable solids
76 Fluid mechanics
78 Optics, electromagnetic theory
80 Classical thermodynamics, heat transfer
81 Quantum Theory
82 Statistical mechanics, structure of matter
83 Relativity and gravitational theory
85 Astronomy and astrophysics
86 Geophysics
90 Economics, operations research, programming
91 Game theory, economics, social and behavioral sciences
92 Biology and other natural sciences
93 Systems theory; control
94 Information and communication, circuits
97 Mathematics education

Appendiks B. AMS-klassifikasjonen av Algebraisk geometri

14–XX Algebraic geometry

14Axx Foundations
14Bxx Local theory
14Cxx Cycles and subschemes
14Dxx Families, fibrations
14Exx Birational Geometry
14Fxx (Co)homology theory [See also 13Dxx]
14Gxx Arithmetic problems. Diophantine geometry [See also 11Dxx, 11Gxx]
14Hxx Curves
14Jxx Surfaces and higher-dimensional varieties
[For analytic theory, see 32Jxx]
14Kxx Abelian varieties and schemes
14Lxx Algebraic Groups [For linear algebraic groups, see 20Gxx;
for Lie algebras, see 17B45]
14Mxx Special varieties
14Nxx Projective and enumerative geometry
14Pxx Real algebraic and real analytic geometry
14Qxx Computational aspects in algebraic geometry
[See also 12Y05, 13Pxx, 68W30]
14Rxx Affine Geometry

Appendiks C. AMS-klassifikasjonen av 14Hxx, kurver

14Hxx Curves

14H05 Algebraic functions; function fields [See also 11R58]
14H10 Families, moduli (algebraic)
14H15 Families, moduli (analytic) [See also 30F10, 32Gxx]
14H20 Singularities, local rings [See also 13Hxx, 14B05]
14H25 Arithmetic ground fields [See also 11Dxx, 11G05, 14Gxx]
14H30 Coverings, fundamental group [See also 14E20, 14F35]
14H37 Automorphisms
14H40 Jacobians, Prym varieties [See also 32G20]
14H42 Theta functions; Schottky problem [See also 14K25, 32G20]
14H45 Special curves and curves of low genus
14H50 Plane and space curves
14H51 Special divisors (gonality, Brill–Noether theory)
14H52 Elliptic curves [See also 11G05, 11G07, 14Kxx]
14H55 Riemann surfaces; Weierstrass points; gap sequences [See also 30Fxx]
14H60 Vector bundles on curves and their moduli [See also 14D20, 14F05]
14H70 Relationships with integrable systems
14H81 Relationships with physics
14H99 None of the above, but in this section

Bibliografi

[1] Ian Andersson, *A first course in Combinatorial Mathematics*. (Second edition.) Clarendon Press, Oxford 2000.

[2] *AMS subject classification 2000*. American Mathematical Society, Providence, RI, 2000.

[3] Simon Singh, *Fermats gåta*. Norstedts, Stockholm 1998.

[4] James Tanton, *Solve This*. The Mathematical Association of America, Washington, DC, 2001. ISBN 0-88385-717-0.