EXAMENSARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Matematiska bevis

Beskrivning av olika bevismetoder och hur de används

av

Åsa Wall Månsson

2005 - No 2

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 10691 STOCKHOLM

Matematiska bevis

Beskrivning av olika bevismetoder och hur de används

Åsa Wall Månsson

Examensarbete i matematik 20 poäng

Handledare: Christian Gottlieb

2005

Innehåll

Kapitel 1

Inledning

*"**Det dunkelt sagda är det dunkelt tänkta**"*
Essaias Tegnér, 1782-1846, författare och biskop

1.1 Bakgrund

I läroböckerna inom matematik för gymnasiet förekommer ganska få bevis, och det verkar över huvud taget som om gymnaisekurserna inte lägger så mycket tid på bevis och bevishantering. I en undersökning vid Stockholms Universitet uppgav endast cirka 30 procent av de nya studenterna vid institutionen för Matematik att de haft möjlighet att öva både muntlig och skriftlig bevisning under gymnasietiden [8].

Bevis blir en viktig del av kurserna på påbyggnads- och fördjupningsnivåerna. Syftet med mitt examensarbete är därför att övergripande beskriva hur man kan arbeta med bevis, dvs hur man kan läsa och konstruera bevis.

Efter inledningen följer ett kapitel där jag berättar om två olika sätt att tänka när man ska arbeta med matematiska bevis.

Därefter följer ett kapitel som beskriver de vanligaste bevismetoderna, med ett flertal enklare eller mer avancerade exempel. Kapitlet avslutas med ett avsnitt om olika hjälptekniker för att underlätta bearbetandet av ett bevisproblem.

I ett eget kapitel beskrivs det jag valt att kalla "delproblem". Här behandlar jag tekniker för att bevisa satser med olika kvantifierare och hur man bevisar entydighet.

Examensarbetet avslutas med ett kapitel som innehåller ett antal kommenterade bevis.

Eftersom bevis bygger på logik har jag även valt att ta med en bilaga

som ger mycket grundläggande information om logik. Denna bilaga hör speciellt ihop med avsnittet om indirekta bevis och behöver bara läsas av den som inte är bekant med logikens grunder.

Målgruppen för uppsatsen är främst de studenter som kanske för första gången ska börja arbeta med bevis på ett mer strukturerat sätt (exempelvis på kurserna Analys 3 och Analys 4 vid Stockholms Universitet). Andra tänkbara läsare är t.ex matematiklärare på gymnasiet.

1.2 Varför behövs bevis?

För att **motbevisa** en matematisk sats krävs endast ett enda motexempel, så har man visat att satsen inte alltid gäller.

Men för att **bevisa** en sats duger det inte att ge ett exempel på då satsen gäller. Vi måste ge ett matematiskt bevis för att satsen alltid gäller då vissa förutsättningar är uppfyllda (alternativt krävs inga förutsättningar, utan satsen gäller alltid).

Beviset fyller flera funktioner;

Verifiering; Först och främst kan vi genom beviset verifiera att en given sats är sann, dvs ”att påståendet i satsen är en logisk konsekvens av förutsättningarna i denna” [9].

Byggstenar; Mängden av bevisade satser fungerar som byggstenar som kan användas för att bygga vidare på, utan att behöva uppfinna hjulet på nytt varje gång vi behöver använda en matematisk sats.

Förutsättningar; I satsens antagande anges under vilka förutsättningar påståendet gäller. I satsen anges tillräckliga villkor för att påståendet ska vara sant. Ibland anges även nödvändiga villkor (se Bilaga 2 för mer detaljer). Observera dock att satsen oftast inte säger något om vad som händer om förutsättningarna bara delvis är uppfyllda, eller inte alls är uppfyllda.

Generalisering; Vi kan genom beviset se att ett påstående i en sats inte bara är sant i ett givet specialfall, utan att det är sant för alla tänkbara fall - givet att förutsättningarna är uppfyllda.

Undervisning; När vi förstår beviset, ökar det vår allmänna förståelse för matematikens spelregler och för sambanden mellan olika begrepp. Många satser är på formen ”om ...- så ...”, dvs att satsen klargör ett samband som gäller.

Utveckling; Beviset "tvingar" matematikern att skärpa sina tankar så att beviset kan förstås och tolkas av andra, vilket leder till att matematikerns egen förståelse också ökar.

Jag vill ge ett mycket banalt exempel på hur ett bevis kan byggas upp.

SATS:
Summan av två godtyckliga udda tal är jämn.

BEVIS:
Hur kan vi veta att satsen är sann? Vi kan prova oss fram och se att $1+3=4$, som är jämnt. Eller $5+9=14$ som är jämnt. Eller $1231+5679=6910$, som är jämnt. Men vi kan inte testa oss igenom hela mängden av udda tal, eftersom den är oändligt stor. **Vi måste komma på vilka inneboende egenskaper som gör att summan av två udda tal är jämn**, om vi ska våga tro på att det alltid är sant.

För att göra det måste vi börja med att förstå problemet. Till att börja med; vad innebär det att ett heltal är jämnt? Jo, det betyder egentligen att talet är jämnt delbart med 2. Och vad innebär det att ett heltal är udda? Jo, det betyder att om man delar ett udda tal med 2, får man alltid en rest 1. Ett udda tal kan alltså skrivas på formen $(2n+1)$ där n är ett heltal vilket som helst. Talet n är här ett hjälptal för att kunna skriva ett udda tal på en annan form.

När vi adderar två udda heltal kan vi skriva det som:

$$(2n+1)+(2m+1)=2n+2m+2=2(n+m+1)$$

Här är både m och n två hjälptal i form av godtyckliga heltal. När summan skrivs på formen $2(n+m+1)$ är det ganska uppenbart att den är jämnt delbar med 2, och vi kan nog våga tro på att oavsett vilka udda tal vi adderar (dvs oavsett vilka heltal vi sätter in på n:s och m:s platser) så kommer resultatet alltid att vara jämnt delbart med 2. Alltså är satsen visad.

Ovanstående bevis är ett exempel på att man helt och hållet utgår från sitt antagande (att vi har två godtyckliga udda tal) för att bevisa sitt påstående (att summan av två sådana tal är jämn). I den fortsatta texten kommer vi att gå igenom många olika satser och bevis, där man både utgår från det antagna och det påstådda för att genomföra beviset.

Kapitel 2

Att angripa problemet

"Många ting, som inte kan övervinnas när de står tillsammans, ger efter, när vi tar itu med dem ett och ett."

Plutarchos, 46 - 120 e.Kr, grekisk författare och präst

2.1 Inledning

Det första problemet vi ställs inför när vi ska bevisa en sats är att se vad som är **det antagna** och vad som är **det påstådda** i satsen. Många satser/utsagor är på formen "Om A, så B". I dessa fall är A det antagna och B det påstådda. Att A är det antagna innebär att i vårt bevis kan vi utgå från att A är sant, dvs vi behöver inte bevisa att A gäller. Beviset ska istället gå ut på att visa att om vi har A så har vi också B.

Vi måste komma på ett sätt att (stegvis) få dessa två att närma sig varandra, så att vi får en obruten kedja av antaganden och påståenden som leder oss liksom en bro från vårt första antagande till det slutliga påståendet. Denna bro kan byggas från båda håll; dvs vi kan utgå från det antagna för att nå det påstådda, eller tvärt om. Detta är principen i alla matematiska bevis.

I mitt examensarbete har jag tagit stort intryck av två matematiker: George Polya och Daniel Solow. Här nedan beskrivs några av deras idéer angående hur man kan arbeta med matematiska bevis. Både Polyas och Solows metoder behandlar hur man kan **tänka** för att lyckas finna ett sätt att bevisa en sats. Även om deras metoder är olika, så syftar de båda till att närma antagandet och påståendet till varandra.

Båda metoderna har sina fördelar och det är mest en smaksak vilken man föredrar - men man har stor nytta av att känna till båda metoderna!

2.2 Polyas problemlösning

George Polya (1887-1985), som var professor i matematik vid Stanforduniversitetet i USA, har skrivit "*Problemlösning. En handbok i rationellt tänkande.*" [11]. Där beskriver han ett konstruktivt sätt att angripa dels så kallade sökproblem (dvs problem där man ska söka efter en okänd komponent) och dels bevisproblem. I mitt examensarbete har jag begränsat mig till att endast visa hans sätt att angripa bevisproblem.

Polyas metod går ut på att med hjälp av olika frågor bena upp en sats för att kunna vrida och vända på den, och för att lättare kunna se från vilket håll man ska gripa sig an att bevisa satsen.

"Målet med ett 'bevisproblem' är att fullt bindande visa att ett visst klart formulerat påstående är sant eller också att det är falskt. Vi skall svara på frågan: Är detta påstående sant eller falskt? Och svaret måste vara bindande antingen vi visar att påståendet är sant eller falskt. [...] Om ett 'bevisproblem' är ett matematiskt problem av det vanliga slaget utgörs dess huvuddelar av *antagandet* och *påståendet* som skall bevisas eller vederläggas. [...] Om man vill lösa ett 'bevisproblem' måste man veta, och veta mycket exakt, vad som är dess huvuddelar; antagandet och påståendet." ([11], s. 183-185).

Polyas metod innebär att man delar in problemlösningen i fyra faser;

- förstå problemet
- gör upp en plan
- genomför planen
- se tillbaka

Till varje fas hör ett antal frågor som hjälper till att ringa in problemet och som därigenom förhoppningsvis leder till en lösning. (Nedanstående är en sammanställning från Polyas bok, s. 16-17 samt s. 185 med vissa omarbetningar av mig för att anpassa till situationen med bevisproblem.)

1. FÖRSTÅ PROBLEMET
För det första. Du måste förstå problemet.

Frågor under "Förstå problemet":
Vad har vi för antagande? Vad har vi för påstående? Hur lyder antagandet? Vilka förutsättningar måste vara uppfyllda för att antagandet ska gälla? Är dessa förutsättningar uppfyllda? Är antagandet tillräckligt för

att påståendet ska gälla? Eller är det otillräckligt? Eller överflödigt? Eller motsägelsefullt?

Rita en figur, om möjligt. Inför lämpliga beteckningar.

Dela upp antagandets olika delar. Kan du skriva ner dem?

2. GÖR UPP EN PLAN

För det andra. Sök sambandet mellan antagandet och påståendet. Du kan bli tvungen att hitta på en hjälpsats[1] ifall du inte kan finna sambandet direkt. Slutligen ska du komma fram till en plan för lösningen.

Frågor under "Gör upp en plan":

Har du sett detta förut? Har du sett samma problem i en något annorlunda form?

Känner du till något närbesläktat problem? Känner du till någon sats som skulle kunna användas?

Betrakta påståendet! Försök finna en känd sats med samma eller liknande påstående.

Gå tillbaka till definitionerna. Kan du använda definitionerna för antagandet eller påståendet för att närma påståendet till antagandet?

Behåll endast en del av antagandet, förkasta den andra delen. Gäller påståendet fortfarande? *Skulle du kunna härleda någonting användbart ur antagandet? Kan du komma på något annat antagande ur vilket du lätt skulle kunna härleda påståendet? Skulle du kunna ändra på antagandet eller på påståendet, eller på bådadera om nödvändigt, så att det nya antagandet ligger närmare det nya påståendet?*

Använde du hela antagandet? Har du tagit hänsyn till alla de förutsättningar som måste vara uppfyllda för att antagandet ska gälla?

3. GENOMFÖR PLANEN

För det tredje. Genomför planen.

Frågor under "Genomför planen":

När du genomför den plan som utformats för lösningen, så kontrollera varje steg. Kan du klart se att steget är korrekt? Kan du bevisa att det är riktigt?

[1] **Hjälpsats:** Vi försöker bevisa en sats, låt oss kalla den A. Under arbetets gång kommer vi att förmoda att en annan sats, B, kanske är giltig. Om B vore sann skulle vi kanske kunna använda den för att bevisa A. Vi antar provisoriskt att B gäller, sparar beviset till senare och fortsätter istället att bevisa A. En sådan antagen sats B kallas **hjälpsats** till den ursprungliga givna satsen A ([11], s.140-141).

4. SE TILLBAKA
För det fjärde. Granska den funna lösningen.

Frågor under "Se tillbaka":
Kan du kontrollera resultatet? Kan du kontrollera bevisföringen?
Kan du härleda resultatet på något annat sätt? Kan du se det direkt?
Kan du använda resultatet eller metoden på något annat problem?

2.3 Solows framåt-bakåt-metod

Daniel Solow har skrivit en bok som heter "*How to read and do proofs*" [13]. I boken behandlas några olika tekniker för att skapa matematiska bevis. En av Solows grundtankar är den så kallade "**framåt-bakåt-metoden**". Med "framåt" menas att vi rör oss från antagandet mot påståendet. Med "bakåt" menas att vi rör oss i motsatt riktning; från påståendet mot antagandet.

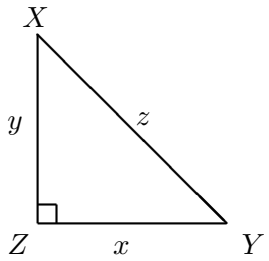
För att använda framåt-bakåt-metoden för att bevisa att "antagande A medför påstående P" börjar man med den så kallade **bakåtprocessen**. Under hela bakåtprocessen förutsätter man att antagandet A är sant. Man ställer och besvarar så kallade **nyckelfrågor**, varigenom man skapar en ny utsaga P1, med egenskapen att om P1 är sann så medför det att även P är sann. Med hjälp av nya nyckelfrågor skapas ännu en ny utsaga P2, med egenskapen att om P2 är sann så är även P1 sann och därmed även P, osv.

Man fortsätter att arbeta bakåt tills man når A (och då är beviset klart), eller tills man inte längre kan ställa eller besvara fler nyckelfrågor. I så fall fortsätter man istället med **framåtprocessen**, som innebär att man skapar en serie utsagor från det första antagandet A, med egenskapen att de alla är sanna som en konsekvens av att A antas vara sant. Målet med framåtprocessen är att få exakt samma utsaga som man fick i det sista påståendet från bakåtprocessen, och då är beviset klart. ([13], s.16)

Följande exempel är fritt hämtat från Solows bok ([13], s. 9-13), med min översättning.

PROPOSITION 1:

Om den rätvinkliga triangeln XYZ med sidor av längd x och y och hypotenusa av längd z har arean $z^2/4$, så är triangeln XYZ likbent.



ANALYS AV BEVIS

Proposition 1 innehåller antagandet (A) och påståendet (P):

A: Den rätvinkliga triangeln XYZ med sidor av längd x och y och hypotenusa av längd z har arean $z^2/4$

P: Triangeln XYZ är likbent

Med framåt-bakåt-metoden börjar man alltid med att arbeta bakåt. I bakåtprocessen utgår man hela tiden från att antagandet A är riktigt. Syftet med bakåtprocessen är att komma så nära antagandet som möjligt, kanske till och med nå ända fram till antagandet.

Bakåtprocessen börjar med att man frågar sig "**Hur eller när kan jag dra slutsatsen att påstående P är sant?**" Detta är vår **nyckelfråga**, och den ska ställas på en abstrakt nivå. I vårt fall lyder en korrekt fråga: "Hur eller när kan jag dra slutsatsen att en godtycklig triangel är likbent?". Vi begränsar oss alltså inte till detta specifika exempel, utan vi lyfter blicken och studerar trianglar i allmänhet.

Nästa steg i processen är nu att besvara nyckelfrågan. Detta görs dels på en abstrakt nivå och dels på en konkret nivå. I vårt fall får vi:

Abstrakt: För att visa att en triangel är likbent, visa att två av dess sidor har samma längd.

Konkret: För att visa att XYZ är likbent, visa att $x = y$. (Eftersom hypotenusan i en rätvinklig triangel alltid är längre än de två sidorna inser vi att det är just sidorna x och y som måste vara lika långa om triangeln ska kunna vara likbent.)

Genom att besvara vår nyckelfråga har vi således fått en ny utsaga:

P1: $x = y$

Om vi kan visa att $x = y$ så är triangeln XYZ likbent, dvs om vi kan visa att P1 gäller så kan vi dra slutsatsen att även P gäller.

En lämplig nyckelfråga kan nu vara: "Hur kan jag visa att två sidor i en triangel är lika?". Eller ännu mer abstrakt: "Hur kan jag visa att två reella tal är lika?".

För att besvara den första frågan skulle vi behöva veta vinklarna X och Y. Om dessa vinklar är lika så vet vi att även sidorna är lika (genom basvinkelsatsen). Tyvärr känner vi inte till vinklarna i detta fall, så vi försöker istället besvara vår andra fråga "Hur kan jag visa att två reella tal är lika?". En möjlighet är att sätta $x - y = 0$. Vi får då en ny utsaga:

P2: $x - y = 0$

Om vi kan visa att P2 är sant, så vet vi att P1 är sant och då vet vi att P är sant. Nu försöker vi besvara nästa nyckelfråga: "Hur kan jag visa att skillnaden mellan två reella tal är 0?".

Den frågan är inte lätt att svara på, så istället försöker vi arbeta oss framåt från vårt antagande. Men låt oss först summera våra resultat så här långt. Vi har funnit att:

$P2 \quad \Leftrightarrow \quad P1 \quad \Leftrightarrow \quad P$

eller:

$x - y = 0 \quad \Leftrightarrow \quad x = y \quad \Leftrightarrow \quad$ Triangeln XYZ är likbent

Eftersom vi inte kommer längre med bakåtprocessen försöker vi istället komma vidare genom framåtprocessen. Vi utgår från att vårt antagande A gäller, och därifrån försöker vi skapa en ny utsaga som vi vet gäller som ett resultat av att A gäller.

Observera att ett av problemen med framåtprocessen är att det är möjligt att producera helt meningslösa utsagor, t.ex i vårt fall att vinkel X är mindre än 90 grader. För att undvika dylika fallgropar ska man alltid **försöka jobba mot en utsaga som ligger i linje med den sista utsaga man tog fram i bakåtprocessen**. Vår sista utsaga i bakåtprocessen var:

P2: $x - y = 0$

Och vårt antagande är:

A: Den rätvinkliga triangeln XYZ med sidor av längd x och y och hypotenusa av längd z har arean $z^2/4$

Vår utsaga P2 innehåller två okända storheter: x och y. Vårt antagande A innehåller tre okända storheter: x, y samt z. Tänk om vi kunde eliminera z på något sätt?

I antagande A uttrycks triangelns area genom $z^2/4$. Ett annat uttryck för en triangels area är (basen $\times$ höjden)/2, dvs i vårt fall: $xy/2$. Vi får alltså följande likhet som vår nya utsaga:

A1: $xy/2 = z^2/4$

Genom Pythagoras sats vet vi också (eftersom XYZ är en rätvinklig triangel) att:

A2: $x^2 + y^2 = z^2$

Genom att kombinera A1 och A2 kan vi nu eliminera z; vi ersätter z^2 i A1 med $x^2 + y^2$ från A2, och vi får då:

A3: $xy/2 = (x^2 + y^2)/4$

Vi vill nu få A3 att ännu mer likna P2. Detta kan vi åstadkomma med hjälp av algebra för att förenkla uttrycket:

$$\begin{aligned} xy/2 &= (x^2 + y^2)/4 \\ &\Updownarrow \\ 2xy &= x^2 + y^2 \\ &\Updownarrow \\ x^2 - 2xy + y^2 &= 0 \end{aligned}$$

Vi får alltså en ny utsaga:

A4: $x^2 - 2xy + y^2 = 0$

Detta kan vi genast se är detsamma som:

A5: $(x - y)^2 = 0$

Genom att ta kvadratroten av båda leden kommer vi fram till det resultat vi ville, nämligen:

P2: $x - y = 0$

Vi får alltså följande kedja av samband:
$A \Leftrightarrow A1 \Leftrightarrow A2 \Leftrightarrow A3 \Leftrightarrow A4 \Leftrightarrow A5 \Leftrightarrow P2 \Leftrightarrow P1 \Leftrightarrow P$
Vi har därmed visat att $A \Rightarrow P$ och $P \Rightarrow A$.

Ovanstående omfattande bevisning kan också skrivas på en kondenserad form:

Från antagandet och formeln för arean av en rät triangel, vet vi att arean av $XYZ = xy/2 = z^2/4$. Genom Pythagoras sats är $x^2+y^2 = z^2$ och genom att ersätta z^2 med x^2+y^2 och därefter genomföra några algebraiska operationer fås att $(x-y)^2 = 0$. Alltså är $x = y$, och alltså är triangeln XYZ likbent.

Kapitel 3

Bevismetoder

"Att lära sig saker handlar om att plötsligt förstå något som man alltid förstått, men på ett nytt sätt."

Doris Lessing, brittisk författare, f. 1919

3.1 Inledning till bevismetoder

För att visa att en sats är falsk behövs bara ett motexempel - men för att visa att en sats är sann krävs ett bevis som övertygar varje kunnig läsare. Detta kan i vissa fall vara mycket enkelt, andra gånger krävs ett stort mått av kreativitet och matematisk förståelse och kunskap.

I arbetet med att skapa ett bevis pendlar man ofta mellan två frågor: "Vad vet jag?" (dvs, "Vad är mitt antagande?") och "Vad vill jag visa?" (dvs, "Vad är mitt påstående?").

Ofta är det en stor hjälp att gå tillbaka till olika definitioner för att verkligen försöka förstå vilka förutsättningar som antagandet bygger på och vilka krav som måste vara uppfyllda, som en hjälp att besvara frågan "Vad vet jag?".

Mitt examensarbete vänder sig till stor del till andra matematikstudenter, som kanske för första gången står inför problemet att "lära sig" olika bevis som sedan ska redovisas på en muntlig tentamen. Många grips av panik vid den tanken.

Min egen erfarenhet är att enda sättet att "lära sig" ett bevis är att **förstå** beviset. Hela syftet med detta examensarbete är att underlätta för andra att förstå de bevis som ingår i kurserna på påbyggnads- och fördjupningsnivåerna.

När jag skriver ”förstå” ett bevis menar jag

- att förstå den bevismetod som används och varför den fungerar;
- att förstå eventuella hjälpstorheter som införs, hur de skapas och på vilket sätt de underlättar beviset;
- att kanske till och med kunna skapa ett alternativt bevis, som använder en annan bevismetod.

I detta kapitel presenterar jag tre huvudsakliga bevismetoder:

- Direkt bevis
- Indirekt bevis (uppdelat i Motsägelsebevis och Bevis med kontrapositiv)
- Induktionsbevis

Dessutom presenteras olika hjälptekniker, dvs olika sätt att omformulera och bearbeta bevisproblemet så att det blir lättare att lösa.

Efter att ha läst igenom ett antal böcker om bevis har jag kommit fram till att ovanstående bevistyper i princip är de som finns - med ett oändligt antal variationer.

I efterföljande kapitel tar jag även upp det jag kallar delproblem, dvs metoder att bevisa satser som innehåller kvantifikatorer (”för alla” och ”det finns”) och metoder att visa entydighet (dvs visa att ett objekt är unikt). Tillsammans bör dessa två kapitel ge vissa insikter som förhoppningsvis underlättar livet för förtvivlade matematikstudenter!

*"**Ett bra bevis är ett bevis som gör oss klokare**"*
Yuri Ivanovich Manin, rysk matematiker och vetenskapsman, f. 1937

3.2 Direkt bevis

3.2.1 Inledning

Metoden med direkt bevis kan sägas vara basen för alla andra bevismetoder. I princip finns det två typer av situationer när man ska arbeta med ett direkt bevis:

1. Vi har ett påstående P.
2. Vi har en utsaga med ett villkor: Om antagande A är sant, så är påstående P också sant, dvs $A \Rightarrow P$.

Metoden med direkt bevis är skenbart enkel.

Metoden är **enkel**, därför att den är rakt på sak; utgå från det vi vet eller det vi antar och bevisa sedan att detta leder till en viss slutsats.

Det **skenbart** enkla ligger i att det finns oändligt många möjligheter att använda denna metod - beroende på hur komplex utsaga eller sats vi utgår från. Av detta skäl finns det i detta examensarbete ett speciellt avsnitt (se avsnitt 3.5) där jag går igenom några vanliga hjälptekniker man kan ha stor nytta av.

För att genomföra ett direkt bevis börjar man alltså med att utgå från det man redan vet och/eller från det som antas gälla enligt utsagan. Man kan då arbeta enligt de riktlinjer som ges av Polya eller Solow (se avsnitt 2). I båda metoderna skapar man en kedja som binder samman det antagna med det påstådda, alternativt en kedja som binder samman något vi vet (t.ex ett axiom eller en definition) med det påstådda.

En liten parentes; bevis av en utsaga med villkor, alltså bevis av utsagor av typen "Om A, så B" börjar ofta med "Låt x vara..." eller "Antag att x är...". Detta är ett sätt att indikera att vi utgår från att antagandet är sant, och det vi då ska bevisa är att i så fall är även påståendet sant.

Några viktiga steg när man arbetar med direkta bevis (hämtat från Garnier & Taylor, "100% Mathematical proof", [5], s.161) är:

1. Försök med några exempel, men kom ihåg att ett exempel inte utgör ett generellt bevis.

2. Försök att specialisera resonemanget till ett visst exempel som kan vara lättare att förstå, försök sedan generalisera till mer allmängiltiga situationer.

3. Försök komma på liknande eller analoga satser vars bevis du känner till.

4. Om utsagan är av typen $A \Rightarrow P$, dvs en utsaga med ett villkor, försök både att arbeta bakåt från påståendet och framåt från antagandet.

5. Om det passar, rita en skiss.

3.2.2 Direkt bevis; enkelt exempel

Ett ganska enkelt exempel på ett direkt bevis har jag hämtat från Daepp & Gorkin ([4], s.54), med mina omarbetningar.

SATS:
Om a, b och c är heltal sådana att a delar b och a delar c, så delar a även $b + c$.

BEVIS:
1. FÖRSTÅ PROBLEMET
Vårt **antagande** är att a, b och c är heltal, samt att a delar b och a delar c. Vårt **påstående** är att i så fall delar a även $b + c$.
Men vad betyder det att a delar b? Det betyder att om vi delar b med a så får vi ett heltal, dvs $b = am$, där m är ett heltal.

2. GÖR UPP EN PLAN
Vi vet alltså att eftersom a delar både b och c så har vi att $b = am$ och $c = an$ (där m och n är heltal). Vi vill visa att a även delar $b + c$, dvs att $b + c = ak$ (där k är ett heltal).
Vi provar att skriva om b och c enligt ovan och ser vad som händer.

3. GENOMFÖR PLANEN
$b + c = am + an = a(m + n) = ak$ (där $k = m + n$)
Eftersom både m och n är heltal, så är även deras summa ett heltal. Alltså har vi visat att $b + c = ak$, dvs a delar $b + c$.

4. SE TILLBAKA
I detta bevis har vi dels gått tillbaka till definitionen av "a delar b" och dels använt de antaganden som var givna för att komma fram till den önskade slutsatsen. Som synes har vi inte behövt använda några knep eller "konstigheter" för att genomföra beviset.

Om man vill kan det vara lärorikt att gå vidare och ställa sig några följdfrågor utifrån detta bevis, exempelvis:

Om vi har att a delar b och b delar c, kan vi då fortfarande dra slutsatsen att a delar $b + c$?

Om a delar b och a delar c, är det då sant att a delar $b - c$?

Detta är ett mycket bra sätt att successivt öka sin matematiska förståelse.

3.2.3 Direkt bevis; avancerat exempel

Nu tar vi ett lite mer avancerat exempel på ett direkt bevis, hämtat från Garnier & Taylor, med min översättning och mina omarbetningar ([5], ss.159-161).

SATS:
Låt G vara en godtycklig grupp.
För alla $x, y \in G$ gäller då att $(xy)^{-1} = y^{-1}x^{-1}$.

BEVIS:
1. FÖRSTÅ PROBLEMET
Här finns det en hel del som vi behöver förstå för att kunna bevisa denna sats. Till att börja med sägs att G är en **grupp**. Vad innebär det?

En definition av grupper finns i Beachy & Blair ([1], s.82):
"En grupp $(G, \cdot)$ är en icke-tom mängd G tillsammans med en binär operation $\cdot$ sådan att följande villkor är uppfyllda:

(G1) Slutenhet: För alla $a, b \in G$ är elementet $a \cdot b$ ett unikt definierat element i G.

(G2) Associativitet: För alla $a, b, c \in G$ gäller att $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(G3) Identitet: Det finns ett identitetselement $e \in G$ sådant att $e \cdot a = a$ och $a \cdot e = a$ för alla $a \in G$.

(G4) Inverser: För varje $a \in G$ finns ett inverst element a^{-1} sådant att $a \cdot a^{-1} = e$ och $a^{-1} \cdot a = e$."

Axiom G3 och G4 medför att enhetselementet är unikt, och att inversen är unik för varje element a. Se även avsnitt 4.1 för bevis av entydighet (att ett objekt är unikt).

En **grupp** är alltså en mängd med en **binär operation** (dvs en operation som använder två element, som kan vara lika eller olika). Dessutom

uppfyller mängden ovanstående fyra egenskaper.

Vårt **antagande** är nu att G är en grupp, och att x och y är två element i G.

Vårt **påstående** är att $(xy)^{-1} = y^{-1}x^{-1}$, dvs att inversen av produkten är lika med produkten av inverserna.

Eftersom x och y är element i G, så är även xy ett element i G, enligt axiom G1. Enligt axiom G4 är då även $(xy)^{-1}$ ett element i G, och vi har att $(xy)[(xy)^{-1}] = e$ och $[(xy)^{-1}](xy) = e$.

2. GÖR UPP EN PLAN

När det gäller grupper så är endast en binär operation definierad, nämligen multiplikation. Man kan därför inte utan vidare dividera ett tal med ett annat tal, men däremot kan man multiplicera detta tal med inversen till det andra talet (som ju är definierad i en grupp) - vilket i praktiken får samma effekt som division. Vi måste alltså använda oss av följande egenskap för inverser: $(g^{-1})g = e = g(g^{-1})$.

För att visa att ett element i en grupp är en invers till ett annat element, måste man alltså visa att deras produkt (skriven på båda sätten) är lika med enhetselementet e.

I vårt fall, för att visa att $y^{-1}x^{-1}$ är en invers till xy, måste vi visa att $(xy)(y^{-1}x^{-1}) = e$ och att $(y^{-1}x^{-1})(xy) = e$. Till vår hjälp har vi de fyra axiomen för grupper.

3. GENOMFÖR PLANEN

Vi börjar med den första ekvationen:

$(xy)(y^{-1}x^{-1}) = (xyy^{-1})x^{-1}$ [pga G2] $= (x(yy^{-1}))x^{-1}$ [pga G2]
$= (xe)x^{-1}$ [pga G4] $= xx^{-1}$ [pga G3] $= e$ [pga G4].

Den andra ekvationen visas på motsvarande sätt. Eftersom vi har visat att $(xy)(y^{-1}x^{-1}) = e$ och att $(y^{-1}x^{-1})(xy) = e$, så följer det att $y^{-1}x^{-1} = (xy)^{-1}$, V.S.B.

4. SE TILLBAKA

I detta bevis behövde vi gå tillbaka till definitionen för grupper. Med hjälp av de axiom som ingår i definitionen så gick det att bevisa satsen.

För att öka sin förståelse kan det vara intressant att ställa sig några följdfrågor, exempelvis:

Gäller det även att $(xy)^{-1} = x^{-1}y^{-1}$?

Gäller det att $(yx)^{-1} = x^{-1}y^{-1}$ *?*

"Genom att försöka med det 'omöjliga' når man högsta graden av det möjliga."

August Strindberg, 1849-1912, författare.

3.3 Indirekt bevis

3.3.1 Inledning

Ett indirekt bevis används då det av olika skäl är svårare att genomföra ett direkt bevis. Avsnittet om indirekta bevis kräver att man har grundläggande kunskaper inom logik. För den som inte har sådana kunskaper hänvisas först till Bilaga 1, innan man fortsätter läsa detta kapitel.

När man arbetar med indirekta bevis är det av vital betydelse att man kan konstruera negationer av olika antaganden och påståenden på ett korrekt sätt. I vardagligt tal tänker vi ofta på en negation som en motsats, men detta kan skapa förvirring då vi arbetar med matematiska problem.

Ta som exempel uttrycket: "Det regnar". Motsatsen till detta uppfattar vi kanske som "Solen skiner". I verkligheten bör motsatsen formuleras som: "Det regnar inte".

Det är alltså lätt att hamna vilse när man ska formulera en negation, och därför ges här först en kort genomgång av hur negationer ska konstrueras. Därefter ges en genomgång av de två typerna av indirekta bevis; motsägelsebevis och bevis med kontrapositiv.

3.3.2 Negationer

(Innehållet i detta avsnitt är delvis hämtat från Cupillari; [3], sid 25-26.)

Det kan vara svårt att skapa en korrekt negation från en utsaga, speciellt om utsagan är sammansatt eller innehåller kvantifikatorer.

Exempelvis är den sammansatta utsagan "A *eller* B" sann om minst en av A eller B är sann. För att "A *eller* B" ska vara falsk så måste därför både A och B vara falska. Detta innebär att negationen till "A *eller* B" blir "$\neg A$ *och* $\neg B$". (Observera att inom matematiken betyder "eller" samma sak som "och/eller" inom det vanliga språket. Detta kan vara förvirrande i början.)

Den sammansatta utsagan "A *och* B" är sann om både A och B är sanna samtidigt. För att "A *och* B" ska vara falsk räcker det alltså att minst en av A eller B är falsk. Negationen till "A *och* B" blir alltså "$\neg A$ *eller* $\neg B$".

Nedanstående tabell ger en sammanställning över några vanliga fall.

Ursprunglig utsaga	**Negation**
A	$\neg A$
$\neg(\neg A)$	A (två negationer i rad annulleras!)
A ***eller*** B	$\neg A$ ***och*** $\neg B$
A ***och*** B	$\neg A$ ***eller*** $\neg B$
Någon/minst en	Ingen
Ingen/ Det finns ingen	Det finns minst en
$\exists x$ (det existerar ett objekt)	$\neg\exists x$ (det existerar inte ett objekt)
Alla/Varje objekt i en mängd har en viss egenskap	Det finns minst ett objekt i mängden som **inte** har egenskapen
$\forall x, x \in M$ (för alla objekt gäller att objektet tillhör M)	$\exists x, x \notin M$ (det finns ett objekt som inte tillhör M)

3.3.3 Motsägelsebevis

Den första typen av indirekta bevis är **motsägelsebevis**. Motsägelsebevis bygger på att sanningstabellerna (se Bilaga 1) för påståendet "$A \Rightarrow B$" och "A *och* $\neg$ B" är varandras motsatser, dvs när det ena är sant är det andra falskt och vice versa.

Ett motsägelsebevis inleds med att man antar att man har "A *och* $\neg$ B". Om detta antagande leder till en motsägelse eller en orimlighet, så har man visat att antagandet är falskt och då är samtidigt utsagan $A \Rightarrow B$ sann, eftersom dessa två utsagor har exakt motsatta sanningstabeller.

Tilläggas bör att vissa matematiker inte accepterar ett motsägelsebevis, men på Matematiska institutionen vid Stockholms Universitet används det ofta i undervisningen och i litteraturen.

Ett motsägelsebevis är speciellt användbart då man har en utsaga vars motsats är väldigt lätt att definiera, t.ex:

B: $x > 0$ $\quad\Rightarrow\quad$ $\neg$ B: $x \leq 0$

Ett annat exempel då motsägelsebevis är väldigt användbart är då utsagan redan från början innehåller ordet ”inte”. Jag genomför här nedan just ett sådant motsägelsebevis (hämtat från Persson och Böiers, [9], s. 33 - men med mina omarbetningar):

SATS: $\sqrt{2}$ *är inte ett rationellt tal.*

BEVIS: Jag använder Polyas angreppssätt för att bevisa satsen.

1. FÖRSTÅ PROBLEMET

Här finns inget antagande, endast ett påstående - att talet $\sqrt{2}$ inte är rationellt.

(Om vi vill kan vi i och för sig skriva om satsen på detta sätt:
$x^2 = 2 \Rightarrow x$ är irrationellt. Det är dock tveksamt om det ger oss någon ytterligare information i just detta fall.)

2. GÖR UPP EN PLAN

Först går vi tillbaka till definitionen av ett rationellt tal; det är ett tal som kan skrivas som kvoten av två heltal.

Nu vill vi prova att göra ett motsägelsebevis, och därför måste vi börja med att anta att $\sqrt{2}$ faktiskt **är** ett rationellt tal, och se om vi då får en motsägelse.

3. GENOMFÖR PLANEN

Antag alltså att $\sqrt{2}$ vore ett rationellt tal. Det skulle då ha formen

$$\sqrt{2} = \frac{p}{q} \tag{3.1}$$

där p och q är heltal och $q \neq 0$. Vi kan dessutom förutsätta att kvoten p/q är förkortat så långt det går, dvs p och q saknar gemensamma faktorer förutom 1, dvs de är relativt prima. (Detta är inte ett nytt antagande. Om de skulle ha gemensamma faktorer så förkortar vi dem helt enkelt tills de inte längre har några gemensamma faktorer.)

Genom kvadrering av (3.1) fås

$$2 = \frac{p^2}{q^2} \tag{3.2}$$

eller omskrivet

$$p^2 = 2q^2 \tag{3.3}$$

Detta visar att p^2 är ett jämnt tal, eftersom högerledet i likheten är delbart med 2. Eftersom kvadraten av ett udda tal alltid är udda (försök gärna bevisa att det är så!), så måste p vara ett jämnt tal. (Denna slutsats kan vi dra pga att "p udda $\Rightarrow$ p^2 udda" är kontrapositivet till "p^2 jämn $\Rightarrow$ p jämn. Se nästföljande avsnitt för mer detaljer om kontrapositiv.) Talet p är alltså jämnt och kan skrivas på formen $p = 2n$ med något heltal n. Sätter vi in detta i (3.3) får vi att

$$4n^2 = 2q^2 \tag{3.4}$$

dvs att

$$q^2 = 2n^2 \tag{3.5}$$

Men detta ger ju att q^2 är jämnt, och därmed är även q ett jämnt tal. Om både p och q är jämna har de en gemensam faktor, nämligen 2. Men detta strider mot vårt val av p och q. Vi har fått en motsägelse. Alltså kan $\sqrt{2}$ inte vara ett rationellt tal. Endast en annan möjlighet återstår; $\sqrt{2}$ måste vara ett irrationellt tal.

4. SE TILLBAKA

Eftersom alla reella tal antingen är rationella eller irrationella så måste $\sqrt{2}$ tillhöra någon av dessa kategorier. Och genom att visa att $\sqrt{2}$ inte är rationellt så har vi visat att det måste vara irrationellt.

Motsägelsebevis kan användas då man har ett påstående P som (enkelt) kan skrivas om som en negation. Genom att anta att både antagande A **och** $\neg P$ gäller (alternativ, om antagande saknas, genom att anta att $\neg P$ gäller) så hoppas man finna en motsägelse - och i så fall kan man säkert sluta sig till att P faktiskt måste gälla.

Några frågor att ställa till sig själv kan vara:
Är $\sqrt{3}$ rationellt eller irrationellt?
Finns det andra rotuttryck som är irrationella tal?
Kan jag bevisa detta för något av dessa tal?

3.3.4 Bevis med kontrapositiv

Om vi har en utsaga att $P \Rightarrow Q$ så är det ekvivalent med utsagan att $\neg Q \Rightarrow \neg P$ (se även Bilaga 1 för mer detaljer).

Utsagan $\neg Q \Rightarrow \neg P$ kallas **kontrapositivet** till utsagan $P \Rightarrow Q$. I många fall är det lättare att visa kontrapositivet än den ursprungliga utsagan. Jag ger ett exempel på hur man använder denna metod. Exemplet har jag hämtat från Biggs [2], s. 21-22, med min egen översättning och egna omarbetningar.

UTSAGA: *Talet* 3 *är ett primtal, och* $3 + 1 = 4$ *är en perfekt kvadrat (dvs ett heltal som är kvadraten av ett annat heltal). Det finns inte några andra primtal* n *sådana att* $n + 1$ *är en perfekt kvadrat.*

BEVIS:
1. FÖRSTÅ PROBLEMET.
Vårt **antagande** är att n är ett primtal skilt från 3. Vårt **påstående** är att $n + 1$ **inte** är en perfekt kvadrat.

2. GÖR UPP EN PLAN
Vi kan skriva om vårt antagande och påstående så här:
n är ett primtal skilt från $3 \Rightarrow n + 1$ är **inte** en perfekt kvadrat.

Ett direkt bevis skulle t.ex kunna vara att räkna upp alla primtal för att kontrollera om det stämmer. Var och en inser att det är en omöjlig uppgift. Istället kan vi prova med ett indirekt bevis, där vi utgår från kontrapositivet till ovanstående utsaga, för att se vad det leder till.

En möjlig arbetsplan blir då:
1) Inför beteckningar så att utsagan blir mer lätthanterlig.
2) Formulera ett kontrapositiv till utsagan.
3) Slutför resonemanget.

3. GENOMFÖR PLANEN
Utsagan skrivs om, med nya beteckningar:
Låt m och n vara heltal. Då gäller:
$n \neq 3$ och n är ett primtal $\Rightarrow n + 1 \neq m^2$

Kontrapositivet till denna utsaga skulle då bli:
Låt m och n vara heltal. Då gäller:
$n + 1 = m^2 \Rightarrow n = 3$ eller n är **inte** ett primtal.

[*Kommentar: Här använder jag att negationen till "A och B" är "¬ A eller ¬ B". Jmf tabellen över negationer i avsnitt 3.3.2.*]

Nu försöker vi bevisa kontrapositivet! Först gör vi en omskrivning:

$$n+1=m^2 \quad \Leftrightarrow \quad n=m^2-1=(m+1)(m-1)$$

n kan alltså skrivas som produkten av två tal. Detta ger oss två olika fall:

1. Om det mindre av talen är 1 (dvs att $(m-1)=1$) är $n=3$:
   $m-1=1 \quad \Leftrightarrow \quad m=2 \quad \Leftrightarrow \quad n=(m+1)(m-1)=3\cdot 1=3$
2. Om det mindre av talen är >1 kan n inte vara ett primtal:
   $n=(m+1)(m-1)$ där både $(m+1)$ och $(m-1)$ är heltal skilda från 1. Per definition är då n inte ett primtal.

Vi har nu visat att om $n+1$ är en perfekt kvadrat så finns det två fall; antingen är $n=3$ eller så är n inte ett primtal. Vi har alltså bevisat kontrapositivet - och därmed har vi även bevisat den ursprungliga utsagan att om n är ett primtal skilt från 3, så kan $n+1$ inte vara en perfekt kvadrat!

4. SE TILLBAKA

Ovanstående är ett exempel på hur man arbetar med bevis med kontrapositiv. Observera också att när man väl har formulerat kontrapositivet så arbetar man sedan med beviset precis som då man genomför ett direkt bevis. Svårigheterna i denna teknik ligger snarast i att kunna bestämma kontrapositivet på ett korrekt sätt. Men övning ger färdighet!

Metoden kräver dels att det finns både ett antagande och ett påstående och att både antagandet och påståendet verkligen har en motsats, så att det går att skapa ett kontrapositiv. Helst bör dessutom en sådan motsats vara någorlunda enkel att konstruera, om metoden ska vara effektiv.

Om det inte finns ett antagande, utan bara ett påstående, så kan man istället använda metoden med motsägelsebevis.

Några tänkbara frågor för att fördjupa sin egen förståelse utifrån detta exempel skulle kunna vara:

Antag att n är ett primtal. Kan t.ex $n+3$ bli en perfekt kvadrat?

Antag att n är ett primtal. För vilka x är det sant att $n+x$ blir en perfekt kvadrat?

På vilka sätt kan man med hjälp av primtal konstruera en perfekt kvadrat?

*"**Tänd hellre ett ljus än klaga över mörkret.**"*
Konfucius, 551-479 f.Kr, kinesisk tänkare.

3.4 Matematisk induktion

3.4.1 Induktionsprincipen

I läroböckerna presenteras matematisk induktion ofta i samband med att man studerar heltalen eller de naturliga talen. Metoden kan dock även användas i mer generella situationer, som vi ska se längre fram (se avsnitt 3.4.7). Till en början koncentrerar vi oss dock på fallet med naturliga tal.

När man arbetar med induktionsbevis utnyttjar man induktionsprincipen, som kortfattat kan beskrivas så här:

Antag att vi har en utsaga $P(n)$ där n är ett naturligt tal. Antag sedan att $P(n)$ har följande egenskaper:

1. *Basfallet: $P(n_0)$ är sann, där n_0 är det minsta heltal för vilket utsagan sägs gälla.*
2. *Induktion: För alla $k \in \mathbb{N}$ med $k \geq n_0$ gäller att om utsagan $P(k)$ är sann så är även utsagan $P(k+1)$ sann.*

Då vet vi att utsagan $P(n)$ är sann för alla $n \geq n_0$.

Observera att det inte alltid är så att basfallet är att $n_0 = 1$. Många gånger gäller att n måste vara större än ett visst värde. Basfallet blir då det minsta värde som n kan anta.

Hur fungerar denna metod? Ofta beskrivs den som en dominoeffekt:
Om vi har visat att induktionen fungerar, så vet vi att om $P(n)$ är sann så är även $P(n+1)$ sann. Genom basfallet har vi visat att $P(n_0)$ är sann. Eftersom vi visat att induktionen fungerar så vet vi att då måste även $P(n_0+1)$ vara sann, och då måste även $P((n_0+1)+1)$ vara sann, o.s.v. Så kan vi fortsätta i all oändlighet. Alltså måste $P(n)$ vara sant för alla $n \geq n_0$.
Alltså; om den första brickan faller, dvs om basfallet är sant, och om vi dessutom har visat att induktionen fungerar, så kommer alla andra brickor också att falla - en efter en.

Notera också följande:
"Många studenter tror felaktigt att villkor (2) [egentligen egenskap (2); min kommentar] innebär att $P(n)$ är sann, och undrar varför man ska behöva slå fast det igen som en slutsats. Titta noga på villkor (2). Observera att

det är en implikation. Vi säger **inte** att $P(n)$ är sann. Vi säger att **om** $P(n)$ är sann, så är $P(n+1)$ sann. Antagandet att $P(n)$ är sann kallas för induktionshypotesen." ([4], s.209)

Sammantaget innebär ovanstående att ett induktionsbevis måste innehålla följande steg:

1. **Basfallet:** Visa att utsagan är sann för basfallet ($P(n_0)$).
2. **Induktionsantagande:** Antag sedan att utsagan är sann för ett visst men godtyckligt k, $n = k$, dvs utsagan $P(k)$ är sann. Detta är vårt induktionsantagande.
3. **Induktionssteg:** Kontrollera om utsagan $P(k+1)$ är sann, genom att använda antagandet att $P(k)$ är sann.
4. **Slutsats:** Om $P(n_0)$ är sann, och om antagandet att $P(k)$ är sann medför att även $P(k+1)$ är sann (dvs om $P(k) \Rightarrow P(k+1)$), så kan vi enligt induktionsprincipen anta att utsagan $P(n)$ är sann för alla naturliga tal $n \geq n_0$.

3.4.2 Induktionsbevis: exempel

Ett exempel visar hur det går till i praktiken:

PROBLEM:
Visa att för alla naturliga tal n gäller att $n^2 + n$ är ett jämnt tal.

LÖSNING:

- **Basfallet:** Visa att utsagan är sann för basfallet. Här är basfallet $n = 1$. Vi får då att $1^2 + 1 = 1 + 1 = 2$. 2 är definitivt ett jämnt tal, så vi ser att utsagan är sann för basfallet.
- **Induktionsantagande:** Antag att utsagan är sann för $n = k$, dvs att $k^2 + k = 2m$ (där även m är ett naturligt tal).
- **Induktionssteg:** Nu testar vi om utsagan är sann för $n = (k+1)$. Vi sätter in $(k+1)$ i formeln:

$$(k+1)^2 + (k+1) = (k^2 + 2k + 1) + (k+1)$$

Vi flyttar om termerna i högra ledet och får:

$$(k^2 + k) + 2k + 2$$

Eftersom vi antagit att $k^2 + k = 2m$ kan vi skriva om ekvationen:

$$2m + 2k + 2 = 2(m + k + 1)$$

- **Slutsats:** Högra ledet är en multipel av 2, dvs ett jämnt tal - vilket skulle visas!

  Vi har visat att basfallet stämmer, och vi har visat att induktionen fungerar. Enligt induktionsprincipen kan vi då anta att utsagan är sann för alla naturliga tal.

Ovanstående exempel är hämtat från Biggs ([2], s. 29), med min översättning och mina omarbetningar.

3.4.3 Induktionsbevis, avancerat exempel

Nedan ges ett annorlunda exempel på induktionsbevis, hämtat från Garnier & Taylor, som vanligt med min översättning och mina omarbetningar, ([5], s.249-251).

SATS:
Om A är en mängd sådan att $|A| = n$, så är $|\mathcal{P}(A)| = 2^{|A|} = 2^n$.

BEVIS:
1. FÖRSTÅ PROBLEMET
Vi måste börja med några förklaringar.
Beteckningen $\mathcal{P}(A)$ står för **potensmängd** ("power set"), dvs mängden av alla delmängder till A. Satsen säger alltså att om mängden A innehåller n element, så är antalet delmängder till A lika med $2^{|A|} = 2^n$.

Exempel:
$S = \{1, 2, 3\}$
S innehåller alltså tre element, dvs $n = 3$.

Hur många olika delmängder finns det till en mängd med tre element? Vi har dels den tomma mängden, och dels den kompletta mängden - dvs två olika mängder med noll respektive tre element. Sedan har vi tre olika delmängder med ett element samt tre olika delmängder med två element. Totalt åtta delmängder.

Detta ger att:
$\mathcal{P}(S) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}\, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Vi får alltså:
$|S| = 3 \quad \Rightarrow \quad |\mathcal{P}(S)| = 8 = 2^3$

2. GÖR UPP EN PLAN

Vi utgår från vår sats, som kan skrivas om:

$$|A| = n \quad \Rightarrow \quad |\mathcal{P}(A)| = 2^n$$

Vi vill här testa att använda oss av induktionsprincipen. Vi måste alltså identifiera basfallet samt kontrollera att induktionen verkligen fungerar.

3. GENOMFÖR PLANEN

Basfallet:

Basfallet är att $n = 0$.

$|A| = 0$, dvs A är en tom mängd, vilket medför att det bara finns en enda delmängd: $\mathcal{P}(A) = \{\emptyset\}$. Detta betyder att $|\mathcal{P}(A)| = 1 = 2^0$

Vi ser alltså att basfallet stämmer:
$|A| = 0 \quad \Rightarrow \quad |\mathcal{P}(A)| = 2^0 = 1$

Induktionsantagande:

Vi antar att sambandet gäller då $n = k$, dvs att
$|A| = k \quad \Rightarrow \quad |\mathcal{P}(A)| = 2^k$

Induktionssteg:

Vi vill visa att om vårt induktionsantagande stämmer, så är det även sant att
$|A| = k + 1 \quad \Rightarrow \quad |\mathcal{P}(A)| = 2^{k+1}$

Att $|A| = k + 1$ innebär att A har $k + 1$ element. En mängd med $k + 1$ element kan skrivas som unionen av två disjunkta mängder; en mängd med k element och en mängd med 1 element. Vi kallar dem B respektive C, dvs $A = B \cup C$ där $|B| = k$ och $|C| = 1$.

Hur många element innehåller då $\mathcal{P}(A) = \mathcal{P}(B \cup C)$?

Vi ger ett litet exempel.

Antag att $A = \{a_1, a_2, a_3\}$ och att $B = \{a_1, a_2\}$ samt att $C = \{a_3\}$.

Detta ger oss att $\mathcal{P}(B) = \{\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\}\}$. $\mathcal{P}(B)$ har alltså fyra element.

Eftersom $B \subset A$ så är varje delmängd till B också en delmängd till A, dvs $\mathcal{P}(B) \subset \mathcal{P}(A)$.

Vilka andra element finns det i $\mathcal{P}(A)$?

Dessa element får vi om vi till varje delmängd till B lägger det enda elementet i C:

$\{\emptyset\} \cup \{a_3\} = \{a_3\}$
$\{a_1\} \cup \{a_3\} = \{a_1, a_3\}$
$\{a_2\} \cup \{a_3\} = \{a_2, a_3\}$
$\{a_1, a_2\} \cup \{a_3\} = \{a_1, a_2, a_3\}$

$\mathcal{P}(A)$ har alltså $4 + 4$ element.

Generellt gäller att om $\mathcal{P}(B)$ innehåller n element (dvs $|\mathcal{P}(B)| = n$), så kommer $\mathcal{P}(A)$ att innehålla dessa n element tillsammans med ytterligare n element, som bildas genom att ta unionen av det enda elementet i C och varje element i $\mathcal{P}(B)$.

Generellt gäller därför att om $|A| = k + 1$, och om $B \subset A$ med $|B| = k$, så är $|\mathcal{P}(A)| = 2 \cdot |\mathcal{P}(B)|$.

I vårt fall får vi:

$A = B \cup C$ (där $|A| = k + 1$, $|B| = k$ och $|C| = 1$) medför att $|\mathcal{P}(A)| = 2 \cdot |\mathcal{P}(B)| = 2 \cdot 2^k$ [enl. vårt induktionsantagande] $= 2^{k+1}$

Slutsats:

Vi ser alltså att induktionsantagandet medför att $|A| = k + 1 \quad \Rightarrow |\mathcal{P}(A)| = 2^{k+1}$, dvs induktionen fungerar.

Eftersom även basfallet visat sig stämma, så kan vi enligt induktionsprincipen dra slutsatsen att den ursprungliga satsen är korrekt, dvs:

Om $|A|$ är en mängd sådan att $|A| = n$, så är $|\mathcal{P}(A)| = 2^n$ för alla $n \in \mathbb{N}$.

4. SE TILLBAKA

Som synes innebär ett induktionsbevis att man konsekvent använder metodens fyra steg:

1. Verifiera basfallet
2. Gör ett induktionsantagande
3. Visa induktionssteget
4. Dra slutsats; om basfallet kan verifieras och om $P(k) \Rightarrow P(k + 1)$, så vet vi att $P(n)$ gäller för alla $n \geq n_0, \quad n \in \mathbb{N}$.

Kommentar: Det är viktigt att bestämma vilket tal som basfallet ska baseras på. Annars kan hela induktionen bli fel.

3.4.4 Den starka principen för matematisk induktion

Ibland talar man om **den starka principen för matematisk induktion** eller **generell induktion**. Den starka induktionsprincipen innebär:

Antag att vi har en utsaga $P(n)$ där n är ett naturligt tal. Antag sedan att $P(n)$ har följande egenskaper:

1. *Basfallet: $P(n_0)$ är sant, där n_0 är det minsta heltal för vilket utsagan sägs gälla.*
2. *Induktion: Om $P(k)$ är sann för **alla** $k = n_0, n_0 + 1, \ldots, n - 1, n$, så är även $P(k + 1)$ sann.*

Då vet vi att utsagan $P(n)$ är sann för alla $n \geq n_0$.

Med den starka induktionsprincipen är vi alltså fria att anta att alla eller vilka som helst av $P(x)$ med $n_0 \leq x \leq n$ är sanna, och använda detta för att visa att i så fall är även $P(n + 1)$ sann.

Oftast räcker det i praktiken att t.ex visa att om $P(n - 1)$ och $P(n)$ är sanna, så är också $P(n + 1)$ sann.

Ett par ord om skillnaden mellan den svaga och den starka induktionsprincipen:

"Om man läser den starka induktionsprincipen så inser man lätt att den svaga induktionsprincipen är en följd av den starka principen. Induktionshypotesen i den svaga principen bygger på antagandet att den givna utsagan är sann för ett godtyckligt tal n. Induktionshypotesen i den starka principen bygger på antagandet att den givna utsagan är sann för alla tal från basfallet upp till ett godtyckligt tal n.

I realiteten är dessa två principer ekvivalenta. Beviset för detta är inte lätt; det består i att bevisa att var och en av de två principerna är ekvivalent med en tredje princip, Välordningsprincipen [se avsnitt 3.5.2]. Därmed är den starka induktionsprincipen och den svaga induktionsprincipen ekvivalenta. " ([3], s.50-51)

Man kan alltid använda den starka induktionsprincipen i ett induktionsbevis, men ofta räcker det att använda den svaga principen och beviset blir då kortare.

3.4.5 Den starka principen, exempel med ett basfall

Nedanstående exempel är hämtat från Garnier & Taylor ([5], s.259-260) med min översättning och mina omarbetningar. Exemplet gäller aritmeti-

kens fundamentalsats. Ett annat bevis för denna sats ges i avsnitt 5.3.

SATS:
Varje heltal större än 1 kan skrivas som en produkt av primtal.

BEVIS:
Vi definierar:
P(n): n kan skrivas som en produkt av primtal.

Eftersom vi måste visa att $P(n)$ är sant för alla $n \geq 2$ ska vi använda induktion.

Basfall:
Eftersom talet 2 är ett primtal i sig själv så kan det skrivas som en produkt av primtal, så $P(2)$ är sant.

Induktionsantagande:
Vi antar att satsen är sann för alla $k \leq n$.

Induktionssteg:
Nu vill vi visa att i så fall är satsen även sann för $n = k + 1$.

Talet $k + 1$ kan antingen vara ett primtal eller ett sammansatt tal.
Om det är ett primtal är vi klara, eftersom alla primtal kan skrivas som en produkt av primtal - nämligen sig självt.
Om det är ett sammansatt tal så kan vi skriva:

$$k + 1 = q_1 q_2 \quad \text{där} \quad 2 \leq q_1, q_2 \leq k$$

Genom vårt induktionsantagande så kan båda talen q_1 och q_2 skrivas som en produkt av primtal, så att:

$$q_1 = a_1 a_2 \cdots a_r \quad \text{och} \quad q_2 = b_1 b_2 \cdots b_s$$

där $a_i, i = 1, 2, \ldots, r$ och $b_j, j = 1, 2, \ldots, s$ är primtal.

Slutsats:
Alltså är $k + 1 = a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s$, dvs $k + 1$ kan skrivas som en produkt av primtal. Därmed har vi visat att induktionen fungerar och eftersom även basfallet var sant, så kan vi slå fast att satsen är sann för alla heltal $n \geq 2$.

3.4.6 Den starka principen, exempel med två basfall

Det är ganska vanligt att man har induktion som bygger på två basfall (eller flera). Jag visar ett exempel hämtat från Biggs ([2], s. 33).

EXEMPEL:
Visa att om u_n *definieras genom* $u_1 = 1$, $u_2 = 5$ *och* $u_{n+1} = 5u_n - 6u_{n-1}$ *för* $n \geq 2$, *så är* $u_n = 3^n - 2^n$ *för alla* $n \in \mathbb{N}$.

LÖSNING:
Basfallet:
Vi ser att utsagan stämmer för $n = 1$ och $n = 2$, eftersom
$3^1 - 2^1 = 1 = u_1$ och $3^2 - 2^2 = 5 = u_2$

Induktionsantagande:
Vi antar att formeln $u_n = 3^n - 2^n$ är korrekt för alla $k \leq n$, och speciellt för u_k och u_{k-1}. Vi får:
$u_k = 3^k - 2^k$
$u_{k-1} = 3^{k-1} - 2^{k-1}$

Induktionssteg: Vi testar om formeln är sann för u_{k+1}. Vi har att
$u_{k+1} = 5u_k - 6u_{k-1}$

Här kan vi nu använda vårt induktionsantagande för u_k och u_{k-1}, och vi skriver om det högra ledet:

$$\begin{aligned}
5_{u_k} - 6_{u_{k-1}} &= 5(3^k - 2^k) - 6(3^{k-1} - 2^{k-1}) \\
&= (5 \cdot 3^k - 5 \cdot 2^k) - (6 \cdot 3^{k-1} - 6 \cdot 2^{k-1}) \\
&= (5 \cdot 3^k - 6 \cdot 3^{k-1}) - (5 \cdot 2^k - 6 \cdot 2^{k-1}) \\
&= (5 \cdot 3 - 6)3^{k-1} - (5 \cdot 2 - 6)2^{k-1} \\
&= 9 \cdot 3^{k-1} - 4 \cdot 2^{k-1} \\
&= 3^2 \cdot 3^{k-1} - 2^2 \cdot 2^{k-1} \\
&= 3^{k+1} - 2^{k+1}
\end{aligned}$$

Slutsats:
Detta är den sökta formeln för u_{k+1}.

Eftersom vi visat att basfallet är sant, och eftersom vi visat att induktionen fungerar - dvs att $P(u_{k-1})$ och $P(u_k) \Rightarrow P(u_{k+1})$ - vet vi genom den starka induktionsprincipen att formeln $u_n = 3^n - 2^n$ stämmer för alla $n \geq 1$.

3.4.7 Spridningsprincipen

Metoden med induktionsbevis är inte bara begränsad till att gälla heltal eller naturliga tal. Generellt kan man säga att metoden innebär att man utgår

från en mängd där man säkert vet att en viss utsaga är sann, och sedan utökar man successivt denna mängd tills man har ringat in alla de fall då utsagan är sann. På detta sätt sprider sig utsagan som ringar på vattnet, till allt större mängder/områden.

Ett exempel på en spridningsprincip skulle kunna se ut så här:

SATS:

Om uttrycken a och b båda är deriverbara kommer även deras produkt ab och summa $a + b$ att vara deriverbara.

Här kan vi tänka oss att vårt basfall är att a är ett polynom av grad 0, dvs på formen $a = c_0$ och att b är ett polynom av grad 1, dvs på formen $b = c_0 + c_1 x$. Produkten ab blir då $c_0^2 + c_0 c_1 x$, vars derivata existerar och är $c_0 c_1$. Summan $a + b$ blir $2c_0 + c_1 x$, som har derivatan c_1.

Vi kan sedan arbeta oss vidare och multiplicera eller addera den nya produkten/summan med b eller med sig själv och på detta sätt hela tiden skapa nya polynom. Vi kommer att finna att alla dessa är deriverbara och till slut kan vi dra slutsatsen att **alla** polynom är deriverbara.

Därefter kan vi gå vidare och titta på trigonometriska uttryck, och vi kommer på samma sätt snart se att alla trigonometriska uttryck och alla kombinationer av polynom och trigonometriska uttryck är deriverbara.

På detta sätt kan vi successivt utöka mängden av deriverbara uttryck tills vi har täckt in alla kända fall.

Ytterligare ett exempel på ett induktionsbevis finns i avsnittet om kommenterade bevis, se avsnitt 5.4.

"Liten nyckel kan öppna stor dörr."
Turkiskt ordspråk

3.5 Olika hjälptekniker

3.5.1 Inledning

Många gånger måste man ta till olika "knep" eller hjälptekniker för att förenkla det problem man arbetar med. Detta avsnitt syftar till att ge några exempel på sådana hjälptekniker. Jag gör inte anspråk på att ha skrivit en komplett förteckning på sådana tekniker, men ger i varje fall en hjälp på vägen.

3.5.2 Välordningsprincipen

En mycket användbar matematisk princip är välordningsprincipen, som säger:

Varje icke-tom mängd av naturliga tal innehåller ett minsta element.

Välordningsprincipen kan även utökas till en starkare formulering:

Varje mängd av heltal som är nedåt begränsad innehåller ett minsta element.

De naturliga talen är som bekant alla icke-negativa heltal. Det är ganska naturligt att en mängd av icke-negativa heltal måste innehålla ett minsta heltal, t.ex 0. Däremot är det inte säkert att en sådan mängd innehåller ett största heltal! Det är lika naturligt att en mängd av heltal som är begränsad nedåt innehåller ett minsta heltal.

För att kunna använda välordningsprincipen måste man **först** visa att det finns en nedåt begränsad mängd av heltal som har den egenskap man behöver, och **därefter** kan man fastställa att i så fall finns ett minsta sådant tal i mängden. På motsvarande sätt gäller att en uppåt begränsad mängd av heltal har ett största element.

Välordningsprincipen används exempelvis för att bevisa Divisionsalgoritmen för heltal - se avsnitt 5.2.

3.5.3 Hjälpstorheter

Många gånger när man vill visa att ett tal eller en funktion har vissa egenskaper inför man någon typ av "hjälpstorhet". Dessa hjälptal kan vara faktiska tal, mängder eller andra matematiska begrepp. Inom detta område ryms också olika typer av substitutioner som man gör för att förenkla sitt arbete. Nedan följer några exempel på hjälpstorheter:

Substitution:
I ekvationen $t^4 + 3t^2 - 4 = 0$ kan vi ersätta t^2 med x, så att vi får en ny ekvation $x^2 + 3x - 4 = 0$.

Hjälpmängd:
I beviset för Divisionsalgoritmen (avsnitt 5.2) införs mängden
$R = \{a - bq | q \in \mathbf{Z}\}$, som består av alla rester då bq subtraheras från a.

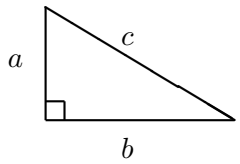
Hjälptal:
I bevis med kontrapositiv (avsnitt 3.3.4) sägs att:
"$n + 1 = m^2 \Rightarrow n = 3$ *eller* n *är inte ett primtal.*"
Här är m^2 ett exempel på ett hjälptal.

Ovanstående är bara några exempel. Listan kan göras mycket längre. När man läser matematiska bevis bör man vara observant på vilka hjälptal som eventuellt införs.

3.5.4 Hjälpkonstruktioner

Speciellt när man arbetar med ett geometriskt problem (eller då man studerar grafer till olika funktioner) kan det vara till stor hjälp att införa en hjälpkonstruktion. Nedanstående exempel, där vi bevisar Pythagoras sats, är hämtat från Persson och Böiers ([9], s.28), med mina egna omarbetningar.

SATS:
Om c är längden av hypotenusan och a och b är längderna av kateterna i en rätvinklig triangel så gäller att:
$c^2 = a^2 + b^2$



BEVIS:

1. FÖRSTÅ PROBLEMET

För det första gäller påståendet i satsen endast rätvinkliga trianglar. Detta är alltså vårt **antagande**, dvs vi antar att vi arbetar med en rätvinklig triangel (med hypotenusan c, och kateterna a och b). **Påståendet** är att satsen är sann för alla rätvinkliga trianglar.

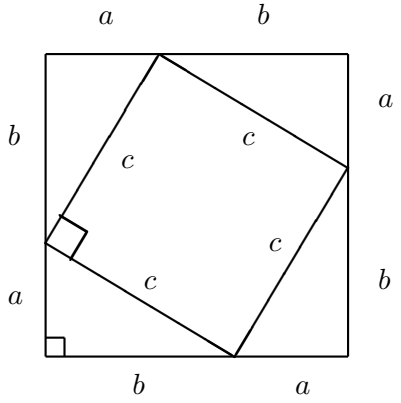
2. GÖR UPP EN PLAN

Vi utgår från en rätvinklig triangel. Finns det någon annan rätvinklig konstruktion som vi kan ta hjälp av? Exempelvis en (rätvinklig) rektangel?

I formeln finns uttrycket c^2. Detta är som bekant areaformeln för en kvadrat med sidan c. Kanske kan vi då skapa en konstruktion med en kvadrat med sidan c, utifrån vår rätvinkliga triangel och se om det ger oss någon öppning?

3. GENOMFÖR PLANEN

Vi lägger ut fyra kopior av vår rätvinkliga trianglar, så att deras kateter formar en yttre kvadrat och deras hypotenusor formar en inre kvadrat:



Enligt formeln för en kvadrats area har vi då att den yttre kvadratens area är $(a+b)^2$. Men man kan också tänka att den yttre kvadratens area är uppbyggd av den inre kvadratens area plus areorna av de fyra trianglarna, dvs den yttre kvadratens area kan också skrivas $c^2+4\frac{ab}{2}$. Vi får alltså följande likhet:

$$c^2 + 4\frac{ab}{2} = (a+b)^2$$

Utveckling av båda leden ger:

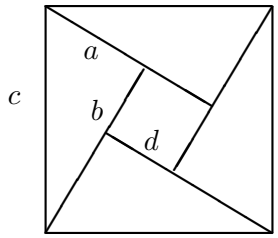
$$c^2 + 2ab = a^2 + 2ab + b^2$$

Och efter förenkling får vi:

$$c^2 = a^2 + b^2$$

4. SE TILLBAKA

Genom att skapa en hjälpkonstruktion kan vi nu alltså bevisa Pythagoras sats. En alternativ konstruktion för att bevisa satsen hade varit att konstruera en annan kvadrat med den **yttre** sidan = c, enligt denna skiss:



Vi får då att c^2 = arean av de fyra inre trianglarna, plus arean av den inre kvadraten, vars sida är $d = (b - a)$, dvs vi får:

$$\begin{aligned} c^2 &= 4\frac{ab}{2} + d^2 = 2ab + (b-a)^2 \\ &= 2ab + b^2 - 2ab + a^2 \\ &= a^2 + b^2 \end{aligned}$$

Att skapa en hjälpkonstruktion kan användas på många olika bevisproblem, både inom geometri och andra matematiska områden.

I detta fall kan vi öka vår förståelse av problemet om vi t.ex försöker besvara denna följdfråga:

Hur blir det om triangeln inte uppfyller kravet på rätvinklighet?

3.5.5 Likheter

Det finns en uppsjö av olika sätt att arbeta med en likhet så att den blir lättare att bevisa. Principen innebär att förändra vänster- och högerledet så att likheten fortfarande gäller. Jag ger ett exempel hämtat från Persson och Böiers ([9] s. 252-253).

SATS (Partiell integration):
Om F är en primitiv funktion till f så är

$$\int f(x)g(x)\,dx = F(x)g(x) - \int F(x)g'(x)\,dx \tag{3.6}$$

BEVIS:
1. FÖRSTÅ PROBLEMET
Vi har ett **antagande** om att F är en primitiv funktion till f. Enligt definitionen av en primitiv funktion betyder det att

$$\int f(x)\,dx = F(x) \tag{3.7}$$

vilket är ekvivalent med att

$$D[\int f(x)\,dx] = D[F(x)] = F'(x) = f(x) \tag{3.8}$$

Vårt **påstående** är uttrycket i ekvation (3.6).

2. GÖR UPP EN PLAN
Vårt påstående är alltså uttrycket

$$\int f(x)g(x)\,dx = F(x)g(x) - \int F(x)g'(x)\,dx$$

Eftersom derivatan av vänstra ledet i detta uttryck är lika med $f(x)g(x)$ så måste även derivatan av högra ledet vara samma sak, för att likheten ska gälla. För att genomföra vårt bevis behöver vi alltså "bara" bevisa att det sambandet gäller.

3. GENOMFÖR PLANEN
Vi vill visa att nedanstående likhet gäller:

$$\int f(x)g(x)\,dx = F(x)g(x) - \int F(x)g'(x)\,dx$$

Om vi deriverar VL och HL var för sig får vi:

$$D[\int f(x)g(x)\,dx] = D[F(x)g(x) - \int F(x)g'(x)\,dx] \tag{3.9}$$

Derivatan av vänstra ledet i ekvation (3.9) fås genom definitionen av en primitiv funktion:

$$D[\int f(x)g(x)\,dx] = f(x)g(x)$$

I högerledet i ekvation (3.9) fås derivatan av första termen genom derivatan av en produkt:

$$D[F(x)g(x)] = F'(x)g(x) + F(x)g'(x)$$

Derivatan av andra termen fås genom definitionen av en primitiv funktion:

$$D[\int F(x)g'(x)\,dx] = F(x)g'(x)$$

Derivatan av hela högra ledet blir alltså:

$$F'(x)g(x) + F(x)g'(x) - F(x)g'(x) = F'(x)g(x) = f(x)g(x)$$

Eftersom derivatan av vänster- och högerledet är lika har vi även visat att det ursprungliga vänster- och högerledet är lika - och beviset är klart.

4. SE TILLBAKA

Genom att helt enkelt derivera både vänster- och högerledet i den ursprungliga likheten har vi visat att formeln för partialintegration gäller. Andra metoder att arbeta med likheter kan exempelvis vara att genomföra en kvadratkomplettering, att göra ett variabelbyte/substitution, att kvadrera eller dra roten ur vänster- och högerledet, osv. Här gäller det att vara kreativ och öppen för att våga prova sig fram.

3.5.6 Trial and error

När man ska försöka bevisa (eller förkasta) en sats kan man ofta komma långt genom att helt enkelt prova sig fram. Låt oss gå tillbaka till föregående sats om partiell integration och prova ett annat angreppssätt.

SATS (Partiell integration):
Om F är en primitiv funktion till f så är

$$\int f(x)g(x)\,dx = F(x)g(x) - \int F(x)g'(x)\,dx \tag{3.10}$$

BEVIS:

1. FÖRSTÅ PROBLEMET

Vi har ett **antagande** om att F är en primitiv funktion till f. Enligt definitionen av en primitiv funktion betyder det att

$$\int f(x)\,dx = F(x)$$

Vårt **påstående** är uttrycket i ekvation (3.10)

2. GÖR UPP EN PLAN
Enligt vårt antagande har vi att

$$\int f(x)\,dx = F(x)$$

Men nu vill vi istället veta resultatet av

$$\int f(x)g(x)\,dx$$

Vi kommer här att prova oss fram tills vi hittar en formel vi kan tro på.

3. GENOMFÖR PLANEN
Vi kan prova med

$$\int f(x)g(x)\,dx \stackrel{?}{=} F(x)g(x)$$

Vi kontrollerar detta resultat genom att jämföra derivatan av vänster- och högerledet. Enligt definitionen av en primitiv funktion är vänsterledets derivata:

$$D[\int f(x)g(x)\,dx] = f(x)g(x)$$

Högerledets derivata är (enligt formeln för derivatan av en produkt):

$$D[F(x)g(x)] = F'(x)g(x) + F(x)g'(x) = f(x)g(x) + F(x)g'(x)$$

Här får vi alltså en "oönskad" extra term $F(x)g'(x)$. För att kompensera för denna kompletterar vi vår formel med den primitiva funktionen till $F(x)g'(x)$, och skriver:

$$\int f(x)g(x)\,dx = F(x)g(x) - \int F(x)g'(x)\,dx$$

4. SE TILLBAKA
På det här sättet kan man alltså själv härleda olika formler, bara genom att prova sig fram. **Just detta exempel kan dessutom vara ett bra sätt att själv återskapa formeln för partiell integration**, om man skulle råka glömma bort den!

Kapitel 4

Delproblem

*"**Verkliga svårigheter kan man övervinna, endast de inbillade är oövervinnerliga.**"*

Gerd Vesperman, 1926-2000, tysk skådespelerska

4.1 Entydighet: Visa att ett objekt är unikt

Det är ganska vanligt i olika bevis att man behöver visa entydighet, dvs att ett objekt (t.ex talet x) med en viss egenskap är unik. Det finns i princip tre sätt att visa att ett objekt är unikt:

1. **Entydigt uttryck:** Man försöker helt enkelt hitta ett entydigt uttryck för objektet, och i så fall är objektet unikt.

2. **Generellt argument:** Ett generellt argument eller ett axiom garanterar att objektet måste vara unikt.

3. **Antag att det finns två objekt:** Man antar att det finns två objekt (exempelvis x_1 och x_2) som har den egenskap som krävs, och sedan visar man att de måste vara lika. Detta kan man visa antingen med direkt eller indirekt bevis.

Många gånger kan man både hitta ett entydigt uttryck och börja med att anta att det finns två objekt. Det är en smaksak vad man föredrar. Kan man hitta ett generellt argument som garanterar entydigheten kan man ofta klara sig med ett mycket kort bevis.

Jag börjar med att ge ett exempel där vi hittar ett **entydigt uttryck** för att visa entydigheten. Problemet är hämtat från Solows bok ([13], s. 105-108).

Proposition:
Om a, b, c, d, e och f är reella tal sådana att $ad - bc \neq 0$ då finns det ***unika*** *reella tal x och y sådana att $ax + by = e$ och $cx + dy = f$.*

Först måste vi egentligen visa att talen x och y existerar, men det hoppar vi över här. Istället koncentrerar vi oss på att visa att x och y är unika. Vi har antagandet och påståendet:

A: a, b, c, d, e och f är reella tal, sådana att $ad - bc \neq 0$

P: Då finns det unika reella tal x och y sådana att $ax + by = e$ och $cx + dy = f$.

BEVIS GENOM ENTYDIGT UTTRYCK:
Vi har alltså två ekvationer att utgå från:
(1): $ax + by = e$
(2): $cx + dy = f$

Genom några algebraiska operationer på ekvation (1) löser vi ut x, och får en ny ekvation
(3): $x = \frac{e-by}{a}$.

Om vi sätter in detta resultat i ekvation (2) finner vi att $y = \frac{af-ce}{ad-bc}$. Detta kan vi skriva, eftersom vi enligt antagandet har att $ad - bc \neq 0$.
Detta uttryck för y sätter vi sedan in i ekvation (3), och får efter några omflyttningar och förenklingar ett entydigt uttryck för x: $x = \frac{de-bf}{ad-bc}$.

Vi har alltså till slut följande resultat:

$$x = \frac{de - bf}{ad - bc} \quad \text{och} \quad y = \frac{af - ce}{ad - bc}$$

Eftersom uttrycken för x och y båda är entydiga (uttryckta i variablerna $a,\ b,\ c,\ d,\ e$ och f), innebär detta att för varje val av reella tal a, b, c, d, e och f, sådana att $ad - bc \neq 0$, så kommer x och y att vara unika!

Jag ger nu ytterligare ett exempel, där en annan sats visas både genom ett **generellt argument** och genom att börja med att anta att det finns **två objekt**.

Proposition:
Om r är ett positivt reellt tal, då finns ett unikt reellt tal x sådant att $x^3 = r$.

I detta bevis behöver man först visa att det reella talet x, för vilket $x^3 = r$, existerar. Här utelämnar jag dock denna del av beviset och går direkt till att visa att x är unikt. Jag antar alltså att jag redan visat att x existerar och uppfyller att $x^3 = r$. Återstår att visa att x är unikt.

BEVIS GENOM GENERELLT ARGUMENT:
Funktionen $f : x \to x^3$ är strängt växande. Det medför att inget funktionsvärde kan antas två gånger. För varje r finns alltså högst ett x sådant att $x^3 = r$. Förutsatt att det finns ett x (som vi i detta fall antar att vi redan har visat) så är detta x alltså unikt.

I detta fall behövs således inga beräkningar, utan vi utgår bara från funktionens egenskaper för att kunna fastställa att x måste vara unik.

BEVIS GENOM ANTAGANDE ATT DET FINNS TVÅ OBJEKT:
Nu antar vi istället att det finns två olika objekt som uppfyller att $x^3 = r$. Vi kan t.ex anta att vi har $x^3 = r$ och $y^3 = r$. I så fall kan vi också skriva $x^3 = y^3$ (eftersom $r = r$), vilket ger att $x^3 - y^3 = 0$.
Genom faktoruppdelning får vi $(x - y)(x^2 + xy + y^2) = 0$.
Kvadratkomplettering ger

$$(x - y)((x + \frac{y}{2})^2 + \frac{3}{4}y^2) = 0$$

Någon av faktorerna måste vara noll. Antingen är $(x - y) = 0$. I så fall innebär det att $x = y$, och vi ha visat entydigheten.
Eller så är

$$((x + \frac{y}{2})^2 + \frac{3}{4}y^2) = 0$$

Eftersom detta är en summa av två icke-negativa tal, så måste vi ha att båda talen är noll, för att likheten ska kunna gälla. Vi får alltså att $(x + \frac{y}{2}) = 0$ och samtidigt att $y = 0$, vilket i sin tur ger att $x = 0$, dvs $x = y$. Vi har återigen visat entydigheten!

Observera att vi använt olika hjälptekniker för att manipulera ekvationen för att få det resultat vi strävar mot!

Ovanstående är ett **direkt bevis**, men satsen kan också bevisas genom ett **indirekt bevis** som bygger på antagandet att det finns två objekt.

Återigen antar vi att $x^3 = r$ och $y^3 = r$, men dessutom antar vi att $x \neq y$. Till en början inleder vi precis som nyss, och får att

$$(x - y)((x + \frac{y}{2})^2 + \frac{3}{4}y^2) = 0$$

Eftersom vi antagit att $x \neq y$, dvs att $x - y \neq 0$, kan vi dela båda sidor med $(x - y)$ och får:

$$((x + \frac{y}{2})^2 + \frac{3}{4}y^2) = 0$$

Precis som ovan ger detta att $x = y = 0$, vilket är en motsägelse till vårt antagande att $x \neq y$, och alltså har vi återigen visat entydigheten!

KOMMENTARER:
Detta exempel visar att det inte alltid krävs särskilt omfattande beräkningar för att påvisa entydighet, och att man kan nå samma resultat på flera olika sätt.

*"**Erfarenhet är inte vad som händer oss, utan vad vi gör av det som händer oss.**"*

Aldous Huxley, 1894-1963, brittisk författare

4.2 Kvantifikatorer

Inom matematiken är det vanligt med så kallade **kvantifikatorer**. Dessa kan vara **universella**, dvs av typen "för alla", eller **existentiella**, dvs av typen "det finns". Några exempel där kvantifikatorer används i ett påstående är:

- Ett reellt tal x^* är ett maximum till funktionen f om och endast om det ***för varje*** reellt tal x gäller att $f(x) \leq f(x^*)$.
- Ett reellt tal r är rationellt om och endast om ***det finns*** heltal p och q med $q \neq 0$ sådana att $r = p/q$.

Observera att när man arbetar med kvantifikatorer är det mycket viktigt att definiera det "universum" där varje variabel finns. Ett bra tips är att alltid tydligt skriva ner definitionen för varje variabel. Ett universum kan t.ex vara mängden av reella tal, $\mathbb{R}$, eller alla naturliga tal, $\mathbb{N}$. Ibland är universum en definierad mängd, t.ex $S = \{x > 5 : x \in \mathbb{R}\}$, dvs mängden S består av alla reella tal som är större än 5.

4.2.1 Existens: "Det finns"

Relativt många matematiska satser är på formen "*Det finns ett tal x som uppfyller att...*". För att bevisa sådana satser måste man visa att det finns ett tal x som har de egenskaper som satsen säger. Observera dock att det räcker att visa att det finns **minst ett** sådant tal x!

För att göra detta finns det i princip tre metoder:

1. **Konstruktion:** Genom att konstruera ett exempel på ett objekt (t.ex ett tal) som har de egenskaper som satsen säger, visar man att det faktiskt finns ett sådant objekt (tal).
2. **Generellt argument:** Genom ett generellt argument, t.ex ett axiom, visar man att det måste finna ett sådant objekt som satsen anger. Ett par exempel på sådana användbara generella argument är Välordningsprincipen samt Supremumaxiomet.
3. **Bevis:** Med hjälp av någon bevismetod (se kapitel 3) visar man att det måste finnas ett sådant objekt som satsen anger.

Jag vill göra läsaren uppmärksam på att det finns stora likheter i metodiken för bevis av existens och bevis av entydighet.

Jag ger nu några exempel på tillämpningar av dessa tre metoder. Först ett par exempel där vi använder **konstruktion**. Det första är hämtat från Cupillari ([3], s.55-56).

SATS:
Mellan två olika godtyckliga rationella tal finns ett annat rationellt tal.

BEVIS GENOM KONSTRUKTION:
Om a och b är två olika rationella tal, kan vi skriva dem på formen: $a = m/n$ och $b = p/q$, där m, n, p, q är heltal och $n \neq 0$ samt $q \neq 0$.

Eftersom medelvärdet av två tal alltid ligger mellan de två talen (bevisas inte här), så kan vi konstruera medelvärdet av dessa två tal:

$$c = \frac{a+b}{2} = \frac{1}{2}(\frac{m}{n} + \frac{p}{q}) = \frac{mq+np}{2nq}$$

Talet $mq + np$ är ett heltal, eftersom m, n, p, q är heltal. Talet $2nq$ är ett heltal skilt från 0, eftersom $n \neq 0$ och $q \neq 0$. Talet c är alltså ett rationellt tal som ligger mellan de två rationella talen a och b, och beviset är klart.

Ett annat exempel har jag hämtat från Garnier & Taylor ([5], s. 187).

SATS:
Vissa primtal är på formen $32n + 1$*, där* n *är ett heltal.*

BEVIS GENOM KONSTRUKTION:
Det räcker att vi kan hitta ett exempel då satsen är sann.
Om vi listar alla tal som kan skrivas på formen $32n + 1$, så får vi:
$1, 33, 65, 97, 129, 161, 193, \ldots$

Är det något av dessa tal som är ett primtal?
Talet 1 är per definition inte ett primtal.
$33 = 3 \times 11$, så 33 är inte ett primtal.
$65 = 5 \times 13$, så 65 är inte ett primtal.
Men talet 97 är ett primtal.

Vårt bevis blir alltså:

$97 = 32 \times 3 + 1$ och 97 är som bekant ett primtal.

Som synes är dessa exempel ganska rakt på sak - genom att konstruera ett enda tal som uppfyller kraven, så har vi visat att det faktiskt finns minst ett sådant tal.

Ett enkelt exempel där man använder ett **generellt argument** är följande:

SATS:
Det finns transcendenta tal.

BEVIS GENOM GENERELLT ARGUMENT
Generella argument:
1) De reella talen är överuppräkneliga.
2) De algebraiska talen (dvs mängden av reella tal som utgör en rot till någon ekvation med heltalskoefficienter) är uppräkneliga.

Alltså måste det finnas en icke-tom mängd av reella tal som inte är algebraiska, och vi kallar dem transcendenta tal.

(Den intresserade läsaren rekommenderas att även läsa "På tal om tal" av Lars Nystedt, som där bl.a skriver om transcendenta tal och ger ett bevis genom konstruktion för att det finns sådana tal; [7], s.161-166.)

Slutligen ger jag ett exempel där man använder en vanlig **bevismetod** - i detta fall ett indirekt bevis genom motsägelse. Detta har jag hämtat från Garnier & Taylor ([5], s. 192-193) samt från Daepp & Gorkin ([4], s.59).

SATS:
Det finns primtal som är större än 10^{100}.

BEVIS GENOM MOTSÄGELSE:
Talet 10^{100} är så stort att det faktiskt överstiger det uppskattade antalet atomer i den synliga delen av universum (som uppskattas till cirka 10^{79}). Var och en inser att det skulle vara mycket svårt att direkt kontrollera om det finns primtal som är större än detta tal.

Därför måste vi använda en annan metod än tidigare. Vi provar här med ett motsägelsebevis:

För att få en motsägelse antar vi att det **inte** finns primtal som är större

än 10^{100}. Det innebär att varje primtal p uppfyller att $2 \leq p \leq 10^{100}$. I så fall kan det bara finnas ändligt många primtal. Om det bara finns ändligt många primtal kan vi skriva upp dem i stigande ordning:

$$2, 3, 5, 7, \ldots, N \qquad (N \leq 10^{100})$$

Vi antar alltså att N är det största primtalet som finns.
Nu konstruerar vi ett nytt tal M:

$$M = (2 \cdot 3 \cdot 5 \cdot 7 \cdots N) + 1$$

Om M i sig själv är ett primtal så får vi direkt en motsägelse eftersom $M > N$, och då är satsen sann.

Enligt Aritmetikens fundamentalsats så har alla heltal $a > 1$ en unik primtalsfaktorisering. Om M inte är ett primtal i sig själv så måste det alltså vara delbart med ett mindre tal som är ett primtal, dvs något av talen $2, 3, \ldots, N$. Men om vi delar M med något av dessa tal får vi resten 1. Alltså är inget av dessa tal en faktor i M och alltså måste M innehålla en annan primtalsfaktor, som då måste vara större än N.

Detta motsäger återigen vårt antagande att N var det största primtalet, och alltså kan vi dra slutsatsen att det finns primtal som är större än 10^{100}.

Denna del av beviset används för övrigt för att bevisa Euklides sats: *Det finns oändligt många primtal.*

4.2.2 Universalitet: ”För alla”

Den universella kvantifikatorn ”för alla” eller $\forall$ innebär att en viss utsaga sägs vara sann för alla objekt som tillhör en viss mängd, t.ex

För alla heltal x gäller att om x är udda så är x^2 udda.

Det är dock mycket vanligt att kvantifikatorn ”för alla” inte skrivs ut i satsen. Exempelvis kan en sats lyda:

SATS: *Om funktionen f är definierad i ett intervall samt är strängt monoton och kontinuerlig så har dess invers samma egenskaper.*

Här är det underförstått att påståendet gäller för alla funktioner som är definierade på ett intervall och som är strängt monotona samt kontinuerliga. Detta innebär att flertalet satser egentligen är av typen ”för alla”, utan att det skrivs ut. Detta måste man vara observant på.

När det gäller ”det finns” så räcker det att påvisa existensen av **ett** objekt med en viss egenskap, för att visa att satsen är sann. Men när det gäller ”för alla” måste man visa att satsen är sann för **alla** objekt som har en viss egenskap! Och om satsen är av typen ”För alla reella tal...” kan det bli mycket mödosamt att visa! Vi måste alltså hitta en smartare metod.

Det finns två principer som vi kan ha nytta av för denna typ av bevis:

Universal Generalization (U.G.): Vi kan dra en generell slutsats om alla objekt i en viss mängd, baserad på de egenskaper ett **godtyckligt** objekt i mängden har. Detta kan också uttryckas så här:

Om $F(a)$ är sann för ett godtyckligt element a i en viss mängd M, så gäller att $\forall x F(x)$ är sann, om $x \in M$.

Exempel: ”En godtycklig siameskatt är en katt. Därför är alla siameskatter katter.”

Universal Instantiation (U.I.): Vi kan dra en slutsats om ett **speciellt** element i en mängd, baserad på en generell sanning om alla element i mängden. Detta kan också uttryckas så här:

Om $\forall x F(x)$ är sann i en viss mängd M och om a är ett speciellt element i mängden, så är $F(a)$ sann.

Exempel: ”Alla katter är däggdjur, så om Missan är en katt så är hon ett däggdjur.”

I denna typ av bevis handlar det alltid om att på något sätt välja ett objekt att arbeta vidare med. Objektet väljs på olika sätt beroende på om ”för alla” förekommer i antagandet eller i påståendet.

Om ”för alla” förekommer i själva påståendet så väljer man ett **godtyckligt** objekt och försöker bevisa att påståendet är sant för detta godtyckliga objekt. I så fall kan man dra slutsatsen att det även är sant för alla objekt som tillhör den aktuella mängden. Detta är regeln för ”universal generalization”, som jag kallar metoden med generalisering.

Om man istället har ”för alla” i antagandet kan man tryggt förutsätta att antagandet är sant för alla element i den aktuella mängden. Då väljer man ett **speciellt** sådant element (i vissa fall kan man istället välja en speciell delmängd av sådana element) som man tror kan hjälpa en att bevisa att påståendet är sant. Detta är regeln om ”universal instantiation”, som jag kallar metoden med specialisering.

4.2.3 Universalitet: generalisering

Metoden med generalisering används då vi har kvantifikatorn ”för alla” i vårt påstående. Metoden bygger på att om vi lyckas visa att satsen är sann för ett **godtyckligt** element i mängden, så är den också sann för **alla** element i mängden. Vi kan alltså dra en **generell** slutsats om alla element i mängden. Metoden innebär i korthet:

1. Välj ett **godtyckligt** objekt. Skriv ett nytt antagande i framåtprocessen att det godtyckliga objektet uppfyller kraven (t.ex att objektet tillhör en viss mängd.)

2. Arbeta bakåt för att **visa** att påståendet gäller för det godtyckliga objektet.

EXEMPEL:
Om S och T är två mängder definierade genom
$S = \{\text{reella tal } x\text{: } x^2 - 3x + 2 \leq 0\}$
$T = \{\text{reella tal } x\text{: } 1 \leq x \leq 2\}$
då gäller att $S = T$.

(Exemplet är hämtat från Solow ([13], kapitel 5), och omarbetat av mig.)

BEVIS:
1. FÖRSTÅ PROBLEMET
Vårt antagande och påstående är:

A: $S = \{\text{reella tal } x\text{: } x^2 - 3x + 2 \leq 0\}$
och
$T = \{\text{reella tal } x\text{: } 1 \leq x \leq 2\}$

P: $S = T$

Här innehåller vårt påstående inte någon kvantifikator. Men vi ska strax se att när vi kommit en bit in i processen får vi ett påstående som innehåller ”för alla”.

Vi börjar med en nyckelfråga: ”Hur kan jag visa att två mängder är lika?”. Svaret ger oss ett nytt påstående:

P1: $S \subseteq T$, och $T \subseteq S$.

En ny nyckelfråga ger oss ännu ett nytt påstående: ”Hur kan jag visa att en mängd är en delmängd till en annan mängd?”

P2: För alla element $x \in S$ gäller att $x \in T$ (visar att $S \subseteq T$) och för alla element $x \in T$ gäller att $x \in S$ (visar att $T \subseteq S$).

Nu har vi alltså fått ett påstående med kvantifikatorn ”för alla”.

2. GÖR UPP EN PLAN

Påstående **P2** kan egentligen delas upp i två delar;

P2a: För alla element $x \in S$ gäller att $x \in T$ (visar att $S \subseteq T$).

P2b: För alla element $x \in T$ gäller att $x \in S$ (visar att $T \subseteq S$).

Vi arbetar nu vidare med påstående **P2a**. Enligt metoden ska vi då först välja ett godtyckligt element x och skriva ett nytt antagande i framåtprocessen att det valda elementet uppfyller att $x \in S$.

Sedan måste vi visa att x även uppfyller att $x \in T$.

För att arbeta med **P2b** gör man på motsvarande sätt.

3. GENOMFÖR PLANEN

Vi vet att:

$S = \{\text{reella tal } x\text{: } x^2 - 3x + 2 \leq 0\}$

Nu väljer vi ett **godtyckligt** element x från S. Att elementet är godtyckligt innebär att vi **inte antar att det har några andra egenskaper än att det tillhör mängden** S. Vi antar t.ex inte att det element vi valt är det största eller det minsta i mängden, eller att det är jämnt, eller liknande. Vi utgår **bara** från att elementet tillhör S. Vi får nu ett nytt antagande:

A1: $x \in S$

Nu återstår att visa att det godtyckliga elementet x uppfyller kraven, dvs att visa att x tillhör mängden T. Vi skriver detta som ett påstående:

P3: $x \in T$

Nästa nyckelfråga blir nu: ”Hur kan jag visa att ett element (x) tillhör en mängd (T)?”. Svaret är, genom att visa att elementet uppfyller definitionen för mängden, dvs i detta fall:

P4: $1 \leq x \leq 2$

Nyckelfråga: ”Hur kan jag visa att ett objekt (x) ligger mellan två heltal (1 och 2)?” Vi behöver visa att objektet samtidigt uppfyller två olikheter:

P5: $(x - 1) \geq 0$ **och** $(x - 2) \leq 0$

Nu går vi över till framåtprocessen, eftersom vi inte kommer längre med bakåtprocessen.

Enligt vårt antagande A1 har vi att $x \in S$, dvs att x uppfyller definitionen för S:

A2: $x^2 - 3x + 2 \leq 0$

Detta kan vi skriva om. Genom att faktorisera får vi:

A3: $(x-2)(x-1) \leq 0$

Enda sättet att $(x-2)(x-1) \leq 0$ är att den ena termen ≤ 0 och den andra termen ≥ 0, dvs
antingen har vi att $x-2 \geq 0$ och $x-1 \leq 0$
eller att $x-2 \leq 0$ och $x-1 \geq 0$

I det första fallet skulle vi få att $x \geq 2$ **och** $x \leq 1$, vilket är omöjligt. Alltså är det det andra fallet som gäller:

A4: $(x-2) \leq 0$ och $(x-1) \geq 0$

Vi har alltså fått att A4 = P5, och detta gör att denna del av beviset är klar. Vi måste också visa att T är en delmängd av S. Detta lämnas dock som en övning åt läsaren.

4. SE TILLBAKA
Denna metod innebär att vi skapar ett "mönsterbevis" med vars hjälp vi nu kan kontrollera **varje** element i S genom att byta ut x mot vilket reellt tal som helst som finns i S, och kontrollera att även det uppfyller definitionen av T.

I kondenserad form skrivs ovanstående del av beviset så här:
För att visa att $S = T$ visas att $S \subseteq T$ och $T \subseteq S$. För att se att $S \subseteq T$, låt $x \in S$ (ordet "låt" indikerar att vi valt ett objekt). Vi har då att $x^2 - 3x + 2 \leq 0$ och alltså att $(x-2)(x-1) \leq 0$. Detta betyder att antingen $x-2 \geq 0$ och $x-1 \leq 0$ eller också $x-2 \leq 0$ och $x-1 \geq 0$. Det första kan inte gälla, för då skulle $x \geq 2$ och $x \leq 1$. Alltså har vi att $1 \leq x \leq 2$, vilket betyder att $x \in T$. Detta visar att $S \subseteq T$.

4.2.4 Universalitet: specialisering

I föregående avsnitt gick vi igenom hur man kan välja ett godtyckligt objekt när vi får ett **påstående** som innehåller "för alla". I det här avsnittet ska vi istället se hur man gör om det är vårt **antagande** som innehåller kvantifikatorn "för alla".

En stor skillnad mellan dessa två situationer är att om det står "för alla" i antagandet, så kan man i sitt bevis förutsätta att antagandet är sant för **alla** objekt i den aktuella mängden. Vi behöver alltså inte visa det. Metoden

med specialisering innebär att man väljer ut ett **speciellt** objekt i mängden - alltså inte ett godtyckligt objekt. Objektet ska vara speciellt på så sätt att det för oss närmare vårt påstående, som ju är det vi ska visa är sant. I korthet innebär metoden följande:

1. Välj ut ett **speciellt** objekt eller en speciell delmängd som uppfyller kraven enligt antagandet. (Vilket objekt/vilken delmängd man ska välja framkommer ofta genom bakåtprocessen.)

2. Arbeta framåt för att **visa** att detta objekt även uppfyller kraven i påståendet.

EXEMPEL:
Låt ABC vara en triangel och låt P vara skärningspunkten mellan mittpunktsnormalerna till sidorna AB och AC. Då är P medelpunkt i triangelns omskrivna cirkel.

BEVIS:
1. FÖRSTÅ PROBLEMET
Eftersom mittpunktsnormalerna till två sidor i en triangel aldrig kan vara parallella, måste de skära varandra någonstans. Alltså vet vi att det måste finnas en skärningspunkt P mellan de två mittpunktsnormalerna.

Vårt antagande och påstående är:

A: ABC är en triangel och P är skärningspunkten mellan mittpunktsnormalerna till AB och AC.

P: P är medelpunkten i den cirkel som omskriver triangeln ABC.

2. GÖR UPP EN PLAN
Till en början har vi ingen kvantifikator i antagandet eller påståendet, så vi börjar med Solows framåt-bakåtmetod. Om vi stöter på en kvantifikator kan vi använda metoden med generalisering eller specialisering, beroende på situationen.

3. GENOMFÖR PLANEN
Nyckelfråga: Hur kan vi visa att P är medelpunkten i en cirkel? Vi kan visa det genom att visa att det är samma avstånd från P till varje punkt på cirkelns rand:

P1: Avståndet från P till varje punkt på cirkelns rand är detsamma.

Nu kommer vi inte längre, så vi går över till framåtprocessen.

Vad vet vi om mittpunktsnormaler?

För varje punkt på mittpunktsnormalen till AB gäller att avståndet till A är samma som avståndet till B. Och givetvis gäller motsvarande för sidan AC.

Detta skriver vi som ett nytt antagande:

A1:a För varje punkt på mittpunktsnormalen till AB gäller att avståndet till A är samma som avståndet till B.

A1:b För varje punkt på mittpunktsnormalen till AC gäller att avståndet till A är samma som avståndet till C.

Nu har vi två antaganden som innehåller ”för varje”. Vi använder därför metoden med specialisering.

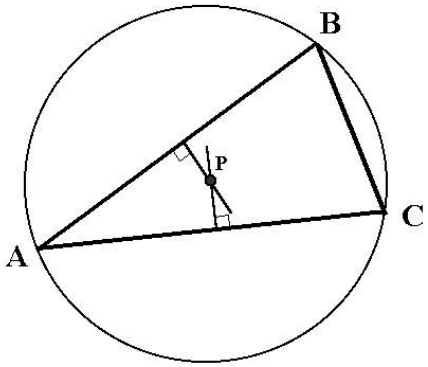
Eftersom antagandena **A1:a** och **A1:b** gäller för varje punkt på respektive mittpunktsnormal, så gäller de även för dessa normalers skärningspunkt, P. Därmed ser vi att:

A2: AP = BP och AP = CP

Alltså kan vi skriva:

A3: AP = BP = CP

Alla hörn i triangeln ligger alltså på samma avstånd från punkten P. Därmed kan vi konstruera en cirkel, vars radie är lika stor som detta avstånd, vars rand tangerar de tre hörnen och vars medelpunkt är punkten P. Och beviset är klart!



4. SE TILLBAKA

Det är värt att nämna att eftersom vi nu ser att BP = CP, så kommer även mittpunktsnormalen till sidan BC att gå genom punkten P, eftersom alla punkter som ligger på samma avstånd från B respektive C ligger på mittpunktsnormalen till sidan. Alltså går alla tre mittpunktsnormalerna genom punkten P.

4.2.5 Blandade kvantifikatorer

I den bästa av världar skulle vi bara stöta på uttryck med endast en kvantifikator. I verkligheten kommer vi dock att tvingas hantera uttryck med flera kvantifikatorer, exempelvis:

För alla *reella tal* x *med* $0 \leq x \leq 1$ ***finns det*** *ett reellt tal* y *med* $-1 \leq y \leq 1$ *sådant att* $x + y^2 = 1$.

När man stöter på blandade kvantifikatorer är det mycket viktigt i vilken ordning de står. Jämför exempelvis dessa två satser:

S1: Det finns ett reellt tal $M \geq 0$ sådant att för alla element $x \in T$ gäller att $x \leq M$.

S2: För alla reella tal $M \geq 0$ finns det ett element $x \in T$ sådant att $x \leq M$.

S1 innebär att det finns ett positivt reellt tal M sådant att oavsett vilket element x vi väljer i T så är $x \leq M$.

S2 å andra sidan innebär att för **varje** reellt tal M kan vi hitta ett element $x \in T$ för vilket $x \leq M$. Observera att formuleringen i **S2** innebär att x kan **bero** av M, dvs om vi ändrar värde på M kan även värdet på x komma att ändras.

Det bör vara tydligt att **S1** och **S2** inte betyder samma sak!

När man har uttryck med blandade kvantifikatorer ska man alltid arbeta **från vänster till höger** enligt de metoder som beskrivits tidigare i detta kapitel.

(Ovanstående är hämtat från Solow ([13], kapitel 7), men översatt och omarbetat av mig.)

EXEMPEL:

För alla reella tal x *med* $0 \leq x \leq 1$ *finns det ett reellt tal* y *med* $-1 \leq y \leq 1$ *sådant att* $x + y^2 = 1$.

BEVIS:

1. FÖRSTÅ PROBLEMET

Vi har följande antagande och påstående:

A: x är ett reellt tal sådant att $0 \leq x \leq 1$.

P: För varje sådant tal x finns det ett reellt tal y med $-1 \leq y \leq 1$, sådant att $x + y^2 = 1$.

2. GÖR UPP EN PLAN

Vi noterar att den första kvantifikatorn i påståendet är "för varje", vilket leder till att vi ska använda generalisering:

1. Välj ett godtyckligt objekt. Skriv ett nytt antagande i framåtprocessen att det godtyckliga objektet uppfyller kraven.
2. Arbeta bakåt för att **visa** att påståendet gäller för det godtyckliga objektet.

Den andra kvantifikatorn är "det finns", vilket innebär att vi t.ex kan prova att konstruera ett objekt som uppfyller kraven.

3. GENOMFÖR PLANEN

Vi börjar alltså med att använda metoden med generalisering på påstående **P1**: För varje sådant tal x finns det ett reellt tal y med $-1 \leq y \leq 1$, sådant att $x + y^2 = 1$.

Vi väljer nu ett godtyckligt exempel på ett sådant reellt tal:

A1: $0 \leq x \leq 1$ och $x \in \mathbb{R}$

Att $0 \leq x \leq 1$ innebär att $0 \leq (1 - x) \leq 1$. Vi skriver detta som ett nytt antagande:

A2: $0 \leq (1 - x) \leq 1$

Därefter övergår vi till bakåtprocessen. För detta tal x måste vi visa att:

P1: Det finns ett reellt tal y med $-1 \leq y \leq 1$, sådant att $x + y^2 = 1$.

Vi försöker konstruera ett tal y.

$x + y^2 = 1$ kan skrivas om till: $y^2 = 1 - x$.
Det i sin tur är ekvivalent med att: $y = \pm\sqrt{1 - x}$.
Vi har alltså konstruerat ett tal y som uppfyller att $x + y^2 = 1$. Vi behöver nu visa att y är reellt med $-1 \leq y \leq 1$.

Vi börjar med att skriva ett nytt påstående:

P2: Det finns ett reellt tal y med $-1 \leq y \leq 1$, sådant att $y = \pm\sqrt{1-x}$.

För att visa att y är reellt och att $-1 \leq y \leq 1$ går vi över till framåtprocessen. Eftersom vi enligt antagande **A2** har att $0 \leq (1-x) \leq 1$, så är $(1-x)$ ett icke-negativt tal, och alltså är $\sqrt{1-x}$ ett reellt tal. Vårt konstruerade tal y är alltså reellt.

Antagande **A2** medför också att $|\pm\sqrt{1-x}| \leq 1$, vilket kan skrivas om till $-1 \leq \pm\sqrt{1-x} \leq 1$.

Sammantaget kan vi nu skriva ett nytt antagande:

A3: $-1 \leq \pm\sqrt{1-x} \leq 1$ och $\sqrt{1-x} \in \mathbb{R}$.

Om vi sätter $y = \pm\sqrt{1-x}$ så har vi alltså visat att y är reellt med $-1 \leq y \leq 1$ - och vi är klara med beviset!

4. SE TILLBAKA

Talet y är alltså ett reellt tal som beror av x. Oavsett hur vi väljer x (så länge $0 \leq x \leq 1$), kan vi enligt satsen hitta ett reellt tal $-1 \leq y \leq 1$ som uppfyller att $x + y^2 = 1$.

I kondenserad form skulle beviset kunna skrivas:

Låt x vara ett reellt tal sådant att $0 \leq x \leq 1$. Detta medför att $0 \leq 1 - x \leq 1$. Att $x + y^2 = 1$ är ekvivalent med att $y = \pm\sqrt{1-x}$. Eftersom $0 \leq 1 - x \leq 1$ är y ett reellt tal med $-1 \leq y \leq 1$.

Som framgår av detta exempel så kan vi även bevisa satser som innehåller blandade kvantifikatorer. Huvudregeln är att behandla varje kvantifikator för sig i den ordning de uppträder, från vänster till höger, så reder det ut sig!

Kapitel 5

Kommenterade bevis

*"**Sjömannen ber inte om medvind - han lär sig segla.**"*
Gustaf Lindborg, 1875-1927, matematiker och författare

5.1 Inledning

Detta kapitel syftar till att visa bevisen för några kända satser där bevisen innehåller flera bevismetoder eller av andra skäl är illustrativa. Bevisen är rikt kommenterade och strukturerade enligt Polyas metod.

5.2 Divisionsalgoritmen

Divisionsalgoritmen har en stor betydelse inom matematiken, och därför kan det vara intressant att i detalj gå igenom beviset för denna sats. Jag har hämtat satsen och beviset från Beachy och Blair ([1], s. 7), med min egen översättning och rikliga egna omarbetningar.

SATS: Divisionsalgoritmen.
För två godtyckliga heltal a och b, med $b > 0$, existerar det unika heltal q (kvoten) och r (resten) sådana att $a = bq + r$, med $0 \leq r < b$.

BEVIS.
1. FÖRSTÅ PROBLEMET
Vårt **antagande** är att talen a och b är heltal, och att $b > 0$.
Vårt **påstående** kan delas upp i flera delar:
a) Det existerar två heltal q och r, så att $a = bq + r$
b) För r gäller att $0 \leq r$
c) För r gäller dessutom att $r < b$
d) Slutligen är r och q unika, om de uppfyller a) - c).

2. GÖR UPP EN PLAN
Vi behöver genomföra beviset i flera steg;

1. Vi måste visa att r och q existerar - bevis av existens.
2. Vi måste kontrollera att r uppfyller kraven i vårt påstående.
3. Vi måste visa att om r och q existerar så är de i så fall unika - bevis av entydighet.

3. GENOMFÖR PLANEN
Existensen av r och q
Första delen av beviset går ut på att visa att q och r existerar, och att vi då har att $a = bq + r$. Det räcker att visa att det finns minst **ett** tal r och minst **ett** tal q. Enklaste sättet är ofta att **konstruera** ett exempel på det objekt man ska visa existensen av (se 4.2.1).

Vi börjar med att skriva om sambandet $a = bq + r$ till $r = a - bq$. Betrakta nu mängden $R = \{r = a - bq \mid q \in \mathbb{Z}\}$. Elementen i R är potentiella rester. För att visa att åtminstone ett tal r existerar behöver vi visa att mängden R är icke-tom.

Eftersom vi enligt vårt antagande har att b är ett heltal > 0 medför det att $b \geq 1$. När det gäller q är det enda kravet att q ska vara ett heltal. Vi kan alltså välja q hur vi vill bland alla heltal. Exempelvis kan vi välja $q = -|a|$. Det medför att talet $a - b(-|a|) = a + b \cdot |a|$ tillhör R. Mängden R existerar alltså.

Eftersom $b \geq 1$ kan vi konstatera att talet $a + b \cdot |a|$ är icke-negativt.
Om $a < 0$ så är $a - b(-|a|) \geq 0$.
Om $a = 0$ så är $a - b(-|a|) = 0$.
Om $a > 0$ så är $a - b(-|a|) \geq 2a \geq 0$.

Detta innebär att mängden R innehåller en icke-tom delmängd R^+ som endast innehåller icke-negativa tal, och R^+ är nedåt begränsad.

Vi har nu visat att r och q existerar och uppfyller att $a = bq + r$, och att det finns en mängd med icke-negativa rester.

Kontroll att r uppfyller kraven
Genom välordningsprincipen vet vi att eftersom mängden R^+ existerar så innehåller den också ett minsta element, som vi kallar r. Vi vill visa att $0 \leq r < b$.

Per definition gäller att $r \geq 0$ (eftersom $r \in R^+$), och då måste vi också ha att $r = a - bq$ för något heltal q. Detta vet vi eftersom *alla* tal i R^+ är konstruerade på detta sätt!

Nu vill vi visa att $r < b$. Vi gör då ett indirekt bevis, dvs vi antar att $r \geq b$. Om $r \geq b$ så måste det finns ett annat heltal s, sådant att $s = r - b = a - bq - b = a - b(q + 1) \in R^+$ - eftersom $q + 1$ är ett heltal. Vi har alltså att $s \in R^+$. Då är $s \geq 0$ med $s < r$. Detta är en motsägelse till det sätt som vi valde r, nämligen att r är det minsta talet i R^+. Då kan inte samtidigt gälla att $s < r$. Alltså måste vi ha att $r < b$.

Vi har nu visat att r uppfyller villkoren $0 \leq r$ och $r < b$.

Visa att r och q är unika

För att visa att q och r är unika kan man t.ex börja med att anta att det finns två tal q_1 och q_2, samt två tal r_1 och r_2. Därefter behöver vi visa att $q_1 = q_2$ samt att $r_1 = r_2$ (se avsnitt 4.1).

Vi antar alltså att vi både kan skriva $a = bq_1 + r_1$ och $a = bq_2 + r_2$ för heltalen q_1, q_2, r_1, r_2. Vi har att $0 \leq r_1 < b$ och $0 \leq r_2 < b$, vilket medför att $|r_2 - r_1| < b$. Men $bq_2 + r_2 = bq_1 + r_1$ så $r_2 - r_1 = b(q_1 - q_2)$, vilket visar att b delar $(r_2 - r_1)$.

Enda möjligheten att b kan vara en delare till ett tal som har ett mindre absolutbelopp än b är om detta tal är 0, och alltså måste vi ha att $r_2 - r_1 = 0$, eller $r_2 = r_1$. Då är $bq_2 = bq_1$, vilket medför att $q_2 = q_1$ eftersom $b > 0$. Alltså är kvoten och resten unika, och vi har genomfört beviset av satsen. (Om b hade varit lika med 0 hade vi däremot inte kunnat säga någonting om q_1 och q_2.)

Ett alternativt sätt att visa entydigheten skulle kunna vara enligt följande:

Vi har att $r = a - bq$ där $q \in \mathbf{Z}$. Om vi sätter in heltalsvärden på q kommer vi att få en aritmetisk talföljd som är obegränsad åt båda hållen enligt följande:

$$\ldots a + 2b \quad a + b \quad a \quad a - b \quad a - 2b \quad a - 3b \ldots$$

Talet r är ett av dessa tal. Eftersom differensen mellan två på varandra följande tal är b finns det i denna följd bara en representant för mängden av tal r i intervallet [0,b). Villkoret $0 \leq r < b$ gör då att r är unikt, och därmed är också q unikt (genom sambandet $r = a - bq$).

4. SE TILLBAKA

I ovanstående bevis har vi visat existensen av q och r, vi har använt oss av en hjälpmängd för att sedan kunna använda välordningsprincipen och indirekt bevis för att visa att talet r uppfyller kraven. När vi väljer r som det minsta elementet i R^+ är detta ett exempel på specialisering. Vi har också visat entydighet på två olika sätt, och då i ena fallet använt ett hjälptal (s). Detta om något är ett exempel på att de olika tekniker och metoder som används för att bevisa matematiska satser inte är ömsesidigt uteslutande utan tvärtom kompletterar varandra på ett mycket bra sätt!

Som jämförelse har jag här kopierat det kondenserade bevis som ges i Beachy och Blair ([1], s. 7):

"Betrakta mängden $R = \{a - bq | q \in \mathbf{Z}\}$. Elementen i R är de potentiella resterna, och bland dessa behöver vi finna det minsta icke-negativa elementet. Vi vill tillämpa välordningsprincipen på mängden R^+ av icke-negativa heltal i R, så vi måste först visa att R^+ är icke-tom. Eftersom $b \geq 1$, är talet $a - b(-|a|) = a + b \cdot |a|$ icke-negativt och tillhör R^+.

Genom välordningsprincipen har R^+ ett minsta element, som vi kallar r. Vi ska visa att $a = bq + r$, med $0 \leq r < b$. Per definition är $r \geq 0$, och eftersom $r \in R^+$ måste vi ha att $r = a - bq$ för något heltal q. Om $r \geq b$ då är $s = r - b = a - b(q + 1) \in R^+$ och alltså är $s \geq 0$ med $s < r$. Detta motsäger definitionen av r, så vi måste ha att $r < b$. Vi har nu bevisat existensen av r och q, och att dessa uppfyller villkoret att $a = bq + r$, med $0 \leq r < b$.

För att visa att q och r är unika, antag att vi också kan skriva $a = bp + s$ för heltalen p och s med $0 \leq r < b$, och detta ger att $|s - r| < b$. Men $bp + s = bq + r$ och alltså är $s - r = b(q - p)$, vilket visar att b delar $(s - r)$. Enda sättet som b kan vara den delare till ett tal med mindre absolutbelopp är om det talet är 0, så vi måste ha att $s - r = 0$, eller att $s = r$. Då är $bp = bq$, vilket ger att $p = q$ eftersom $b > 0$. Alltså är kvoten och resten unika, och vi har slutfört beviset."

5.3 Aritmetikens fundamentalsats

Jag ger nu exempel på ett motsägelsebevis, beviset för aritmetikens fundamentalsats, hämtat från Beachy och Blair ([1], s.17-18), med min översättning och vissa omskrivningar.

I detta bevis måste vi använda oss av ett lemma, som jag skriver ut men inte bevisar här. Det kompletta beviset finns i Beachy och Blair ([1], Lemma 1.2.5, sid 17). Dessutom kommer vi att använda oss av välordningsprincipen som beskrivs mer i detalj i avsnitt 3.5.2.

SATS; ARITMETIKENS FUNDAMENTALSATS:
Varje heltal $a > 1$ kan ges en unik primtalsfaktorisering, på formen

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$$

där $p_1 < p_2 < \cdots < p_n$ och exponenterna $\alpha_1, \alpha_2, \ldots, \alpha_n$ alla är positiva.

LEMMA; EUKLIDES LEMMA:
Ett heltal $p > 1$ är ett primtal om och endast om det upfyller följande egenskap: Om p delar ab för heltalen a och b, då gäller att p delar a eller b.

[*Observera att inom matematiken betyder "eller" egentligen "och/eller", så i detta fall ska sista bisatsen läsas "då gäller att p delar a* ***och/eller*** *b".*]

BEVIS:
1. FÖRSTÅ PROBLEMET
Vårt **antagande** är att vi endast studerar heltal som är större än 1. Vårt **påstående** är att alla sådana heltal kan ges en unik primtalsfaktorisering, på den form som ges i satsen.

2. GÖR UPP EN PLAN
Satsen kan lätt skrivas om, för att dela upp problemet:
För varje heltal $a > 1$ gäller att a har en unik primtalsfaktorisering...

Detta kan delas upp i två uppgifter:

1. Bevisa att varje heltal $a > 1$ har en primtalsfaktorisering - bevis av universalitet.

   (Eftersom ett heltal antingen har eller inte har en primtalsfaktorisering, bör detta vara ett bra tillfälle att använda motsägelsebevis.)

2. Bevisa att denna primtalsfaktorisering är unik - bevis av entydighet.

3. GENOMFÖR PLANEN

Varje heltal $a > 1$ har en primtalsfaktorisering

Om man vill genomföra ett direkt bevis av universalitet kan man använda metoden med generalisering, som beskrivs i avsnitt 4.2.3. Men här provar vi att genomföra ett indirekt bevis.

För detta måste vi bestämma negationen till "Varje heltal $a > 1$ har en primtalsfaktorisering". Negationen blir "Det finns ett heltal $a > 1$ som saknar primtalsfaktorisering".

Antag alltså att det finns ett heltal som **inte** kan skrivas som en produkt av primtal. I så fall måste mängden av tal $a > 1$ utan primtalsfaktorisering vara icke-tom, och enligt välordningsprincipen (se avsnitt 3.5.2) innehålla ett minsta tal, säg b.

[*Kommentar: Här använder vi oss både av välordningsprincipen och metoden med specialisering, eftersom talet b är en specialisering av alla tal som saknar primtalsfaktorisering.*]

b kan inte själv vara ett primtal, för då skulle det ha en primtalsfaktorisering. Alltså är b ett sammansatt tal, och vi kan skriva $b = cd$ för heltalen c och d som båda är mindre än b.

Genom vårt antagande att b är det minsta talet utan primtalsfaktorisering måste både c och d ha en sådan faktorisering, vilket medför att även b har en primtalsfaktorisering. Men detta är återigen en motsägelse mot vårt antagande att b saknar primtalsfaktorisering.

Vi kan alltså konstatera att det inte finns några tal $b > 1$ som saknar primtalsfaktorisering, och alltså måste det stämma att alla tal $a > 1$ har en primtalsfaktorisering. Eftersom multiplikation är kommutativ kan faktorerna sedan ordnas så att vi uppfyller att $p_1 < p_2 < \cdots < p_n$.

Denna primtalsfaktorisering är unik

För att visa entydigheten av ett objekt kan man t.ex börja med att anta att det finns **två** objekt, och sedan visa att de måste vara lika (se avsnitt 4.1). Här skulle vi kunna använda ett motsägelsebevis för att visa att dessa två objekt egentligen är lika.

Om det existerar ett heltal > 1 som **inte** har en unik faktorisering, så säger välordningsprincipen (se avsnitt 3.5.2) att det måste finnas ett minsta sådant tal, säg a. Antag att a har **två** primtalsfaktoriseringar;

$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ och $a = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$,
där $p_1 < p_2 < \cdots < p_n$ och $q_1 < q_2 < \cdots < q_m$,

med $\alpha_i > 0$ för $i = 1, \ldots, n$ och $\beta_j > 0$ för $j = 1, \ldots, m$.

Vi får alltså att $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m}$

Det innebär att p_1 delar det högra ledet. Enligt Euklides lemma vet vi då att p_1 delar q_j för något j med $1 \leq j \leq m$. Men eftersom q_j är ett primtal måste $p_1 = q_j$.

[*Kommentar: Egentligen använder vi här en generalisering av Euklides lemma, som ju endast behandlar fallet med två faktorer. Generalisering kan visas genom induktion.*]

På samma sätt innebär ovanstående likhet att q_1 delar det vänstra ledet, och att q_1 därmed delar p_k. Vi inser som tidigare att $q_1 = p_k$.

Men eftersom $q_1 \leq q_j = p_1 \leq p_k = q_1$, så får vi att $j = k = 1$, dvs att $q_1 = p_1$.

Alltså kan vi sätta

$$s = \frac{a}{p_1} = \frac{a}{q_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = q_1^{\beta_1 - 1} q_2^{\beta_2} \ldots q_m^{\beta_m}$$

Om $s = 1$ har vi att $a = p_1 = q_1$, och då har a en unik primtalsfaktorisering (eftersom $p_1 = q_1$ i så fall), vilket motsäger vårt val av a.

Om $s > 1$, då har vi att eftersom $s < a$ och s har två faktoriseringar så får vi återigen en motsägelse till valet av a.

Slutsatsen blir alltså att a faktiskt har en unik primtalsfaktorisering.

(Observera att s inte kan vara < 1. Varför?)

4. SE TILLBAKA

Detta bevis innehåller både bevis av universalitet (satsen gäller för alla heltal $a > 1$) och bevis av entydighet (primtalsfaktoriseringen är unik). I båda delarna av beviset kunde vi använda motsägelsebevis för att visa universalitet respektive entydighet.

5.4 Geometriskt och aritmetiskt medelvärde

Nedanstående satser är hämtade från Hyltén-Cavallius & Sandgren, ([6], sid 41-42), men jag ger här en variant på deras bevis för Sats 2. Satserna visar tillsammans att det geometriska medelvärdet alltid är mindre än eller lika med det aritmetiska medelvärdet, för samma talföljd.

Det aritmetiska medelvärdet är det "vanliga" medelvärdet, och det skrivs:

$$A = \frac{a_1 + a_2}{2} = \frac{1}{2}(a_1 + a_2)$$

Det geometriska medelvärdet (där $a_1 > 0$ och $a_2 > 0$) skrivs:

$$G = (a_1 a_2)^{\frac{1}{2}}$$

SATS 1:
Om $a_1 > 0$ och $a_2 > 0$ *så gäller att* $G \leq A$, *med likhet om och endast om* $a_1 = a_2$.

BEVIS:
Eftersom Sats 1 här endast fungerar som hjälpsats till Sats 2 nedan, så går jag inte igenom beviset i detalj, utan återger det bara i korthet. Vi kan skriva:

$$A - G = \frac{1}{2}(a_1 + a_2) - (a_1 a_2)^{\frac{1}{2}} = \frac{1}{2}(a_1 + a_2 - 2\sqrt{a_1 a_2}) = \frac{1}{2}(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$$

dvs vi har att $A \geq G$. Om $a_1 = a_2 = x$ får vi likhet, eftersom

$$A - G = \frac{1}{2}(x + x - 2\sqrt{x^2}) = \frac{1}{2}(2x - 2x) = 0$$

SATS 2:
Om $a_v \geq 0, \quad v = 1, 2, \ldots, n$ *så är*

$$(a_1 a_2 \ldots a_n)^{\frac{1}{n}} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}$$

Kommentar: Satsen betyder att $G(a_1, \ldots, a_n) \leq A(a_1, \ldots, a_n)$. Skrivsättet $G(a_1, \ldots, a_n)$ ska utläsas "det geometriska medelvärdet av talen a_1 till a_n".

Ovanstående olikhet kan också skrivas som:

$$a_1 a_2 \dots a_n \leq \left(\frac{a_1 + a_2 + \dots + a_n}{n} \right)^n$$

BEVIS:

1. FÖRSTÅ PROBLEMET:

Vårt **antagande** är att vi har n stycken termer $(a_1, a_2, \dots, a_n)$.

Vårt **påstående** är att i så fall är det geometriska medelvärdet alltid mindre än eller lika med det aritmetiska medelvärdet för dessa tal.

2. GÖR UPP EN PLAN:

Eftersom antalet termer alltid måste vara ett naturligt tal, så skulle det kunna vara intressant att se vad vi kan åstadkomma med ett induktionsbevis.

Basen måste i så fall vara $n = 2$. Sats 1 säger oss att om $n = 2$ så gäller olikheten. Vi vet alltså redan att

$$(a_1 a_2)^{\frac{1}{2}} \leq \frac{1}{2}(a_1 + a_2)$$

Detta är ekvivalent med att

$$(a_1 a_2) \leq \left(\frac{a_1 + a_2}{2} \right)^2$$

På samma sätt vet vi att

$$(a_3 a_4) \leq \left(\frac{a_3 + a_4}{2} \right)^2$$

Ovanstående gör att vi kan sluta oss till att

$$a_1 a_2 a_3 a_4 \leq \left(\frac{a_1 + a_2}{2} \right)^2 \cdot \left(\frac{a_3 + a_4}{2} \right)^2 = (xy)^2$$

där $x = \frac{a_1 + a_2}{2}$ och $y = \frac{a_3 + a_4}{2}$.

Förnyad användning av olikheten $xy \leq (\frac{x+y}{2})^2$ ger att

$$a_1 a_2 a_3 a_4 \leq \left(\frac{a_1 + a_2 + a_3 + a_4}{4} \right)^4$$

Sats 1 verkar säkerställa att sambandet $G \leq A$ gäller om antalet termer är en 2-potens. Låt oss försöka bevisa detta genom induktion.

3. GENOMFÖR PLANEN:
Induktionsbas:
Sats 1 säger oss att om $n = 2$ så gäller sambandet.

Induktionsantagande:
Antag att sambandet gäller för $n = k$

Induktionssteg:
Vi vill visa att sambandet då även gäller för $n = 2k$. [Kommentar: pga att basen är 2, och pga att vi visar induktion för $n = 2k$ kommer vi att visa att satsen gäller då antalet termer är en 2-potens; basfallet är $n = 2$, nästa steg är $n = 2 \cdot 2$, nästa steg är $n = 2 \cdot 2 \cdot 2$ osv.]
Vi vill alltså visa att:
$G(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}) \leq A(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k})$

Detta är ekvivalent med att visa att:
$(G(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}))^{2k} \leq (A(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}))^{2k}$

Vi får att:

$$\begin{aligned}
(G(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}))^{2k} &= \left((a_1 \cdots a_k)^{1/(2k)} \cdot (a_{k+1} \cdots a_{2k})^{1/(2k)}\right)^{2k} \\
&= (a_1 \cdots a_k) \cdot (a_{k+1} \cdots a_{2k}) \\
&\leq \left(\frac{a_1 + \cdots + a_k}{k}\right)^k \left(\frac{a_{k+1} + \cdots + a_{2k}}{k}\right)^k \\
&\quad [\textit{Enligt induktionsantagandet}] \\
&= \left(\left(\frac{a_1 + \cdots + a_k}{k}\right) \cdot \left(\frac{a_{k+1} + \cdots + a_{2k}}{k}\right)\right)^k \\
&\leq \left(\left(\frac{\frac{a_1 + \cdots + a_k}{k} + \frac{a_{k+1} + \cdots + a_{2k}}{k}}{2}\right)^2\right)^k \\
&\quad [\textit{Enl. induktionsbasen}] \\
&= \left(\frac{a_1 + \cdots + a_{2k}}{2k}\right)^{2k} = (A(a_1, \ldots, a_{2k}))^{2k}
\end{aligned}$$

Slutsats:
Alltså har vi visat att $G(a_1, \ldots, a_{2k}) \leq A(a_1, \ldots, a_{2k})$, där $2k$ är en 2-potens ($2k = 2, 4, 8 \ldots$).

[*Kommentar: I den ursprungliga Sats 1 är a_1 och a_2 godtyckliga. Här ovan använder vi specialisering och sätter $a_1 = \frac{a_1 + \cdots + a_k}{k}$ och $a_2 = \frac{a_{k+1} + \cdots + a_{2k}}{k}$*]

Men hur är det om n inte är en 2-potens, utan ett godtyckligt tal? En tänkbar lösning är att även här använda induktionsbevis, men försöka visa att om sambandet gäller då $n = m$ så gäller det också då $n = m-1$. I så fall kan vi täcka in alla tänkbara fall om vi sätter $m = 2k$, och sedan "stegar" oss bakåt ett steg i taget.

Tillsammans ger dessa två induktionsbevis då att sambandet $G \leq A$ gäller för alla talföljder!

Induktionsbas:
$n = 2k$; visades i föregående del av beviset.

Induktionsantagande:
Antag att sambandet gäller för $n = m$.

Induktionssteg:
Visa att sambandet då även gäller för $n = m - 1$.

Talen $a_1, a_2, \ldots, a_{m-1}$ är givna, men för att kunna använda vårt induktionsantagande behöver vi även ett m:te tal (där $m = 2k$ för något k) så att vi kan utnyttja resultatet från det föregående induktionsbeviset. Vi konstruerar därför ett **hjälptal** b, genom att låta b vara lika med medelvärdet av alla talen a_1 till a_{m-1}:

$$b = \frac{a_1 + \cdots + a_{m-1}}{m-1} = A(a_1, \ldots, a_{m-1})$$

Eftersom b är lika med medelvärdet för alla talen a_1 till a_{m-1}, så gäller även att:

$$b = A(a_1, \ldots, a_{m-1}, b)$$

dvs att b även är lika med medelvärdet av alla talen a_1 till a_{m-1} samt talet b.

Enligt vårt induktionsantagande har vi då att:

$$b = A(a_1, \ldots, a_{m-1}, b) \geq G(a_1, \ldots, a_{m-1}, b) = (a_1 \cdot \cdots \cdot a_{m-1} \cdot b)^{1/m}$$

$$\Updownarrow$$

$$b^m \geq \left((a_1 \cdot \cdots \cdot a_{m-1} \cdot b)^{1/m}\right)^m = a_1 \cdot \cdots \cdot a_{m-1} \cdot b$$

$$\Updownarrow$$

$$b^{m-1} \geq a_1 \cdot \cdots \cdot a_{m-1}$$

$$\Updownarrow$$

$$b \geq (a_1 \cdot \cdots \cdot a_{m-1})^{1/(m-1)} = G(a_1, \ldots, a_{m-1})$$

$$\Updownarrow$$

$$A(a_1, \ldots, a_{m-1}) \geq G(a_1, \ldots, a_{m-1})$$

Slutsats:
Därmed har vi visat att sambandet $G \leq A$ gäller för en följd med ett godtyckligt antal tal.

4. SE TILLBAKA:
Observera att den senare delen av detta bevis är en "bakvänd" induktion, på så sätt att vi stegar oss nedåt istället för uppåt. Vi börjar med att anta att satsen är sann för $n = m = 2k$ för något k (dvs att antalet termer är en godtycklig 2-potens).

Sedan visar vi att i så fall är den även sann för $n = m - 1$.

Därefter kan vi dra slutsatsen att satsen faktiskt är sann för all talföljder med färre än $2k$ termer i följden - och alltså är satsen sann för **alla** följder!

Den intresserade rekommenderas att även läsa igenom beviset som ges av Hyltén-Cavallius & Sandgren, [6].

5.5 Diskontinuerliga funktioner

Nedanstående bevis är ett ganska enkelt, men elegant bevis som visar hur man i ett direkt bevis kan ha användning av olika hjälpstorheter.

Satsen och beviset är hämtat från Rudin ([12], s.96-97), med min översättning och mina omarbetningar.

SATS:
Låt f vara monoton på (a,b). Då är mängden av punkter som tillhör (a,b) och där f är diskontinuerlig som mest uppräknelig.

BEVIS:
1. FÖRSTÅ PROBLEMET:
Vårt **antagande** är att f är monoton på intervallet (a, b).
Vårt **påstående** är att då är mängden av punkter som tillhör (a,b) och där f är diskontinuerlig som mest uppräknelig.

2. GÖR UPP EN PLAN:
Det finns inga speciella "konstigheter" i denna sats som gör att vi behöver något speciellt knep, utan vi provar att göra ett direkt bevis.

3. GENOMFÖR PLANEN:
Enligt Solows framåt-bakåtmetod så börjar vi att arbeta från påståendet.

Nyckelfråga: Hur kan vi visa att en mängd är som mest uppräknelig?
Ett sätt är att visa att det finns en injektion från mängden till en annan uppräknelig mängd - t.ex mängden av rationella tal. [*Varför vi väljer just de rationella talen kommer att framgå senare.*]

Antag för enkelhets skull att f är monotont växande.
Låt E vara mängden av punkter där f är diskontinuerlig.
[*Här inför vi mängden E som en* ***hjälpmängd****.*]

Till varje punkt $x \in E$ associerar vi ett rationellt tal $r(x)$ sådant att $f(x^-) < r(x) < f(x^+)$. [*Talen $r(x)$ är på samma sätt* ***hjälptal****.*]

[*Nu framgår varför det är bättre att välja de rationella talen som jämförelsemängd, istället för t.ex de naturliga talen. De två talen $f(x^-)$ och $f(x^+)$ är reella. Mellan två reella tal kan man alltid finna ett rationellt tal. Faktum är att det finns oändligt många rationella tal mellan två reella tal. Genom specialisering väljer vi ett av dessa tal, och kallar det r(x).*

Hade vi istället valt att jämföra med de naturliga talen hade det blivit knepigare - då hade vi varit tvungna att hitta någon form av funktion som skulle kunna koppla varje diskontinuerlig punkt till ett naturligt tal.

Genom att koppla varje diskontinuerlig punkt till ett rationellt tal får vi istället ett enkelt samband mellan de diskontinuerliga punkterna och de rationella talen.]

Eftersom olikheten $x_1 < x_2$ medför att $r(x_1) < f(x_1^+) \leq f(x_2^-) < r(x_2)$ inser vi att om $x_1 \neq x_2$, så är $r(x_1) \neq r(x_2)$. Alltså kan vi betrakta funktionen $r(x)$ som en injektion mellan mängden E och mängden av rationella tal. De rationella talen är uppräkneliga, och alltså är E högst uppräknelig.

4. SE TILLBAKA:
Samma resonemang kan genomföras om f är monotont avtagande.

5.6 Taylors sats

Nedanstående sats och bevis är hämtade från Rudin ([12], s. 110-111), med min översättning och mina omarbetningar.

Jag har valt att ta med Taylors[1] sats pga att den dels är en "viktig" sats inom matematisk analys, och dels pga att den är ett intressant exempel på hur man visar existens genom att använda ett antal olika hjälpstorheter, samt genom dold induktion.

SATS:

Antag att f är en reell funktion på [a,b], n är ett positivt heltal, $f^{(n-1)}$ *är kontinuerlig på [a,b],* $f^{(n)}(t)$ *existerar för varje* $t \in (a, b)$.

Låt α, β *vara olika punkter på [a,b] och definiera:*

$$P(t) = \sum_{k=0}^{n-1} \frac{f^{(k)}(\alpha)}{k!}(t-\alpha)^k \tag{5.1}$$

Då existerar det en punkt x mellan α *och* β *sådan att*

$$f(\beta) = P(\beta) + \frac{f^{(n)}(x)}{n!}(\beta-\alpha)^n \tag{5.2}$$

BEVIS:

1. FÖRSTÅ PROBLEMET:

Observera till att börja med att $P(t)$ är det så kallade Taylor-polynomet av ordning $n-1$. Taylors sats visar att f kan uppskattas med ett polynom av grad $n-1$, och att vi genom ekvation (5.2) kan uppskatta felet om vi känner till begränsningen av $|f^{(n)}(x)|$.

Större delen av satsen utgörs av själva **antagandet**, som är ovanligt väl specificerat i denna sats.

Själva **påståendet** är: Det existerar en punkt x mellan α och β sådan att (5.2) uppfylls.

2. GÖR UPP EN PLAN:

Vi ska alltså visa existensen av ett tal x som ligger mellan talen α och β. Och för detta tal x gäller följande samband:

$$f(\beta) = P(\beta) + \frac{f^{(n)}(x)}{n!}(\beta-\alpha)^n \tag{5.3}$$

[1] **Taylor, Brook:** Brook Taylor var en engelsk matematiker som levde 1685-1731. Betydelsen av Taylors sats insågs inte förrän 1772, då J. L. Lagrange utsåg den till den viktigaste satsen inom differentialkalkyl/analys (Internet: en.wikipedia.org).

För att visa existensen av ett objekt (i vårt fall talet x) har vi i princip tre metoder att välja på: konstruera ett sådant objekt, använda någon generell princip eller ett axiom för att visa att ett sådant objekt måste finnas, eller att använda någon form av bevismetod för att bevisa att objektet finns.

I det här fallet känner jag inte till någon generell princip vi kan luta oss mot, så vi har att välja på att konstruera objektet eller att visa att det finns med någon bevismetod. Vi kan som alltid börja med att försöka genomföra ett direkt bevis.

3. GENOMFÖR PLANEN:

Enligt Solows framåt-bakåt-metod kan vi börja med att utgå från påståendet. En nyckelfråga är då, hur kan vi visa att ett tal x uppfyller ekvationen

$$f(\beta) = P(\beta) + \frac{f^{(n)}(x)}{n!}(\beta - \alpha)^n \ ?$$

Vi kan ju börja med att förenkla livet för oss själva genom att förenkla ovanstående ekvation. Vi låter därför M [*som alltså är ett* ***hjälptal***] vara det tal som definieras genom

$$f(\beta) = P(\beta) + M(\beta - \alpha)^n \tag{5.4}$$

Vi kan nu skriva om påståendet:

P1: Det finns ett tal $x \in (\alpha, \beta)$ sådant att

$$M = \frac{f^{(n)}(x)}{n!}$$

Det är ekvivalent med att $n!M = f^{(n)}(x)$, så vi får ett nytt påstående:

P2: Det finns ett tal $x \in (\alpha, \beta)$ sådant att $n!M = f^{(n)}(x)$ där M definieras genom $f(\beta) = P(\beta) + M(\beta - \alpha)^n$

En ny nyckelfråga blir då, hur kan vi visa att en likhet är uppfylld?

Det visar vi genom att visa att VL minus HL är 0. Detta ger oss ett nytt påstående:

P3: Det finns ett tal $x \in (\alpha, \beta)$ sådant att $f^{(n)}(x) - n!M = 0$ där M definieras genom $f(\beta) = P(\beta) + M(\beta - \alpha)^n$

Just nu kommer vi inte längre genom att arbeta bakåt, men definitionen av talet M ger oss en idé. Definitionen kan skrivas om till följande likhet:

$$f(\beta) - P(\beta) - M(\beta - \alpha)^n = 0$$

Det skulle vara intressant att ta reda på när detta är uppfyllt. Därför inför vi en **hjälpfunktion**, som vi generaliserar genom att sätta $\beta = x$:

$$g(x) = f(x) - P(x) - M(x - \alpha)^n \quad (\alpha \leq x \leq \beta) \tag{5.5}$$

Vad kan vi säga om denna funktion? Det bör vara intressant att undersöka den dels i ändpunkterna av intervallet, dvs att studera $g(\alpha)$ och $g(\beta)$ och dels att studera hur funktionen beter sig emellan dessa punkter.

Om vi deriverar $g(x)$ med avseende på x, så finner vi följande samband:

$$\begin{aligned} g(x) &= f(x) - P(x) - M(x - \alpha)^n \\ g'(x) &= f'(x) - P'(x) - nM(x - \alpha)^{n-1} \\ g''(x) &= f''(x) - P''(x) - n(n-1)M(x - \alpha)^{n-2} \end{aligned}$$

Om vi fortsätter på samma sätt [*dold induktion!*] finner vi:

$$\begin{aligned} g^{(n-1)}(x) &= f^{(n-1)}(x) - P^{(n-1)}(x) - n(n-1)\cdots 2M(x - \alpha) \\ g^{(n)}(x) &= f^{(n)}(x) - P^{(n)}(x) - n!M(x - \alpha)^0 = f^{(n)}(x) - P^{(n)}(x) - n!M \end{aligned}$$

Hur kan detta hjälpa oss?

En central punkt i antagandet är själva Taylorpolynomet, $P(t)$. Vad vet vi om detta polynom? Vi kan se av formeln att det är ett polynom av grad $n - 1$ (eftersom summatecknets övre gräns är $n - 1$). Eftersom polynomet är av grad $n - 1$ måste den n:te derivatan bli noll. (Att den n:te derivatan existerar framgår av antagandet.)

Vi har alltså att $P^{(n)}(t) = 0$. Detta medför att

$$g^{(n)}(x) = f^{(n)}(x) - n!M \tag{5.6}$$

Om vi kan visa att $g^{(n)}(x) = 0$ för något $x \in (\alpha, \beta)$, så har vi visat påstående **P3** och då har vi lyckats! Så nu kan vi inrikta arbetet på att visa att $g^{(n)}(x) = 0$, för **något** $x \in]\alpha, \beta[$.

Vilken mer information som kan vara till hjälp kan vi få ut från Taylorpolynomet $P(x)$?

Om vi upprepade gånger deriverar $P(x)$ med avseende på x, så får vi:

$$
\begin{aligned}
P(x) &= f(\alpha) + f'(\alpha)(x-\alpha) + \frac{f''(\alpha)}{2!}(x-\alpha)^2 + \cdots + \frac{f^{(n-1)}(\alpha)}{(n-1!)}(x-\alpha)^{(n-1)} \\
P'(x) &= f'(\alpha) + f''(\alpha)(x-\alpha) + \cdots + \frac{f^{(n-1)}(\alpha)}{(n-2)!}(x-\alpha)^{(n-2)} \\
P''(x) &= f''(\alpha) + \cdots + \frac{f^{(n-1)}(\alpha)}{(n-3)!}(x-\alpha)^{(n-3)} \\
&\quad [\textit{med dold induktion får vi till slut:}] \\
P^{(n-1)}(x) &= f^{(n-1)}(\alpha) \\
P^{(n)}(x) &= 0
\end{aligned}
$$

Om vi sedan sätter in α istället för x i dessa ekvationer får vi ett snyggt samband, eftersom många termer kommer att bli noll:

$$
\begin{aligned}
P(\alpha) &= f(\alpha) \\
P'(\alpha) &= f'(\alpha) \\
P''(\alpha) &= f''(\alpha) \\
&\quad [\textit{dold induktion ger till slut:}] \\
P^{(n-1)}(\alpha) &= f^{(n-1)}(\alpha) \\
P^{(n)}(\alpha) &= 0
\end{aligned}
$$

Detta i sin tur ger oss ett mycket intressant resultat för funktionen $g(\alpha)$:

$$
\begin{aligned}
g(\alpha) &= f(\alpha) - P(\alpha) - M(\alpha-\alpha)^n = f(\alpha) - f(\alpha) - M \cdot 0^n = 0 \\
g'(\alpha) &= f'(\alpha) - P'(\alpha) - nM(\alpha-\alpha)^{(n-1)} = 0 \\
g''(\alpha) &= f''(\alpha) - P''(\alpha) - n(n-1)M(\alpha-\alpha)^{(n-2)} = 0 \\
&\quad [\textit{dold induktion ger till slut:}] \\
g^{(n-1)}(\alpha) &= f^{(n-1)}(\alpha) - P^{(n-1)}(\alpha) - n(n-1)\cdots 2M(\alpha-\alpha) = 0 \\
g^{(n)}(\alpha) &= f^{(n)}(\alpha) - P^{(n)}(\alpha) - n!M(\alpha-\alpha)^0 = f^{(n)}(\alpha) - n!M
\end{aligned}
$$

Alla derivator upp till och med $n-1$ är alltså lika med 0 för $g(\alpha)$!

Om vi nu slutligen sätter in β istället för x i funktionen g finner vi:
$g(\beta) = f(\beta) - P(\beta) - M(\beta-\alpha)^n$ där definitionen av M säger att $f(\beta) = P(\beta) + M(\beta-\alpha)^n$.
Alltså är $g(\beta) = P(\beta) + M(\beta-\alpha)^n - P(\beta) - M(\beta-\alpha)^n = 0$.

Vi har alltså fått som resultat att $g(\alpha) = g(\beta) = 0$.

Då bör vi påminna oss **Rolles sats**:

Om funktionen $f : x \to f(x)$ är kontinuerlig för $a \leq x \leq b$, och deriverbar för $a < x < b$, och om $f(a) = f(b)$ så finns det ett tal ξ mellan a och *b sådant att $f'(\xi) = 0$.*

Det visar sig att vi med hjälp av denna sats kan slutföra beviset:

$$\begin{aligned}
g(\alpha) = g(\beta) = 0 \quad &\Rightarrow \quad \text{det existerar en punkt } x_1 \text{ där } g'(x_1) = 0 \\
g'(\alpha) = g'(x_1) = 0 \quad &\Rightarrow \quad \text{det existerar en punkt } x_2 \text{ där } g''(x_2) = 0 \\
g''(\alpha) = g''(x_2) = 0 \quad &\Rightarrow \quad \text{det existerar en punkt } x_3 \text{ där } g^{(3)}(x_3) = 0 \\
&\qquad [\textit{dold induktion ger oss:}] \\
g^{(n-1)}(\alpha) = g^{(n-1)}(x_{(n-1)}) = 0 \quad &\Rightarrow \quad \text{det existerar en punkt } x_n \text{ där } g^{(n)}(x_n) = 0
\end{aligned}$$

Observera att alla punkterna $x_1, x_2, \ldots x_n$ ligger inom intervallet $[\alpha, \beta]$. Nu har vi visat att två olika likheter gäller, nämligen:

$$\begin{aligned}
g^{(n)}(x_n) &= 0 \\
g^{(n)}(x_n) &= f^{(n)}(x_n) - n!M \text{ [se ekvation(5.6)!]}
\end{aligned}$$

Alltså kan vi dra slutsatsen att

$$f^{(n)}(x_n) - n!M = 0$$

vilket är ekvivalent med att

$$M = \frac{f^{(n)}(x_n)}{n!} \text{ för något tal } x \in]\alpha, \beta[$$

och satsen är visad!

4. SE TILLBAKA:

Vi kan göra en intressant observation om vi sätter in $n = 1$. Då får vi nämligen följande resultat:

$$P(t) = \sum_{k=0}^{0} \frac{f^{(0)}(\alpha)}{0!}(t - \alpha)^0 = f(\alpha)$$

$$f(\beta) = P(\beta) + \frac{f'(x)}{1!}(\beta - \alpha)^1 = P(\beta) + f'(x)(\beta - \alpha)$$

Om vi sätter in β istället för t i den första likheten, och om vi sätter in detta i den andra likheten får vi följande:

$$f(\beta) = f(\alpha) + f'(x)(\beta - \alpha)$$

$$\Updownarrow$$

$$f(\beta) - f(\alpha) = f'(x)(\beta - \alpha)$$

Detta är som bekant medelvärdessatsen! Taylors polynom är alltså en generalisering av medelvärdessatsen.

Det man kan konstatera då man läser detta bevis är att själva svårigheten ligger i att komma på att hjälpfunktionen $g(x)$ bär på fröet till hela lösningen.

Hur kan man komma på att denna hjälpfunktion kan vara till nytta? I just det här fallet tror jag att man skulle behöva vara en mycket duktig matematiker för att själv "komma på" detta bevis.

Jag föreställer mig också att Taylor själv inte började med att komma på satsen och sedan försökte bevisa den. Troligen upptäckte han snarare ett samband som han ville visa att det även gällde generellt. Och det är ju inte allt för djärvt att tänka sig att han redan i sin upptäckt hade början till beviset klart för sig.

Hur som helst tycker jag att detta bevis är ganska vackert med sin regelbundenhet.

.

Bilaga 1: Grundläggande logik

För att verkligen kunna förstå olika bevismetoder som presenteras i detta examensarbete är det nödvändigt att ha en viss kännedom om grundläggande logik. Här ges därför en kort presentation av vissa logiska resonemang som är nyttiga inför läsandet av resten av uppsatsen. För den som redan är insatt i logik och logiska resonemang är denna bilaga överflödig. Bilagan innehåller följande:

1. Olika typer av utsagor

Inom logiken arbetar man bl.a med olika utsagor (eller propositioner). En utsaga kan t.ex vara:

- *Om x är ett udda heltal, så är x^2 alltid udda.*
- *Ett heltal x är jämnt om och endast om det delas av 2.*

Den första utsagan kan skrivas på formen:

Om A, så B

eller:

$A \quad \Rightarrow \quad B$ (läses "A medför B")

Den andra utsagan är av en annan typ. Uttrycket "om och endast om" ska nämligen utläsas som en dubbel implikation, dvs hela utsagan kan skrivas om enligt följande:

Om ett heltal x är jämnt, så delas det av 2.
OCH
Om ett tal delas av 2, så är det jämnt.

eller:

$A \quad \Rightarrow \quad B \quad OCH \quad B \quad \Rightarrow \quad A$

Oftast skriver man ännu kortare:

$A \quad \Leftrightarrow \quad B$ (läses "A om och endast om B")

I huvudsak har vi alltså hittills följande typer av utsagor:

- $A \quad \Rightarrow \quad B$
- $A \quad \Leftrightarrow \quad B$

Man kan så klart hitta ännu fler olika typer av utsagor, men ovanstående två typer räcker för att åskådliggöra det jag vill visa.

2. Sant och falskt: sanningstabeller

En viktig företeelse inom logiken som har stor betydelse när man arbetar med matematiska bevis, är så kallade sanningstabeller. I en sådan skriver man helt enkelt upp alla tänkbara utfall av de antaganden och påståenden som ingår i en utsaga, och kontrollerar sedan i vilka situationer som hela utsagan är sann. Vi kan t.ex utgå från den öppna utsagan[2] "*Om x är ett udda heltal, så är x^2 alltid udda.*"

Om vi kallar vårt antagande (att x är ett udda heltal) för A, så kan A ha två utfall. Antingen är A sant (x är ett udda heltal) eller så är A falskt (x är inte ett udda heltal). Även vårt påstående, som vi kallar B, kan ha två utfall. Antingen är B sant (x^2 är udda) eller så är B falskt (x^2 är inte udda). Totalt får vi fyra möjliga kombinationer enligt nedanstående tabell (F = false, T = true):

A	***B***
F	F
F	T
T	F
T	T

Men när är då hela utsagan sann, dvs när är $A \Rightarrow B$ sann? Vi resonerar

[2]**Öppen utsaga:** En utsaga som beror av en variabel. I detta fall beror utsagan av variabeln x.

oss fram till detta:

Fall 1: A är falsk och B är falsk. I detta fall kan vi egentligen inte säga säkert om utsagan $A \Rightarrow B$ är sann, eftersom vi inte har A. Men den är i varje fall inte bevisat falsk. Därför räknas även i detta fall utsagan $A \Rightarrow B$ som sann.

Fall 2: A är falsk och B är sann. I detta fall kan vi inte heller säga säkert om utsagan $A \Rightarrow B$ är sann. Men den är inte bevisat falsk. Därför räknas även i detta fall utsagan $A \Rightarrow B$ som sann.

Fall 3: A är sann och B är falsk. Nu får vi helt klart som resultat att utsagan $A \Rightarrow B$ är falsk! Utsagan betyder ju att om A är sann så är B sann. Men i detta fall har vi att A är sann **och** B är falsk. Alltså är utsagan falsk i detta fall.

Fall 4: A är sann och B är sann. Detta stämmer precis med utsagan, så här får vi naturligt att utsagan $A \Rightarrow B$ är sann!

Nu kan vi skriva en ny sanningstabell, där vi även tar med en kolumn som visar när hela utsagan är sann respektive falsk:

A	B	$A \Rightarrow B$
F	F	T
F	T	T
T	F	F
T	T	T

Värt att notera är alltså att för utsagor av typen $A \Rightarrow B$ så finns det bara ett fall då utsagan räknas som falsk, nämligen då vi har att A är sann **samtidigt** som B är falsk. Om vi kan visa att denna situation aldrig kan inträffa så har vi visat att den (öppna) utsaga vi startade med är sann.

Hur används då detta när man arbetar med bevis?

Till att börja med är det helt ointressant att studera de fall då A är falsk, eftersom den sats vi försöker bevisa förutsätter att A är sann. Satsen är ju av typen: ”Om A är sann, så är B sann”.

Vi antar alltså att A är sann, och försöker sedan se vad det leder till när det gäller B. Ovanstående sanningstabell innebär då att om vi kan bevisa att det är omöjligt att B är falsk samtidigt som A är sann, så har vi visat att satsen som helhet är sann!

Nu tittar vi på utsagor av typen $A \Leftrightarrow B$.

Som tidigare nämnts är dessa utsagor egentligen en sammansättning av två utsagor, nämligen $A \Rightarrow B$ **och** $B \Rightarrow A$. Enligt ovanstående resonemang för utsagor av typen $A \Rightarrow B$, så är en sådan utsaga endast falsk då A är sann samtidigt som B är falsk. Motsvarande gäller så klart för $B \Rightarrow A$. Vi kan skriva en sanningstabell som visar utfallen för $A, B, A \Rightarrow B$ samt $B \Rightarrow A$:

$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{A \Rightarrow B}$	$\boldsymbol{B \Rightarrow A}$
F	F	T	T
F	T	T	F
T	F	F	T
T	T	T	T

Eftersom $A \Leftrightarrow B$ egentligen betyder att $A \Rightarrow B$ **och** $B \Rightarrow A$, så är hela utsagan $A \Leftrightarrow B$ bara sann då både $A \Rightarrow B$ och $B \Rightarrow A$ är sanna samtidigt. Den kompletta sanningstabellen blir alltså:

$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{A \Rightarrow B}$	$\boldsymbol{B \Rightarrow A}$	$\boldsymbol{A \Leftrightarrow B}$
F	F	T	T	T
F	T	T	F	F
T	F	F	T	F
T	T	T	T	T

Slutsatsen av ovanstående sanningstabell blir att en utsaga av typen $A \Leftrightarrow B$ bara är sann antingen då både A och B är falska eller då både A och B är sanna. När det gäller hur detta ska användas i matematiska bevis så ska man komma ihåg att en utsaga med dubbel implikation alltid måste bevisas åt **båda hållen**! För att visa $A \Leftrightarrow B$ måste man alltså **både** visa $A \Rightarrow B$ **och** $B \Rightarrow A$.

3. Besläktade utsagor och indirekta bevis

Innehållet i detta avsnitt är inspirerat av Antonella Cupillari ([3], sid 19-21).

Inom logiken är två utsagor **ekvivalenta** om de har samma sanningstabell. Det innebär att om vi vill kan vi skriva om en utsaga så att vi får

en annan ekvivalent utsaga som är lättare att arbeta med. (Observera att tecknet ¬ används för att beteckna "inte"; "$\neg A$" betyder alltså "*inte* A".)

Från utsagan "$A \Rightarrow B$" kan man konstruera tre besläktade utsagor:

Motsatsen: $B \Rightarrow A$

Inversen: $\neg A \Rightarrow \neg B$

Kontrapositivet: $\neg B \Rightarrow \neg A$

Nu gör vi en sanningstabell som visar när dessa fyra olika utsagor är sanna:

$\boldsymbol{A}$	$\boldsymbol{B}$	$\neg\, \boldsymbol{A}$	$\neg\, \boldsymbol{B}$	$\boldsymbol{A \Rightarrow B}$	Motsats: $\boldsymbol{B \Rightarrow A}$	Invers: $\boldsymbol{\neg\, A \Rightarrow \neg\, B}$	Kontrapos.: $\boldsymbol{\neg\, B \Rightarrow \neg\, A}$
F	F	T	T	**T**	T	T	**T**
F	T	T	F	**T**	F	F	**T**
T	F	F	T	**F**	T	T	**F**
T	T	F	F	**T**	T	T	**T**

Som framgår av tabellen visar det sig att utsagan $A \Rightarrow B$ är ekvivalent med sitt kontrapositiv $\neg B \Rightarrow \neg A$. Detta innebär att vi kan välja att bevisa $\neg B \Rightarrow \neg A$ istället för att bevisa $A \Rightarrow B$. De två utsagorna är nämligen sanna och falska precis samtidigt. Detta används få man arbetar med indirekta bevis med kontrapositiv.

Ett indirekt bevis med motsägelse använder ett annat resonemang. Om man kan visa att "A *och* $\neg B$" är falsk, kan man dra slutsatsen att $A \Rightarrow B$ måste vara sann.

Hur kan det komma sig att om "A *och* $\neg B$" är falsk, så är $A \Rightarrow B$ sann? Vi sa tidigare att $A \Rightarrow B$ är falsk endast om vi har A samtidigt som vi **inte** har B, dvs att situationen "A *och* $\neg B$" leder till att $A \Rightarrow B$ är falsk.

Vi studerar sanningstabellen för de två utsagorna:

$\boldsymbol{A}$	$\boldsymbol{B}$	$\neg\, \boldsymbol{B}$	$\boldsymbol{A \Rightarrow B}$	$\boldsymbol{A}$ *och* $\neg\, \boldsymbol{B}$
F	F	T	**T**	F
F	T	F	**T**	F
T	F	T	**F**	T
T	T	F	**T**	F

Som framgår av tabellen är utsagan "A *och* $\neg B$" falsk precis när $A \Rightarrow B$ är sann, och vice versa. Alltså: om vi kan visa att "A *och* $\neg B$" är falsk, så är det samma sak som att $A \Rightarrow B$ är sann!

Detta utnyttjas i den speciella typ av indirekta bevis som kallas motsägelsebevis: Om vi kan visa att det är omöjligt att vi **samtidigt** har A och $\neg B$, så kan vi alltså dra slutsatsen att utsagan $A \Rightarrow B$ måste vara sann.

När man arbetar med indirekta bevis krävs det ofta en del eftertanke för att formulera negationer av olika utsagor på ett korrekt sätt. Mer detaljer om hur man formulerar negationer finns i avsnittet 3.3.2.

4. Slutsatser av betydelse för matematiska bevis

Utsagor av typen "$A \Rightarrow B$": Denna typ av utsaga är endast falsk då vi samtidigt har A och $\neg B$. Det innebär att om vi kan visa att det är omöjligt att få $\neg B$ om man utgår från A, så kan vi bevisa utsagan $A \Rightarrow B$.

En annan möjlighet att bevisa denna typ av utsaga är genom indirekta bevis, som det finns två varianter av.

- Den första varianten innebär att man visar **kontrapositivet** ("$\neg B \Rightarrow \neg A$"), som har samma sanningstabell som den ursprungliga utsagan.
- Den andra varianten är **motsägelsebevis**, som inleds med att man antar att man har "A *och* $\neg$ B". Om detta antagande leder till en motsägelse eller en orimlighet, så har man visat att antagandet är falskt och då är samtidigt utsagan $A \Rightarrow B$ sann, eftersom dessa två utsagor har exakt motsatta sanningstabeller (när den ena är sann är den andra falsk och vice versa).

Utsagor av typen "$A \Leftrightarrow B$": Tecknet $\Leftrightarrow$ motsvarar orden "om och endast om" i löpande text. När man stöter på orden "om och endast om" ska man vara medveten om att detta innebär en dubbel implikation, som medför att man måste visa dels $A \Rightarrow B$ och dels $B \Rightarrow A$, enligt någon av de metoder som nämns här ovan.

Bilaga 2: Tillräckligt/nödvändigt villkor

I matematisk text finner man ofta uttrycken "tillräckligt villkor" samt "nödvändigt villkor". Det är dock inte alldeles självklart vad som menas med dessa uttryck. I denna bilaga ges därför en kort förklaring vad dessa uttryck egentligen betyder.

Tillräckligt villkor

Om vi utgår från en sats som är på formen $A \Rightarrow B$, så betyder det att om A är sann, så är också B sann.

Man säger att ***A* är ett tillräckligt villkor för *B***. Med det menas att om A är sann, så vet man att också B är sann - det garanteras ju av satsen! Man kan alltså säga att det är **tillräckligt** att veta att A är sann, så vet man att också B är sann.

Nödvändigt villkor

Vi utgår från samma sats som ovan: $A \Rightarrow B$.

Man säger då att ***B* är ett nödvändigt villkor för *A***. Med det menas att A kan inte vara sann utan att även B är sann. Det är alltså **nödvändigt** att B är sann för att A ska kunna vara sann. Men observera att detta **inte** innebär att $B \Rightarrow A$! Istället innebär det att om B inte är sann, så kan A inte heller vara sann.

Detta är samma sak som $\neg B \Rightarrow \neg A$, vilket som bekant (se Bilaga 1) är kontrapositivet till vår ursprungliga utsaga $A \Rightarrow B$. Eftersom kontrapositivet är sant samtidigt som den ursprungliga utsagan är sann, så innebär ovanstående sammantaget att man kan säga att B är ett nödvändigt villkor för A.

Exempel 1

Antag att vi har utsagan $x = 2 \Rightarrow x^2 = 4$.

$x = 2$ är här ett **tillräckligt villkor** för $x^2 = 4$.

(Men det finns även andra x som uppfyller att $x^2 = 4$, nämligen om $x = -2$.)

$x^2 = 4$ är ett **nödvändigt villkor** för $x = 2$. För om $x^2 \neq 4$ så medför det att $x \neq 2$.

Exempel 2

Vi utgår från denna sats:

Om en funktion f är deriverbar så är den kontinuerlig

Deriverbarhet är alltså ett **tillräckligt villkor** för kontinuitet, dvs om man vet att funktionen är deriverbar så vet man också att den är kontinuerlig.

Kontinuitet är ett **nödvändigt villkor** för deriverbarhet, för om en funktion inte är kontinuerlig så kommer det att finnas punkter där funktionen saknar derivata. Observera som tidigare att det faktum att kontinuitet är ett nödvändigt villkor för deriverbarhet **inte** innebär att kontinuitet medför deriverbarhet! Exempelvis funktionen $f(x) = |x|$ är kontinuerlig, men inte deriverbar i $x = 0$, eftersom den saknar gränsvärde i $x = 0$. Bevis för detta ges av Persson & Böjers ([9], s. 185).

Tillräckligt *och* nödvändigt villkor

Om man har en sats av denna typ: $A \Leftrightarrow B$, så säger man att A är både ett tillräckligt och nödvändigt villkor för B, och samtidigt är B både ett tillräckligt och nödvändigt villkor för A.

Tack!

Jag vill framföra mitt varmaste tack till några personer som gjort det möjligt för mig att skriva detta examensarbete.

Först vill jag tacka min handledare, Christian Gottlieb. Christian har gett mig ovärderligt stöd i form av tips och idéer och en fast förankring i den matematiska världen - där jag själv bara är nybörjare. Med sitt vänliga tålamod och sin detaljerade granskning av mitt arbete har han ständigt uppmuntrat mig att förbättra mitt examensarbete.

Jag vill också tacka Jocke Sundberg, Lars Domeij och Elin Gawell vilka alla tre hjälpt mig väldigt mycket på några av kurserna på påbyggnadsnivån. Utan deras hjälp tvivlar jag på att jag hade klarat kurserna! Och då hade inte heller detta examensarbete blivit gjort.

Sist men inte minst vill jag tacka min man, Göran Månsson, för hans tålamod och stöd under de år jag har läst matematik. Tidvis har han knappt sett mig annat än till middagen, eftersom jag ägnat så mycket tid åt mina studier. Därför är det en befrielse för oss båda att mitt examensarbete nu är färdigt!

.

Litteraturförteckning

[1] Beachy, John A. & Blair, William D.; *Abstract Algebra, Second Edition*, Waveland Press Inc, 1996.

[2] Biggs, Norman L.; *Discrete Mathematics*, Oxford University Press, 2002.

[3] Cupillari, Antonella; *The Nuts and Bolts of Proofs*, Academic Press, 2001.

[4] Daepp, Ulrich & Gorkin, Pamela; *Reading, Writing and Proving*, New York Springer, 2003.

[5] Garnier, Rowan & Taylor, John; *100% Mathematical Proof*, John Wiley & Sons Ltd, 1996.

[6] Hyltén-Cavallius, Carl & Sandgren, Lennart; *Matematisk analys 2*, Studentlitteratur, 1968.

[7] Nystedt, Lars; *På tal om tal. En läsebok i matematik.*, Instant mathematics, 1993.

[8] Nyström, Kirsti; *Swedish university entrants' experiences about and attitudes towards proofs and proving*, Stockholms Universitet, 2003.

[9] Persson, Arne & Böiers, Lars-Christer; *Analys i en variabel*, Studentlitteratur, 2001.

[10] Persson, Arne & Böiers, Lars-Christer; *Analys i flera variabler*, Studentlitteratur, 1988.

[11] Polya, George; *Problemlösning - en handbok i rationellt tänkande*, Prisma Förlag, 2003. (Originalets titel: *How to solve it.*)

[12] Rudin, Walter; *Principles of Mathematical Analysis*, McGraw-Hill Book Company, 1976.

[13] Solow, Daniel; *How to read and do proofs*, Johan Wiley and Sons Inc., 2002.