UPPSALA UNIVERSITET Matematik för språkteknologer (5LN445)
Institutionen för lingvistik och filologi VT 2014
(Marco Kuhlmann 2013, tillägg och omarbetning Mats Dahllöf 2014).

1 Lite om matematisk notation

1.1 Matematisk notation

För att kunna specificera matematiska modeller krävs en bra **notation**. Samtidigt kan notationen göra det svårt för ej insatta att förstå den matematiska modellen. En viktig färdighet som ni kommer att behöva under hela kursen är att bli bekväma med och behärska den matematiska notation som införs på kursen.

1.2 Några viktiga typer av uttryck

Utsagor, satser, etc: Uttryck som är sanna eller falska, t.ex. ”$0 < 5$”, ”$0 + 7 < 5$”.

Enskilda värden: Uttryck som står för bestämda värden, t.ex. 0, 5, $0,33$, $\emptyset$, $\{1, 2, 3, 4\}$.

Variabler: Uttryck som kan anta olika värden, t.ex. i generella utsagor eller vid beräkningar som bygger på att beräkningssteg upprepas. De utgörs oftast av lämpligt utvalda bokstäver, latinska eller grekiska.

Relationer: Relationer appliceras på ett givet antal värden och ger en utsaga (som alltså är sann eller falsk), t.ex. i ”$0 < 5$” appliceras mindre-än-relationen ($<$) på argumenten 0 och 5. Ordningen är viktig!

Negerande streck över relationssymboler: När ett snedstreck står över en relationssymbol, t.ex. som i ”$\neq$” och ”$\notin$” betyder det att relationerna ”$=$” respektive ”$\in$” inte råder.

Funktioner: Funktionssymboler appliceras på ett givet antal värden och ger ett uttryck som representerar *ett* bestämt värde. Detta kan ofta räknas ut. De fyra räknesätten (addition: $+$, subtraktion: $-$, multiplikation: $\cdot$, och division: $/$) är funktioner. Additionen ”$0 + 7$” står för värdet 7, t.ex. En annan funktion är fakultet (mer senare) och skrivs ”!”. Dess symbol placeras efter argumentet, som i uttrycket ”5!” ($5! = 120$).

Serier: Man har ofta anledning att skriva serier av värden. Eftersom dessa kan vara väldigt långa eller oändliga behövs en notation med ”…”, som används så att läsaren kan förstå vilka värden punkterna matchar. Om vi t.ex. skriver

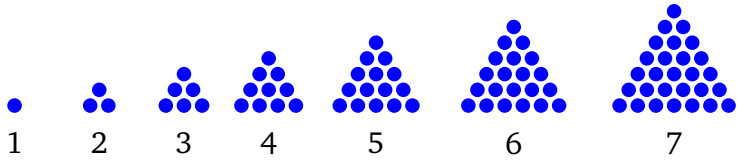
$$(n + 1) \times (n + 2) \times \cdots \times (m - 1)$$

så menar vi produkten av alla heltal större än n och mindre än m. (Om $n = 5$ och mindre än $m = 7$, så skulle det bara bli 6 rakt av, trots att det ser ut som om minst tre värden skall multipliceras.)

1.3 Notation för summor

Fråga: Vilket är nästa tal i denna serie? $1, 3, 6, 10, 15, \ldots$

Om vi funderar ett slag så inser vi kanske detta, som vi skulle kunna visualisera så här:



Dessa tal kallas för *triangulärtalen*. Det $n$ta triangulärtalet, som vi kan skriva $T(n)$, är $1 + \cdots + n$. Några exempel:

$$T(1) = 1$$
$$T(2) = 1 + 2$$
$$T(3) = 1 + 2 + 3$$
$$T(4) = 1 + 2 + 3 + 4$$
$$T(5) = 1 + 2 + 3 + 4 + 5$$

Vi har nu infört T som en funktionssymbol.

En kompakt och mera precis notation för en sådan summa är denna, med grekisk versal sigma (Σ) för summa.

$$T(n) = \sum_{i=1}^{n} i$$

Detta uttryck står för en summa. Man räknar ut dess värde genom att för varje värde av variabeln i mellan 1 och n utvärdera uttrycket som står efter Σ-symbolen (som ju bara är i) och addera dessa värden. Symbolen i kallas för **summationsindex**, värdet 1 kallas för **undre gräns**, värdet n kallas för **övre gräns**, och uttrycket efter Σ-symbolen kallas för **summaterm**.

Ett annat exempel:

$$\sum_{i=1}^{4} (i + 5)^2 = 6^2 + 7^2 + 8^2 + 9^2$$

När undre gränsen är större än övre gränsen säger man att summan är **tom**. Då definierar man att den ska läsas som ett uttryck för 0.

$$\sum_{i=k}^{n} f(i) \;=\; 0 \qquad (\text{om } k > n)$$

Fråga: Multiplikation bygger, som bekant, på addition: Hur kan man skriva produkten $m \cdot n$ genom en summaterm?

$$m \cdot n \;=\; \underbrace{m + \cdots + m}_{n \text{ gånger}} \;=\; \sum_{i=1}^{n} m \qquad \text{eller} \qquad m \cdot n \;=\; \underbrace{n + \cdots + n}_{m \text{ gånger}} \;=\; \sum_{i=1}^{m} n$$

1.4 Notation för produkter

På liknande sätt som för summor kan man göra med produkter (och använder då grekisk versal pi, Π), t.ex. så här:

$$\prod_{i=1}^{n} i$$

Detta uttryck definierar fakulteten (factorial) av n, som brukar skrivas $n!$. (Vi kommer att återvända till detta.)

Även ! är en funktionssymbol, som av hävd placeras efter sitt argument.

Några exempel:

$1! = 1$
$2! = 1 \cdot 2$
$3! = 1 \cdot 2 \cdot 3$
$4! = 1 \cdot 2 \cdot 3 \cdot 4$
$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

Fråga: Vad får man när man ersätter $\sum$ genom $\prod$ i uttrycket $\sum_{i=1}^{n} m$?

Då får man ett uttryck för potensen m^n:

$$\prod_{i=1}^{n} m \;=\; \underbrace{m \cdot \cdots \cdot m}_{n \text{ gånger}} \;=\; m^n$$

Den tomma produkten läses som ett uttryck för 1.

$$\prod_{i=k}^{n} f(i) \;=\; 1 \qquad (\text{om } k > n)$$

Fråga: Vad borde triangulärtalet $T(0)$ och fakulteten 0! ha för några värden?

2 Mängder

Diskret matematik handlar om diskreta strukturer. I denna lektion kommer vi att behandla den mest elementära diskreta strukturen, som alla andra diskreta strukturer bygger på: *mängden*. Mängdbegreppet, relationer mellan mängder och operationer på mängder utgör den diskreta matematikens mest grundläggande verktyg. Det är därför viktigt att kunna hantera dessa begrepp.

2.1 Grundläggande begrepp

En **mängd** är en uppsättning av objekt. Objekten kallas för mängdens **element**. Man skriver $a \in A$ som en förkortning för ”objektet a tillhör mängden A” och $a \notin A$ som en förkortning för ”objektet a tillhör *inte* mängden A”. Det är vanligt att använda sig av stora bokstäver för att beteckna mängder, och av små bokstäver för att beteckna element. (Vi kommer dock in på mängder som har mängder som element ganska snart.)

2.1.1 Beskrivningar av mängder

Mängder brukar beskrivas på två olika sätt.

Uppräkning Man kan helt enkelt räkna upp mängdens element. Om mängden ifråga är väldigt stor (i synnerhet oändligt stor) kan man även använda utelämningstecknet – i hopp på att det är klart vad som har utelämnats. Här kommer, som exempel, mängden av sanningsvärden, mängden av alla medlemmar i *Beatles* år 1964 och mängden av alla naturliga tal.

$$\mathbb{B} = \{\text{true}, \text{false}\} \qquad B = \{\text{John}, \text{Paul}, \text{George}, \text{Ringo}\} \qquad \mathbb{N} = \{0, 1, 2, \dots\}$$

Mängdbyggaren Man kan beskriva en mängd genom att specificera vilka egenskaper som utmärker de element som tillhör mängden. Till exempel:

$$B = \{x \mid x \text{ var en medlem i } \textit{Beatles} \text{ år } 1964\}$$

Detta ska läsas som: ”Mängden B är mängden av alla x sådana att x var en medlem i *Beatles* år 1964.” Denna notation kallas för **mängdbyggaren**.

Exkurs: Russell’s paradox

Användning av mängdbyggaren kan ge upphov till **Russell’s paradox** (efter britten Bertrand Russell, 1872–1970), som visar att den naiva mängdläran (som

hade utvecklats av den tyska matematikern Georg Cantor, 1845–1918) är motsägelsefull. Betrakta mängden

$$R = \{A \mid A \text{ är en mängd som inte innehåller sig själv}\}.$$

Eftersom R är mängden av alla mängder som inte innehåller sig själva kan det inte vara fallet att $R \in R$. Låt oss alltså anta motsatsen, att $R \notin R$. Då uppfyller R egenskapen som utmärker de element som tillhör R, alltså måste det gälla att $R \in R$. Paradox!

2.1.2 Extensionalitetsprincipen

Hur man beskriver en mängd spelar ingen roll; det enda som är viktigt är vilka element ingår i mängden. Det vill säga, två mängder är identiska om och endast om de har samma element. Detta kallas för **extensionalitetsprincipen**. Den innebär bland annat att ordningen i vilken man anger mängdens element är irrelevant, så att $\{1, 2, 3\}$ och $\{3, 2, 1\}$ beskriver samma mängd. En annan konsekvens är att varje element bara kan räknas en gång, så att exempelvis $\{1\}$ och $\{1, 1\}$ beskriver samma mängd.

2.1.3 Den tomma mängden

Den **tomma mängden** är mängden som inte har några element. Den brukar skrivas $\emptyset$.

Fråga: Kan du komma på en beskrivning av den tomma mängden?

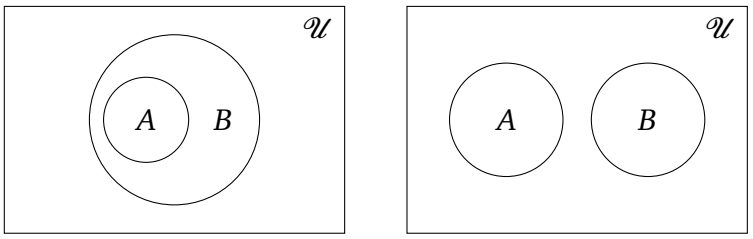
$\emptyset = \{ x \mid x$ är en kvinna och är eller har varit Sveriges statsminister$\}$

Ett vanligt misstag är att blanda ihop $\emptyset$ (den tomma mängden) och $\{\emptyset\}$ (mängden som innehåller den tomma mängden som sitt enda element).

2.1.4 Delmängder

En mängd A är en **delmängd** till en mängd B om och endast om varje element i A är ett element i B. Man skriver $A \subseteq B$ som en förkortning för ”A är en delmängd till B” och $A \nsubseteq B$ som en förkortning för ”A är *inte* en delmängd till B”.

Delmängdsrelationen kan beskrivas genom vad som brukar kallas för **Venn-diagram** (efter britten John Venn, 1834–1923); se Figur 1a. I dessa diagram representeras mängder genom cirklar. Cirklarnas placering representerar relationerna mellan mängderna.



(a) $A \subseteq B$ (b) $A \parallel B$

Figur 1: Två relationer mellan mängder: ”är delmängd till” och ”är disjunkt till”.

Den omgivande rektangeln i ett Venn-diagram beskriver mängden som innehåller alla i sammanhanget relevanta objekt. Denna mängd kallas även för **universum** och skrivs ibland $\mathscr{U}$. Vilka element ingår i universumet framgår oftast ur sammanhanget; men vill man vara riktigt noggrann anger man universumsmängden när man specificerar mängder. Använder man mängdbyggaren brukar man skriva universumsmängden till vänster om det lodrätta strecket. Till exempel:

$$J = \{ n \in \mathbb{N} \mid n \text{ är jämt} \}$$

Vi kommer för det mesta *inte* ange $\mathscr{U}$ i mängdbyggarna eller Venn-diagrammen.

Delmängdsrelationen är **transitiv**: $A \subseteq B$ och $B \subseteq C$ implicerar generellt att $A \subseteq C$. Den är även **reflexiv**: $A \subseteq A$, generellt.

Fråga: Kan du ge ett exempel på en annan transitiv relation?

Ett exempel är relationen ”är mindre eller lika med” på heltalen: $a \leq b$ och $b \leq c$ implicerar att $a \leq c$. Vi kommer att prata mer om transitivitet i lektion 2.3.

Fråga: Hur bevisar man att $A \subseteq B$? Hur bevisar man att $A \nsubseteq B$?

För att visa att $A \subseteq B$ måste vi visa att varje element i A är ett element i B. För att visa att $A \nsubseteq B$ måste vi bara hitta ett element i A som inte finns med i B.

Man kan visa att $\emptyset \subseteq A$, för godtyckliga mängder A. För att visa att $\emptyset \subseteq A$ gäller måste vi visa att varje element i $\emptyset$ är ett element i A. Men den tomma mängden innehåller ju inga element, så påståendet gäller på ett trivialt sätt. (Ett liknande påstående är: ”Varje Hollywood-film som jag någonsin har medverkat i har fått en Oscar.”)

Fråga: Kan du förklara skillnaden mellan "$\emptyset \subseteq A$" och "$\emptyset \in A$"?

Påståendet "$\emptyset \subseteq A$" säger att den tomma mängden är en delmängd till mängden A. Detta påståendet är sant för godtyckliga mängder A (som vi har just bevisat), och ger därför ingen information. Påståendet "$\emptyset \in A$" säger att den tomma mängden är ett av elementen i A. Detta gäller inte för godtyckliga mängder. En mängd som det gäller för är $\{\emptyset\}$.

Delmängdsrelationen är central för många matematiska argument. Ett exempel: Det vanligaste sättet att bevisa att två mängder är lika är att dela upp beviset och visa

$$\text{(i) } A \subseteq B \qquad \text{och} \qquad \text{(ii) } B \subseteq A$$

Fråga: Kan du förklara varför detta bevis fungerar?

Om $A \subseteq B$ så är alla element i A även element i B; om $B \subseteq A$ så är alla element i B även element i A. Då följer att $A = B$ genom extensionalitetsprincipen.

2.1.5 Potensmängden

Potensmängden till en mängd A är mängden som består av alla delmängder till A. Potensmängden till A skrivs ofta $\mathscr{P}(A)$.

Fråga: Vad är potensmängden till mängden $\{0, 1, 2\}$?

Potensmängden till $\{0, 1, 2\}$ är mängden av alla delmängder till $\{0, 1, 2\}$, så

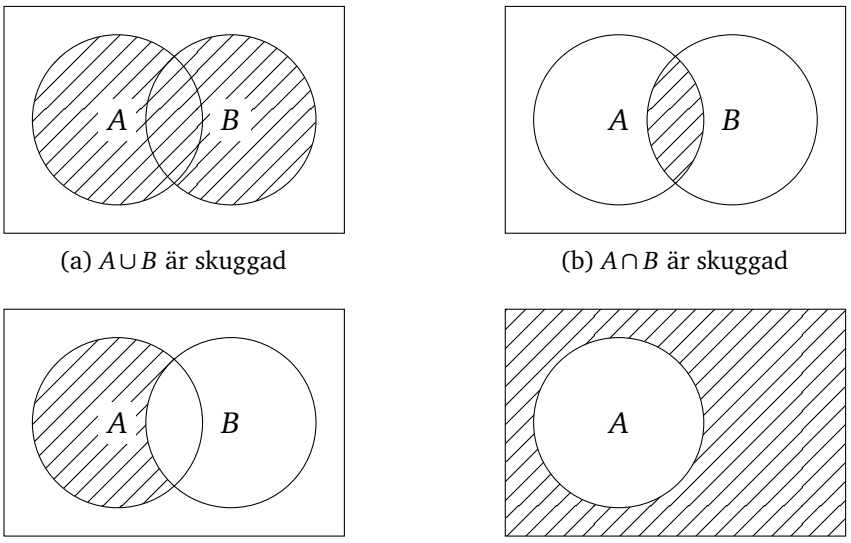
$$\mathscr{P}(\{0,1,2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{1,2\}, \{0,2\}, \{0,1,2\}\}$$

Fråga: Vad är potensmängden till den tomma mängden?

Potensmängden till den tomma mängden är den tomma mängden.

2.1.6 Disjunkthetsrelationen

Två mängder A och B är **disjunkta** om de inte har några gemensamma element. Ibland ser man notationen $A \parallel B$ som förkortning för "A och B är disjunkta".



(a) $A \cup B$ är skuggad (b) $A \cap B$ är skuggad

(c) $A - B$ är skuggad (d) A^c är skuggad

Figur 2: Mängdoperationer.

Fråga: Kan du rita ett Venn-diagram som illustrerar disjunkthetsrelationen?

Se Figur 1b.

2.2 Mängdoperationer

På samma sätt som man kan räkna med tal kan man även räkna med mängder. När vi räknar med tal har vi operationer som addition och multiplikation. När vi räknar med mängder har vi dessa operationer:

$$A \cup B = \{x \mid x \in A \text{ eller } x \in B\} \quad (\textbf{unionen} \text{ av mängderna } A \text{ och } B)$$
$$A \cap B = \{x \mid x \in A \text{ och } x \in B\} \quad (\textbf{snittet} \text{ av mängderna } A \text{ och } B)$$
$$A - B = \{x \mid x \in A \text{ men } x \notin B\} \quad (\textbf{differensen} \text{ mellan mängderna } A \text{ och } B)$$

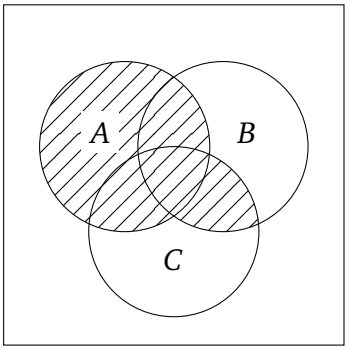
Differensen mellan mängderna A och B skrivs även som $A \setminus B$. Operationerna kan illustreras genom Venn-diagrammen i Figur 2a–c.

Differensen mellan universumet och en mängd A kallas för A:s **komplement** och skrivs A^c:

$$A^c = \mathcal{U} - A = \{x \mid x \in \mathcal{U} \text{ och } x \notin A\}$$

Fråga: Kan du rita ett Venn-diagram för A:s komplement?

Se Figur 2d.



Figur 3: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ är skuggad.

Precis som för operationer som addition och multiplikation finns det räkneregler för mängdoperationer. Ett exempel: För tal gäller *distributivitetslagen* $a \cdot (b + c) = ab + ac$. För mängder gäller distributivitetslagen

$$A \cup (B \cap C) \;=\; (A \cup B) \cap (A \cup C)$$

Hur kan vi bevisa detta? Ett sätt är att bevisa ömsesidig inklusion. Ett annat sätt är att rita ett Venn-diagram för de tre mängderna och att övertyga sig om att det vänstra uttrycket beskriver samma område i diagrammet som det högra uttrycket (se Figur 3).

I Eriksson och Gavel finns det många fler räkneregler för mängdoperationerna (avsnitt 2.3). Jag rekommenderar er varmt att försöka bevisa några av dem.

2.3 Kardinalitet

Storleken hos en mängd A kallas A:s **kardinalitet** och skrivs $|A|$. För ändligt stora mängder anger $|A|$ antalet element i A. (För oändligt stora mängder finns det ingen självklar definition av ”storlek”. Vi kommer tillbaka till denna punkt senare i kursen.)

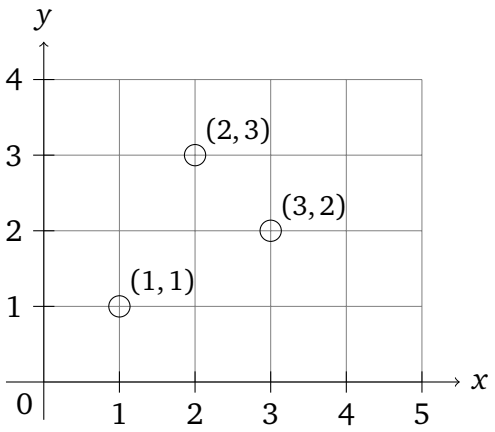
Fråga: Om A och B är (ändligt stora) mängder så att $A \subseteq B$ gäller, vad gäller då för deras kardinaliteter?

Det gäller att $|A| \leq |B|$.

Fråga: Hur kan man räkna ut kardinaliteten $|A \cup B|$?

En första gissning är att $|A \cup B| = |A| + |B|$, men i det senare uttrycket räknas de gemensamma elementen två gånger, dels som element i A, dels som element i B. De gemensamma elementen är elementen i snittet $A \cap B$. För att få ett korrekt uttryck måste vi alltså ta bort $|A \cap B|$ många element från $|A| + |B|$:

$$|A \cup B| \;=\; |A| + |B| - |A \cap B|$$



Figur 4: Ett koordinatsystem.

Fråga: Om en mängd A har n element, hur många element har då A:s potensmängd?

Potensmängden till A består av alla delmängder till A. Varje delmängd $B \subseteq A$ kan beskrivas genom att för varje element $a \in A$ ställa frågan: Är $a \in B$, ja eller nej? På denna fråga finns det två svar, så om det finns n element i A finns det sammanlagt

$$\underbrace{2 \cdot \cdots \cdot 2}_{n \text{ gånger}} = \prod_{i=1}^{n} 2^i = 2^n$$

olika möjligheter att svara. Detta visar att $|\mathscr{P}(A)| \leq 2^n$. Samtidigt är det så att olika svar på frågorna specificerar olika delmängder, vilket visar att $2^n \leq |\mathscr{P}(A)|$. Därför gäller att $|\mathscr{P}(A)| = 2^n$.

2.4 Par och tupler

Det *kartesiska koordinatsystemet* är ett koordinatsystem som i planet består av en x-axel och en y-axel som skär varandra vinkelrätt. Man brukar rita x-axeln från vänster till höger och y-axeln nerifrån uppåt. Genom att markera enhetslängder för båda axlarna definierar man ett rutnät. Varje punkt på detta nät kan skrivas som (x, y), där x anger koordinaten på x-axeln och y anger koordinaten på y-axeln. Ett exempel på ett koordinatsystem visas i Figur 4.

Uppdrag: Rita in punkterna för koordinaterna $(2,2)$, $(2,3)$ och $(3,2)$!

Koordinater som dessa är exempel på **par**. I ett par (x,y) kallar man x och y parets **komponenter**. Notera att $(2,3) \neq (3,2)$! Det vill säga, ordningen mellan komponenterna spelar en roll.

Ett pars komponenter behöver inte vara tal. Låt A och B vara godtyckliga mängder. Mängden av alla par (a,b) där $a \in A$ och $b \in B$ kallas för **produktmängden** av A och B. Den skrivs $A \times B$ och kan beskrivas genom mängdbyggaren

$$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

I exemplet hade vi två mängder X och Y:

$$X = \{1,2,3,4,5\} \qquad Y = \{1,2,3,4\} \qquad X \times Y = \{(x,y) \mid x \in X, y \in Y\}$$

Fråga: Låt A och B vara godtyckliga mängder. Betrakta produktmängden $A \times B$. Hur många element har den?

Om A har m element och B har n element så har produktmängden $A \times B$ exakt m gånger n element. (Och det passar ju bra ihop med beteckningen ”produktmängd”!) Observera att om en av mängderna är tom, så kan man inte bilda några par, så produktmängden blir tom den också: Om $m = 0$ eller $n = 0$ så är $mn = 0$.

För att beskriva en tredimensionell rymd snarare än ett tvådimensionellt plan lägger man till en z-axel vinkelrätt mot (x,y)-planet. Även här har vi punkter, men dessa har nu *tre* koordinater. Man kan kalla dem för **triplar**. På samma sätt kan man definiera quadrupler, quintupler, och mera allmänt n-tupler.

2.5 Läsning och övningar

Eriksson och Gavel kapitel 2, förutom avsnitt 2.6.2 och övning 2.37.

3 Rekursion och induktion

3.1 Rekursiva definitioner

Rekursiva definitioner är definitioner som refererar till sig själva. De är nära besläktade med rekursiva subrutiner i ett datorprogram, alltså subrutiner som anropar sig själva.

> **Fråga:** Har ni stött på rekursion i era programmeringskurser?

3.1.1 Fakultetsfunktionen

Ett exempel är den rekursiva definitionen av **fakulteten** av ett tal, skrivet $n!$, som är produkten av talen från 1 till n:

$$n! \;=\; 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n \;=\; \prod_{i=1}^{n} i$$

Vi kan räkna ut fakulteten av n för några konkreta värden av n:

$$1! = 1\,, \quad 2! = 1 \cdot 2 = 2\,, \quad 3! = 1 \cdot 2 \cdot 3 = 6\,, \quad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$$

> **Fråga:** Vad anger fakulteten av n? Vad är fakulteten av 0?
>
> Fakulteten av n anger antalet möjligheter att ordna en sekvens med n element. Om $n = 0$ har vi $n! = \prod_{i=1}^{0} i$, den tomma produkten. För den har vi sagt att den ska ha värdet 1. Och det passar ju bra: om det inte finns några element att anordna, så finns det bara ett sätt att göra det på.

När man tittar på termerna i produkten som man måste räkna ut för $n!$ ser man att de allra flesta redan förekommer i produkten för $(n-1)!$:

$$1! = 1 \qquad 2! = \underbrace{1}_{1!} \cdot 2 = 2 \qquad 3! = \underbrace{1 \cdot 2}_{2!} \cdot 3 = 6 \qquad 4! = \underbrace{1 \cdot 2 \cdot 3}_{3!} \cdot 4 = 24$$

Det vill säga, om $n > 1$ är fakulteten av n lika med fakulteten av $n-1$, gånger n. Detta kan vi även säga i fallet $n = 1$, eftersom $1! = 0! \cdot 1 = 1 \cdot 1 = 1$. Alltså gäller:

$$n! \;=\; \begin{cases} 1 & \text{om } n = 0 \\ (n-1)! \cdot n & \text{om } n > 0 \end{cases}$$

Vi kan ta det här som en rekursiv definition av fakulteten. Fallet $n > 0$ refererar tillbaka till definitionen och kallas därför **rekursivt**. Fallet $n = 0$ kallas **basfall**; detta fall refererar *inte* tillbaka till definitionen. För att en rekursiv definition ska vara korrekt behövs det minst ett basfall. I nästa exemplet kommer vi att se en rekursiv funktion vars definition har *två* basfall.

3.1.2 Fibonaccitalen (E&G 4.1.1)

Vad kännetecknar denna (oändliga) talserie? (Vilket är det 500:de talet i den, t.ex.?)

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

Jo, vi har börjat med 0 och 1 och sedan räknat ut följande tal som summan av de två föregående (t.ex. $21 + 34 = 55$, med talen på plats 8 till 10).

Vi får en rekursiv definition. Låt oss skriva $f(n)$ för talet på plats n.

$$f(n) = \begin{cases} 0 & \text{om } n = 0 \\ 1 & \text{om } n = 1 \\ f(n-1) + f(n-2) & \text{om } n > 1 \end{cases}$$

Observera att det här finns två basfall. Detta är viktigt, eftersom det rekursiva fallet refererar till två olika mindre fall: $n-1$ och $n-2$.

Denna talföljd omnämndes år 1201 av matematikern Leonardo da Pisa, som även kallas för Fibonacci (son till Bonaccio), men den hade varit känd redan för antikens greker och indier. (Den är på många sätt intressant, och ni kan lätt hitta mer att läsa om den.)

3.1.3 Antalet delmängder med en viss storlek (se även E&G 5.5)

Potensmängden $\mathscr{P}(A)$ (se avsnitt 2.1.5) innehåller per definition alla delmängder till A, och $|\mathscr{P}(A)| = 2^{|A|}$ (se avsnitt 2.3).

Men hur många delmängder finns det som har en given storlek? Lite terminologi först. Man brukar tala om k-kombinationer av mängden A, när man avser delmängder med kardinaliteten k. Alltså: En mängd K är en k-kombination av mängden A om och endast om $K \subseteq A$ och $|K| = k$.

Antalet olika k-kombinationer av en mängd med n element har en speciell beteckning: binomialtal (eller binomialkoefficienter), som brukar skrivas $\binom{n}{k}$, och kan utläsas "n välj k". (Konkretisering: Du blir bjuden 3 valfria bitar ur en chokladlåda med 20 olika praliner: Hur många olika val av dina 3 bitar kan du göra? Jo, $\binom{20}{3} = 1140$.)

Notationen $\binom{n}{k}$ är ännu ett exempel på hur en funktionssymbol kan utformas typografiskt.

Några generellt och relativt uppenbart sanna ekvationer:

$\binom{n}{0} = 1$ (eftersom $\emptyset$ är enda 0-kombinationen).
$\binom{n}{n} = 1$ (eftersom A är den enda n-kombinationen, då $|A| = n$).

$\binom{n}{1} = n$ (en 1-kombination för varje element i A).
$\binom{n}{n-1} = n$ (varje $(n-1)$-kombination svarar mot ett bortplockat element).
$\binom{n}{k} = 0$ om $k > n$ (eftersom inga delmängder till A är större än A).

$\binom{n}{k}$ kan definieras rekursivt på detta sätt (vi skall senare i avsnitt 3.2.2 bevisa att detta stämmer):

$$\binom{n}{k} = \begin{cases} 0 & \text{om } k > n \\ 1 & \text{om } k = 0 \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{om } k \leq n \text{ och } k > 0 \end{cases}$$

Om vi ställer upp dessa värden med en rad för varje värde på $n \geq 0$, en cell för varje värde på k när $0 \leq k \leq n$, och centrerar raderna, så får vi denna tabell, som kallas ”Pascals triangel”.

			1				$n = 0$
		1		1			$n = 1$
	1		2		1		$n = 2$
1		3		3		1	$n = 3$
1		4		6		4	1 $n = 4$
1		5		10		10	5 1 $n = 5$
1	6		15		20		15 6 1 $n = 6$

o.s.v.

Den rekursiva ekvationen svarar mot att att varje cell med två värden över sig innehåller summan av dessa.

$\binom{n-1}{k-1}$	$\binom{n-1}{k}$
$\binom{n}{k}$	

Vi får också tänka oss att det finns oändligt med celler med värdet 0 för alla fall då $k > n$, alltså till höger. De definieras av första basfallet.

Värdena för fallen då $\binom{n}{n} = 1$ fås alltså på detta sätt:

$\binom{n-1}{n-1} = 1$	$\binom{n-1}{n} = 0$
$\binom{n}{n} = 1$	

Cellerna med värdet 1 längst till vänster motsvarar andra basfallet (då $k = 0$).

Om du fyller på triangeln med nästföljande 14 rader, så borde du kunna se att $\binom{20}{3} = 1140$. (Gör gärna det som övning, fast den borde inte kännas helt stimulerande ända fram till fullbordan.)

Binomialtalen dyker även upp i binomialutvecklingarna. Dessa räkneregler borde ni ha stött på på gymnasiet:

$$
\begin{aligned}
(a+b)^0 &= \mathbf{1} \\
(a+b)^1 &= \mathbf{1}a + \mathbf{1}b \\
(a+b)^2 &= \mathbf{1}a^2 + \mathbf{2}ab + \mathbf{1}b^2 \\
(a+b)^3 &= \mathbf{1}a^3 + \mathbf{3}a^2b + \mathbf{3}ab^2 + \mathbf{1}b^3 \\
(a+b)^4 &= \mathbf{1}a^4 + \mathbf{4}a^3b + \mathbf{6}a^2b^2 + \mathbf{4}ab^3 + \mathbf{1}b^4 \\
&\text{o.s.v}
\end{aligned}
$$

3.2 Induktionsbevis

Induktion är en teknik för att bevisa egenskaper i samband med objekt som definieras rekursivt. I samband med språkteknologi kan det röra sig om rekursiva algoritmer och dataprogram, och i del 3 av kursen kommer vi också använda oss av induktion för att bevisa egenskaper hos grammatiker.

3.2.1 Induktionsprincipen

Det finns folk som tycker om att ställa upp dominobrickor och sedan välta omkull dem på mer eller mindre dramatiska sätt:

`http://youtu.be/8H4ipvzGkBY`

Det hela bygger på att, om man välter den första brickan och brickorna står så tätt placerade att en fallande bricka slår omkull den nästa, så kommer så småningom alla brickor att välta omkull.

Antag att vi vill bevisa påståendet att ”bricka n välter omkull”, för godtyckliga värden av n. (Vi antar alltså att alla brickor är numrerade från 1 uppåt.) Detta kan vi klara genom två delbevis:

1. Vi visar att bricka 1 välter omkull.
2. Vi visar att om bricka $n-1$ välter omkull så slår den omkull bricka n.

Observera att det andra steget refererar tillbaka till det påstående som vi vill bevisa, men med ett mindre värde av n. Detta steg kallas för **induktionssteg**, och hela

bevisprincipen kallas för **induktionsprincipen**. Det funkar förstås inte bara för dominobrickor. För att illustrera detta går vi till ett annat spel i avsnitt 3.2.3. Innan dess skall vi se på ett induktivt bevis för att binomialtalen ger antalet k-kombinationer av mängder.

3.2.2 Binomialtalen

Som vi såg i avsnitt 3.1.3, så kan binomialtalen definieras så här:

$$\binom{n}{k} = \begin{cases} 0 & \text{om } k > n \text{ (Basfall 1)} \\ 1 & \text{om } k = 0 \text{ (Basfall 2)} \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{om } k \leq n \text{ och } k > 0 \text{ (Rekursiva fallet)} \end{cases}$$

En av innebörderna av dessa tal är följande:

> Antalet olika k-kombinationer (delmängder med k element) av en mängd med n element är $\binom{n}{k}$. (Antalssatsen.)

Denna sats, som vi kan kalla Antalssatsen (inte något vedertaget namn), har vi dock inte bevisat.

Låt oss gå igenom detta bevis och ge konkreta exempelvärden för bevisets svåraste del efteråt.

Om vi har en godtycklig mängd A och ett godtyckligt heltal $k \geq 0$ så kan vi kalla mängden av k-kombinationer av A för K. Detta kan vi även uttrycka så här:

$$K = \{S \mid S \subseteq A \text{ och } |S| = k\}$$

(Direkt konsekvens: $K \subseteq \mathscr{P}(A)$ – Varför?).

Vi skall då bevisa att $|K| = \binom{n}{k}$ med $n = |A|$ (som nu är en parafras av Antalssatsen).

De enklaste fallen är då $n = 0$ vilket innebär samma sak som $A = \emptyset$. Detta ger det induktiva argumentets bassteg. Om $k = 0$, så är $\emptyset$ den enda k-kombinationen. Detta stämmer med definitionens Basfall 2, som implicerar: $\binom{0}{0} = 1$. Om $k > n$ så finns ingen k-kombination ($K = \emptyset$), eftersom ingen delmängd kan innehålla fler element än utgångsmängden (just här $\emptyset$). Detta stämmer med definitionens Basfall 1, vars konsekvens blir $\binom{0}{k} = 0$.

Induktionssteget, för godtyckliga fall när $n > 0$ (alternativt $A \neq \emptyset$), bygger på induktionsantagandet att Antalssatsen är sann för ett godtyckligt fall om den är sann för alla ett snäpp enklare fall (alltså för mängder med kardinaliteten $n-1$). Vi kan dela upp det i två fall:

Fall 1 av induktionssteget, när $k > n$: Då finns ingen k-kombination ($K = \emptyset$), eftersom ingen delmängd kan inehålla fler element än utgångsmängden, $\binom{n}{k} = 0$. Basfall 1 i definitionen ger oss detta.

Fall 2 av induktionssteget, när $k \leq n$: Det finns (eftersom $A \neq \emptyset$) något värde $x \in A$. Låt oss ta (välja ett godtyckligt) x och dela upp K i två disjunkta delmängder (som i sin tur består av delmängder till A – lite komplext).

$$K_1 = \{S \mid S \in K \text{ och } x \in S\}$$
$$K_2 = \{S \mid S \in K \text{ och } x \notin S\}$$

K_1 och K_2 är disjunkta eftersom $x \in S$ och $x \notin S$ aldrig kan vara sanna om samma S. Alltså: $|K| = |K_1| + |K_2|$. (Bevisa detta steg för dig själv!)

Om vi s.a.s. plockar bort x ur varje delmängd i K_1 får vi en mängd av samma kardinalitet, i mängdnotation:

$$L = \{S \mid S' \in K_1 \text{ och } S = S' \setminus \{x\}\}$$

Hur vet vi detta ($|L| = |K_1|$)? Jo, för att deras element står i ett ett-till-ett-förhållande (plocka bort/lägg till x) till varandra.

Vi kan också notera detta:

$$L = \{S \mid S \subseteq A \setminus \{x\} \text{ och } |S| = k-1\}$$

Eller i ord: att L är mängden av $k-1$-kombinationer av $A \setminus \{x\}$, och eftersom (varför?) $|A \setminus \{x\}| = n-1$, så (enligt induktionsantagandet) $|L| = \binom{n-1}{k-1}$.

Sedan hade vi K_2 (k-kombinationerna av A som inte innehåller x), men detta måste vara samma mängd som mängden av alla k-kombinationerna av $A \setminus \{x\}$. (Varför?)

$$K_2 = \{S \mid S \subseteq (A \setminus \{x\}) \text{ och } |S| = k\}$$

och i så fall (enligt induktionsantagandet)

$$|K_2| = \binom{n}{k-1}$$

Tidigare har vi visat att:

$$|K| = |K_1| + |K_2| \text{ och } |K_1| = |L| = \binom{n-1}{k-1}$$

Alltså (för Fall 2 av induktionssteget) vet vi:

$$|K| = |K_1| + |K_2| = \binom{n-1}{k-1} + \binom{n}{k-1}$$

Därmed har vi bevisat antalssatsen induktivt.

Ett konkret exempel på vilken typ av värden vi skulle få i bevisets sista del, med $n = 5$ och $k = 2$.

> Vi kan t.ex. välja:
>
> $A = \{0, 1, 2, 3, 4\}$ (alltså $n = |A| = 5$ och $|\mathscr{P}(A)| = 32$).
>
> Då blir:
>
> $K = \{\{0,1\},\{0,2\},\{0,3\},\{0,4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$
>
> och ta första bästa:
>
> $x = 0$, varvid vi får:
>
> $K_1 = \{\{0,1\},\{0,2\},\{0,3\},\{0,4\}\}$
>
> $K_2 = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$
>
> $L = \{\{1\},\{2\},\{3\},\{4\}\}$
>
> d.v.s. alla 1-kombinationer av {1, 2, 3, 4}). Elementen i K_1 och L står i ett ett-till-ett-förhållande till varandra (exempel på en bijektion, som vi kommer in på senare på kursen), därmed $|K_1| = |L|$.
>
> Och K_2 är alla 2-kombinationer av {1, 2, 3, 4}).

3.2.3 Schackspelets girige uppfinnare

Schack är ett väldigt gammalt spel. Dess tidigaste föregångare uppstod i Indien på 500-talet, alltså ungefär för 1.500 år sedan. Det finns en legend kopplad till spelet:

När spelets uppfinnare visade upp schackspelet till landets härskare blev denne så belåten att han sa åt uppfinnaren att själv välja sin belöning. Uppfinnaren, som var väldigt smart (lite för smart, som det senare skulle visa sig) önskade sig ett riskorn för den första rutan på schackbrädan, och för varje annan ruta på brädan dubbelt så många riskorn som på föregående ruta. Härskaren tyckte att denna önskan lät väldigt modest och beordrade sin kammarherre att räkna ut hur många riskorn det skulle bli totalt och lämna över riset till uppfinnaren.

Vår uppgift är att också göra denna räkning. Strategin är denna: Vi ska först räkna ut hur många riskorn som ligger på ruta n (för godtyckliga värden av n), och sedan lägga ihop alla dessa värden till en summa.

Antalet riskorn på en viss ruta

Låt oss skriva $r(n)$ för antalet riskorn på ruta n.

Fråga: Kan du ställa upp en rekursiv definition av $r(n)$? Vilka är basfallen?

Funktionen $r(n)$ kan definieras så här:

$$r(n) = \begin{cases} 1 & \text{om } n = 1 \\ 2 \cdot r(n-1) & \text{om } n > 1 \end{cases}$$

Vi kan räkna ut några värden av $r(n)$ för konkreta värden av n:

$$r(1) = 1\,, \quad r(2) = 2 \cdot r(1) = 2 \cdot 1 = 2\,, \quad r(3) = 2 \cdot r(2) = 2 \cdot 2 = 4$$

Om vi har kunskaper i Java kan vi skriva en metod som räknar ut $r(n)$:

```
public int r(int n) {              // argument n ett heltal (int)
    if (n == 1) {                  // basfallet
        return 1;                  // resultat 1
    } else {                       // annars, rekursiva fallet
        return 2 * r(n - 1);       // gör rekursivt anrop
    }
}
```

Fråga: Vad händer om man anropar denna metod med ett värde $n < 1$?

Vi bygger in denna metod i en av våra företags produkter och kunderna verkar vara nöjda. Men en dag så kommer vår chef in i rummet med en lysande idé för hur produkten kan förbättras: Hon föreslår att vår metod ska ersättas med den mycket kortare metoden

```
public int r(int n) {
    return Math.pow(2, n - 1);
}
```

Anropet `Math.pow(double a, double b)` returnerar potensen a^b.

Denna förenkling vore snygg förstås, men vi är inte helt övertygade om att de två metoderna verkligen gör samma sak och sätter oss därför ner för att bevisa det. För att göra detta kan vi använda oss av induktionsprincipen.

Fråga: Vilket påstående måste vi bevisa?

Vi måste bevisa påståendet att $r(n) = 2^{n-1}$.

Vi vill bevisa påståendet att $r(n) = 2^{n-1}$. Induktionsprincipen säger att vi kan bevisa detta genom att visa två saker:

1. Vi måste visa att påståendet är sant för $n = 1$.
2. Vi måste visa att, om påståendet är sant för $n-1$, så är det även sant för n.

Kontroll: Innan man börjar ett induktionsbevis är det bra att kontrollera att påståendet kan stämma genom att räkna ut några konkreta värden. (I det här sammanhanget är det kanske bra att repetera lite potensräkning.)

$$\begin{aligned} r(1) &= 1 & 2^{1-1} &= 2^0 = 1 \\ r(2) &= 2 & 2^{2-1} &= 2^1 = 2 \\ r(3) &= 4 & 2^{3-1} &= 2^2 = 4 \end{aligned}$$

Ja, det verkar ju stämma bra.

Basfall: Vi måste visa att påståendet är sant för $n = 1$. I det här fallet är det bara att räkna: Genom att använda definitionen för $r(n)$ får vi $r(1) = 1$; och $2^{1-1} = 1$, som vi ju redan konstaterat i kontrollen.

Induktionssteg: Vi måste bevisa att, om påståendet är sant för $n-1$, så är det även sant för n. Så låt oss anta att påståendet är sant för $n-1$.

Fråga: Vad innebär detta antagande?

Det innebär att om $n > 1$, så är $r(n-1) = 2^{n-2}$.

Vi får anta att $r(n-1) = 2^{n-2}$ $(n > 1)$. Nu måste vi visa att $r(n) = 2^{n-1}$.

$$\begin{aligned} r(n) &= 2 \cdot r(n-1) && \text{(definition av } r(n)\text{)} \\ &= 2 \cdot 2^{n-2} && \text{(antagandet)} \\ &= 2^{n-1} && \text{(potensräkning)} \end{aligned}$$

Och detta var vad vi ville visa. Så vår chef tycks ha legat rätt för en gångs skull.

Antalet riskorn på schackbrädan

Nu kan vi alltså räkna ut antalet riskorn på en viss ruta på schackbrädan. Det totala antalet riskorn på brädan är summan av alla dessa värden:

$$r(1)+r(2)+\cdots+r(63)+r(64) \quad = \quad 2^0+2^1+\cdots+2^{62}+2^{63}$$

Detta kan vi skriva lite mera koncist genom att använda oss av summanotationen:

$$\sum_{i=1}^{64} r(i) \quad = \quad \sum_{i=1}^{64} 2^{i-1}$$

Låt oss mera allmänt skriva $R(n)$ (med stort R!) för det totala antalet riskorn på en schackbräda med n rutor. Då får vi

$$R(n) \;=\; \sum_{i=1}^{n} 2^{i-1}$$

Även här är det inte svårt att skriva en rekursiv Java-metod som räknar ut denna uttryck. Denna metod bygger på den rekursiva definitionen

$$R(n) \;=\; \begin{cases} 0 & \text{om } n = 0 \\ R(n-1)+r(n) & \text{om } n > 0 \end{cases}$$

Notera att basfallet här är $n = 0$; detta motsvarar den tomma summan.

Men vår petiga chef har än bättre idé igen: Hon påstår att $R(n) = 2^n - 1$, vilket innebär att vi inte behöver en rekursiv metod utan para en enkel potensiering för att räkna ut $R(n)$. Men det måste vi alltså bevisa igen ...

Kontroll: (Den får ni göra själva. Det är bra att göra den, men man brukar inte skriva ner den när man presenterar ett induktionsbevis i en bok eller liknande.)

Basfall: Vi måste visa att påståendet gäller för $n = 0$. (Inte $n = 1$!) Det är bara att räkna: $R(0) = 0$ och $2^0 - 1 = 1 - 1 = 0$, så det stämmer.

Induktionssteg: Vi måste visa att, om påståendet gäller för $n-1$ ($n > 0$), så gäller det även för n. Vi antar alltså att $R(n-1) = 2^{n-1} - 1$ och visar att $R(n) = 2^n - 1$.

$$\begin{aligned} R(n) &= R(n-1)+r(n) && \text{(definition av } R(n)\text{)} \\ &= 2^{n-1}-1+r(n) && \text{(antagendet)} \\ &= 2^{n-1}-1+2^{n-1} && \text{(vårt tidigare bevis att } r(n)=2^{n-1}\text{)} \\ &= 2\cdot 2^{n-1}-1 \\ &= 2^n-1\,. \end{aligned}$$

Då hade chefen rätt igen! Kanske det beror på hennes gedigna utbildning inom diskret matematik?

Det finns 64 rutor på en schackbräda. Om vi lägger ihop antalet riskorn får vi alltså

$$R(64) \;=\; 2^{64}-1 \;=\; 18.446.744.073.709.551.615 \;\sim\; 18.4 \text{ triljoner}$$

Hur mycket är det? (Låt oss fråga Hjärnkontoret: `http://www.svtplay.se/klipp/179080/hur-manga-riskorn-innehaller-ett-kilo-ris`.)

Det går alltså ungefär 48.000 riskorn på ett kilo ris. Man kan då räkna ut att 18.4 triljoner riskorn motsvarar ca. 384,3 gigaton ($384,3 \cdot 10^9$ ton) ris. Världsproduktionen ris år 2009 var 678 megaton ($678 \cdot 10^6$ ton). Väldigt grovt kan man alltså säga att antalet ris på en schackbräda skulle vara ungefär 1.000 gånger så mycket som produceras i hela världen på ett år.

När kungens kammarherre hade berättat detta för kungen låt denne hugga av uppfinnarens huvud för att sätta stopp för dennes matematiska fräckhet.

Potensräkning (förklarande not)

Kom ihåg vår notation för summor och produkter. Två specialfall:

$$\sum_{i=1}^{n} k \;=\; \underbrace{k+\cdots+k}_{n \text{ gånger}} \;=\; n \cdot k \qquad\qquad \prod_{i=1}^{n} k \;=\; \underbrace{k \cdot \cdots \cdot k}_{n \text{ gånger}} \;=\; k^n$$

När summan eller produkten är tom:

$$\sum_{i=1}^{0} k \;=\; 0 \qquad\qquad \prod_{i=1}^{0} k \;=\; 1 \;=\; k^0$$

I bevisen har vi använt oss av denna regel:

$$2 \cdot 2^{n-2} \;=\; 2 \cdot \underbrace{2 \cdot \cdots \cdot 2}_{n-2 \text{ gånger}} \;=\; \underbrace{2 \cdot \cdots \cdot 2}_{n-1 \text{ gånger}} \;=\; 2^{n-1}$$

Mera allmänt gäller:

$$k^m \cdot k^n \;=\; \underbrace{k \cdot \cdots \cdot k}_{m \text{ gånger}} \cdot \underbrace{k \cdot \cdots \cdot k}_{n \text{ gånger}} \;=\; \underbrace{k \cdot \cdots \cdot k}_{m+n \text{ gånger}} \;=\; k^{m+n}$$