Diskret matematik

Gunnar Bergström

20 september 2005

Innehåll

1 Logik och mängdlära **1**
1.1 Satslogik 1
1.1.1 Utsagor 1
1.1.2 Konnektiv 2
1.1.3 Tautolgi och motsägelse 5
1.2 Mängdlära 9
1.2.1 Några talmängder 9
1.2.2 Likhet, = ... 10
1.2.3 Grundmängd 10
1.2.4 Den tomma mängden, $\emptyset$ 10
1.2.5 Komplementmängd, A' 10
1.2.6 Snitt, $\cap$ 10
1.2.7 Union, $\cup$ 10
1.2.8 Delmängd,$\subset$ 11
1.2.9 Sammanfattning 11
1.2.10 Produktmängd, $A \times B$ 11
1.3 Predikatlogik 12
1.3.1 Öppna utsagor 12
1.3.2 Kvantorer 13
1.3.3 Negering av kvantifierade utsagor 14
1.4 Teoriuppbyggnad 14

2 De hela talen **17**
2.1 Delbarhetsegenskaper 17
2.2 Räkning med rester 19
2.3 Största gemensamma delaren 20
2.3.1 Euklides algoritm 20
2.3.2 Minsta gemensamma multipeln 21
2.3.3 Diofantiska ekvationer 23
2.3.4 Olika talsystem 25

3 Induktion och rekursion **29**
3.1 Induktionsprincipen 29
3.1.1 Övningar på induktionsbevis 32
3.2 Rekursiva följder och procedurer 32
3.2.1 Rekursiva definitioner 34
3.3 Linjära rekurrensekvationer 34
3.3.1 Homogena linjära rekurrensekvationer av första och andra ordningen med konstanta koefficienter . 34
3.3.2 ... och inhomogena 36

4 Kombinatorik **39**
4.1 Dirichlets lådprincip 39
4.2 Antalet element i ändliga mängder 40
4.2.1 n-tiplar 40
4.2.2 Multiplikationspricipen 40
4.2.3 Permutationer 41
4.2.4 Kombinationer och binomialkoefficienter 42
4.3 Binomialteoremet 44
4.3.1 Egenskaper hos binomialkoefficienter 44
4.3.2 Binomialteoremet 45
4.4 Oändliga mängder 47
4.4.1 Uppräkneliga mängder 47
4.4.2 Icke uppräkneliga mängder 48

Svar till övningsuppgifterna **51**

Kapitel 1

Logik och mängdlära

Logiken som vetenskap tog sin början i antiken där bl. a. *stoikerna*, c:a 300 f Kr, formulerade regler för korrekt tänkande som står sig väl än i dag. Mängdläran introducerades av *G. Cantor* i slutet av 1800-talet. Logiken och mängdläran i sin moderna form har grundläggande betydelse för datavetenskapen. Man kan säga att mängdläran handlar om datamängdernas och logiken om dataprogrammens strukturer.

1.1 Satslogik

1.1.1 Utsagor

Utsagor är språkliga uttryck som har *mening* eller *sanningsvärde*, dvs antingen är sanna (S) eller falska (F). En utsaga *gäller* om den är sann. Följande är inte utsagor:

Aj!

Vad är klockan?

Håll tyst!

$89 + 116x - \sin x$

Exempel på utsagor:

$5 + 9 = 11$ (falsk)

Kon är i bastun

$\sqrt{23}$ är inte ett rationellt tal

Toronto är inte huvudstad i Canada.

Toronto är huvudstad i Canada.

1.1.2 Konnektiv

Utsagor kan sammansättas eller negeras av *konnektiven* "icke", "och", "eller", "om ... så" med flera.

"Icke", ¬, NOT

$\neg p$ är *negationen* eller *motsatsen* till p.

p: Det är fullsatt.

$\neg p$: Det finns platser kvar.

"$\neg(x > 5)$" är detsamma som "$x \leq 5$" (x reellt tal).

Sanningsvärdetabellen för ¬ är enkel:

p	$\neg p$
S	F
F	S

"och", ∧, AND, &&

$p \wedge q$ kallas *konjunktionen* av p och q och är sann då och endast då både p och q gäller. Exempel på sammansättning med ∧:

"Det blåser och regnar" dvs (det blåser)∧(det regnar)

"$(x > 7) \wedge (x < 9)$" , detsamma som "$7 < x < 9$"

$p \wedge q$ är sann bara då både p och q gäller. Sanningstabell för ∧:

p	q	$p \wedge q$
S	S	S
S	F	F
F	S	F
F	F	F

"eller", ∨, OR ...

$p \vee q$ är *disjunktionen* av p och q. Den är sann då och endast då någon av p och q (eller båda) gäller.

"Det är kappsegling eller (det är)lördag." (Eventuellt gäller båda.)

p	q	$p \vee q$
S	S	S
S	F	S
F	S	S
F	F	F

Negation av konjunktioner och disjunktioner:

$\neg(p \wedge q)$ är detsamma som $(\neg p) \vee (\neg q)$

$\neg(p \vee q)$ är detsamma som $(\neg p) \wedge (\neg q)$

Implikation, $\Rightarrow$, "medför", "om $\cdots$ så"

Implikationen $p \Rightarrow q$ är en utsaga som är falsk, då p är sann men q är falsk, och sann annars.
p kallas *förutsättning* (eller *premiss* eller *hypotes*) och q kallas *slutsats* (eller *konsekvens*).

"Om det regnar så tar jag bussen."

$(x > 1) \Rightarrow (x^2 > 1)$ (S)

$(x^2 > 1) \Rightarrow (x > 1)$ (F)

Sanningstabellen ser ut så här

p	q	$p \Rightarrow q$
S	S	S
S	F	F
F	S	S
F	F	S

Observera att ur en falsk utsaga kan vad som helst följa!

Anm. Implikation är inte oberoende av de andra konnektiven. Uttrycket $\neg p \vee q$ har precis samma sanningstabell som $p \Rightarrow q$, dvs

$$p \Rightarrow q \text{ är detsamma som } \neg p \vee q$$

Visa detta som övning.

Med "$p \Leftarrow q$" menas förstås "$q \Rightarrow p$".

Att $p \Rightarrow q$ formuleras ibland så att

> p är ett *tillräckligt* villkor för q
> (Att det regnar är tillräckligt för att jag ska ta bussen)
>
> q är ett *nödvändigt* villkor för p
> (Det är nödvändigt att jag tar bussen då det regnar)
>
> p gäller *endast då* q gäller.
> (Det regnar endast då jag tar bussen)

De flesta av matematikens satser kan skrivas som implikationer.

Utgående från implikationen $p \Rightarrow q$ kan man bilda

> Den *kontrapositiva formen* $\neg q \Rightarrow \neg p$ (som logiskt sett är detsamma som $p \Rightarrow q$).
>
> *Omvändningen* $q \Rightarrow p$ (som inte behöver gälla även om $p \Rightarrow q$ är sann).

Exempel 1.1.1 Formulera den kontrapositiva formen och omvändningen till utsagan "Om det är torsdag så har jag en tenta idag."

Lösning: Den kontrapositiva utsagan är "Om jag inte har tenta idag är det inte torsdag."
Omvändningen är "Om jag tentar idag är det torsdag."

Att en implikation är sann behöver inte innebära att omvändningen gäller! Exempelvis gäller $x > y \Rightarrow x^2 > y^2$ för alla reella tal x och y men inte omvändningen, eftersom $(-3)^2 > (-2)^2$ men $-3 \not> -2$.

En övning

1. Vilken är den kontrapositiva formen till utsagan "Om det regnar tar jag bussen"?

Ekvivalens, $\Leftrightarrow$, om och endast om ..

$p \Leftrightarrow q$ betyder att p och q antingen båda är sanna eller båda falska. Exempel:

$$x^2 - 5x + 6 = 0 \Leftrightarrow (x = 2) \vee (x = 3)$$

Tabellen för $\Leftrightarrow$:

p	q	$p \Leftrightarrow q$
S	S	S
S	F	F
F	S	F
F	F	S

1.1.3 Tautolgi och motsägelse

En (sammansatt) utsaga är en *tautologi*, om den alltid är sann oberoende av de ingående utsagornas sanningsvärde, dvs är sanna i varje tolkning av de ingående delutsagorna.

Exempel 1.1.2 Vi visar med en sanningsvärdestabell att

$$[p \wedge (p \Rightarrow q)] \Rightarrow q$$

är en tautologi

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$[p \wedge (p \Rightarrow q)] \Rightarrow q$
S	S	S	S	S
S	F	F	F	S
F	S	S	F	S
F	F	S	F	S

Exempel 1.1.3 Visa att varje implikation är ekvivalent med sin kontrapositiva utsaga.
Lösning: Vi gör en (annorlunda) sanningstabell för utsagan

(	p	$\Rightarrow$	q	)	$\Leftrightarrow$	(	$\neg$	q	$\Rightarrow$	$\neg$	p	)
	S	S	S		S		F		S	F		
	S	F	F		S		S		F	F		
	F	S	S		S		F		S	S		
	F	S	F		S		S		S	S		

Alla giltiga härledningsregler är tautologier. Exempelvis metoden "uppdelning i fall".

Exempel 1.1.4 Visa att $x^2 \geq 0$.
Lösning

Fall 1: $x \geq 0$. Det är då tillåtet att multiplicera olikheten $x \geq 0$ med x, som ju är ≥ 0 vilket ger $x \cdot x \geq 0 \cdot x$, dvs $x^2 \geq 0$.

Fall 2: $x < 0$. Då är $-x > 0$ och alltså $(-x)(-x) > 0 \cdot (-x) = 0$ varav följer $x^2 > 0$ och därmed $x^2 \geq 0$ även i detta fall.

Mönstret formaliseras så här:

$$[(p \Rightarrow q) \wedge ((\neg p) \Rightarrow q)] \Rightarrow q$$

som lätt kan konstateras vara en tautologi.

En utsaga som alltid är falsk, oberoende av de ingående enkla utsagornas sanningsvärden, kallas en *motsägelse*. Typfall $w \wedge (\neg w)$

Tekniken med motsägelsebevis

Om man vill bevisa ett påstående kan man göra så att man visar att om påståendet inte vore sant skulle det leda till orimligheter. Vi agerar då enligt följande mönster:

Vi vill visa att utsagan p är sann.

Antag $\neg p$

Då följer en motsägelse

Alltså gäller p

Med logiska konnektiv kan härledningsmönstret skrivas

$$[(\neg p) \Rightarrow (w \wedge (\neg w))] \Rightarrow p$$

som lätt kan verifieras med en sanningstabell. (Gör det som övning.)

Exempel 1.1.5 Visa att ekvationen $2x+1 = 2(x+1)$ saknar lösning.

Antag att $2x + 1 = 2(x + 1)$ för något x.

Då är $2x + 1 = 2x + 2$

Minska med $2x$ i båda leden så följer $1 = 2$ som motsäger $1 \neq 2$

Alltså finns ingen lösning.

Motexempelmetoden

Metoden med sanningstabell för att verifiera en tautologi har sina begränsningar. Antalet rader i tabellen blir 2 upphöjt till antalet delutsagor, så 10 olika enkla usagor skulle ger 1024 rader i sanningstabellen! I stället kan man på ett systematiskt sätt undersöka vad existensen av ett motexempel skulle innebära:

Exempel 1.1.6 Är

$$[(p \Rightarrow q) \wedge (\neg q \vee r)] \Rightarrow (p \Rightarrow r)$$

sann i alla tolkningar av utsagorna p, q, r?

Om denna implikation är falsk är $[(p \Rightarrow q) \wedge (\neg q \vee r)]$ sann och $p \Rightarrow r$ falsk.

Då är $p \Rightarrow q$ sann, $\neg q \vee r$ sann, p sann, r falsk.

Då är q sann, eftersom $p \Rightarrow q$. Men om $\neg q \vee r$ sann och r falsk så måste $\neg q$ också vara sann!

Vi har därmed en motsägelse (på meta-nivån). Alltså kan det inte finnas något motexempel.

Alltså är $[(p \Rightarrow q) \wedge (\neg q \vee r)] \Rightarrow (p \Rightarrow r)$ en tautologi!

Ett schema för detta resonemang kan göras som följer, där varje ny slutsats görs på en ny rad:

$[(p \Rightarrow q) \wedge (\neg q \vee r)] \Rightarrow (p \Rightarrow r)$
F
S F
S S F
S S
F *motsägelse!*

En utveckling av denna metod (G Ståhlmark, ca 1990) är ett mycket framgångsrikt verktyg vid kontroll av datorprogram och reglersystem. Formler med 10^5 "atomer" kan hanteras!

Övningar på satslogik

2. Formalisera följande utsagor

   a. Han är inte nykter.

   b. Hon är både lärd och vacker.

   c. Har man sagt A får man säga B.

   d. En svala gör ingen sommar.

3. Vilken är den kontrapositiva formen till utsagan "Den som sover syndar icke"? Vilken är omvändningen?

4. Avgör om följande påståenden är sanna eller falska:

   a. Om $1 + 1 = 3$ så är $2 + 2 = 5$

   b. Om $1 + 1 = 3$ så är $2 + 2 = 4$

   c. Om $1 + 1 = 2$ så är $2 + 2 = 5$

   d. Om kor kan flyga så är jag skapt som en nors.

   e. Om $2 + 2 = 5$ existerar ett högre väsen.

   f. Om $2 + 2 = 4$ så är $1 + 2 = 3$

5. Gör en sanningstabell för den sammansatta utsagan

   a. $(p \vee \neg q) \Rightarrow q$

   b. $(p \Rightarrow q) \vee (q \Rightarrow p)$

6. Visa att

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \;\Rightarrow\; (p \Rightarrow r)$$

   är en tautologi.

7. Visa att en implikation alltid är ekvivalent med sin kontrapositiva form, dvs att

$$(\neg q \Rightarrow \neg p) \Leftrightarrow (p \Rightarrow q)$$

   är sann för alla tolkningar av p och q.

8. Avgör om härledningsmönstret

$$\begin{array}{rr} p \Rightarrow q \\ \neg p \Rightarrow q \\ \hline \therefore \qquad q \end{array}$$

är en giltig härledningsregel.
(*Ledning:* Formalisera mönstret till en sammansatt utsaga och visa att den är tautologisk.)

9. Formalisera

   a. Om alla gör sitt bästa och vi samarbetar så kan vi inte misslyckas.

   b. Om det finns en bra film eller ett naturprogram så tittar vi på TV, annars får det vara.

   c. Han är varken lat eller dum

   d. Ekvationen $x^2 + x = 6$ har lösningarna $x = 2$, $x = -3$.

10. Använd "motexempelmetoden" för att avgöra om följande formaliserade utsagor är tautologiskt sanna eller inte:

   a. $[(p \Rightarrow q) \wedge (q \Rightarrow r) \wedge (r \Rightarrow s)] \;\Rightarrow\; (p \Rightarrow s)$

   b. $(p \Rightarrow q) \vee [(r \Rightarrow \neg q) \wedge (r \Rightarrow s)] \;\Rightarrow\; (p \Rightarrow s)$

1.2 Mängdlära

En *mängd* är en samling av vissa objekt, *element*.
En mängd kan anges genom uppräkning av dess element inom $\{\}$, exempelvis $A = \{1, 2, 3, 4\}$, eller genom en *definierande utsaga*, till exempel

$$B = \{x; x \text{ är ett reellt tal och } 1 < x < 2\}$$

Att x är ett element i mängden M skrivs $x \in M$, "x tillhör M".
Så gäller till exempel $1 \in A$, $3 \in A$ men $5 \notin B$.

1.2.1 Några talmängder

De naturliga talen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

De hela talen $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

De rationella talen $\mathbb{Q} = \{p/q; p \in \mathbb{Z},\ q \in \mathbb{Z},\ q \neq 0\}$

1.2.2 Likhet, =

Två mängder är *lika* om de innehåller samma element, som till exempel $\{1, 3, 7\} = \{7, 3, 1\} = \{3, 1, 7, 7, 1\}$.

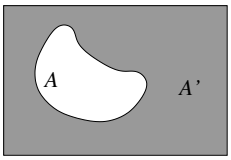
1.2.3 Grundmängd

Det finns alltid en *grundmängd* eller *univers* U. Den kan vara alla reella tal, alla människor i Göteborg eller dylikt. Ingen mängd kan innehålla allting, det skulle leda till motsägelser.

1.2.4 Den tomma mängden, $\emptyset$

Den tomma mängden, $\emptyset$ innehåller inga element, $\emptyset = \{\} = \{x; x \neq x\}$.

1.2.5 Komplementmängd, A'

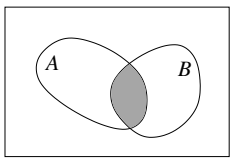


Komplementet till A , A' består av alla element som inte ligger i A,

$$A' = \{x; x \notin A\}$$

Exempel: $\emptyset' = U$ (den aktuella grundmängden) , $U' = \emptyset$, $\{x; |x| < 7\}' = \{x; |x| \geq 7\}$.

1.2.6 Snitt, $\cap$

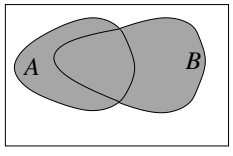


Snittet eller *skärningsmängden* $A \cap B$ av två mängder A och B definieras genom

$$A \cap B = \{x; x \in A \wedge x \in B\}$$

Exempel: $\{x; 1 < x < 3\} \cap \{x; 2 \leq x \leq 5\} = \{x; 2 \leq x < 3\}$.
Exempel: $\{1, 2\} \cap \{3, 4\} = \emptyset$
Om $A \cap B = \emptyset$ är A och B *disjunkta*.

1.2.7 Union, $\cup$



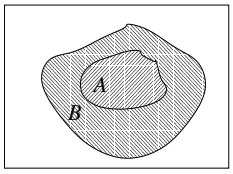
Unionen eller *föreningsmängden* $A \cup B$ av två mängder A och B definieras genom

$$A \cup B = \{x; x \in A \vee x \in B\}$$

Exempel: $\{x; 1 < x < 3\} \cup \{x; 2 \leq x \leq 5\} = \{x; 1 < x \leq 5\}$.

1.2.8 Delmängd,$\subset$

Mängden A är en *delmängd* av mängden B om och endast om varje element i A är ett element i B, dvs



$$A \subset B \text{ om och endast om } x \in A \Rightarrow x \in B$$

Exempel: $\{3,4,5\} \subset \{1,2,3,4,5\}$
Exempel: $\emptyset \subset M \subset U$ för alla mängder M.
$A = B$ är ekvivalent med $A \subset B \wedge B \subset A$

1.2.9 Sammanfattning

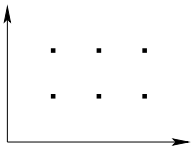
$x \in A'$	är detsamma som	$\neg(x \in A)$
$x \in A \cap B$	är detsamma som	$(x \in A) \wedge (x \in B)$
$x \in A \cup B$	är detsamma som	$(x \in A) \vee (x \in B)$
$A \subset B$	är detsamma som	$(x \in A) \Rightarrow (x \in B)$
$A = B$	är detsamma som	$(x \in A) \Leftrightarrow (x \in B)$

1.2.10 Produktmängd, $A \times B$

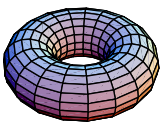
Låt a och b vara två objekt. Av dem kan man bilda det *ordnade paret* a, b. Om $a \neq b$ är $(a,b) \neq (b,a)$. Två ordnade par (a,b) och (x,y) är lika om och endast om $a = x$ och $b = y$.

Låt A och B vara två mängder. *Produktmängden* eller den *Cartesiska produkten* av A och B, $A \times B$ är mängden av ordnade par (a,b), där $a \in A$ och $b \in B$.

Exempel 1.2.1 $\{1,2,3\}\times\{a,b\} = \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$.



Exempel 1.2.2 Låt $\mathbb{R}$ vara de reella talen. $\mathbb{R}\times\mathbb{R}$ kan enkelt åskådliggöras i ett (tvådimensionellt) koordinatsystem, där varje talpar motsvars av en punkt i planet.



Exempel 1.2.3 En *torus* kan uppfattas som produkten $C \times C$ där C är punkterna på en cirkel.

Övningsuppgifter på mängder:

11. Skriv $\{a, 4, a, b, 3, a, b, c, 2, a, b, c, d, 1\}$ på ett enklare sätt

12. Låt $A = \{x; x = 4k + 1 \text{ och } k \in \mathbb{N}\}$
och $B = \{x; x = 3k + 5 \text{ och } k \in \mathbb{N}\}$

    a. Skriv de 10 första elementen i $A \cup B$

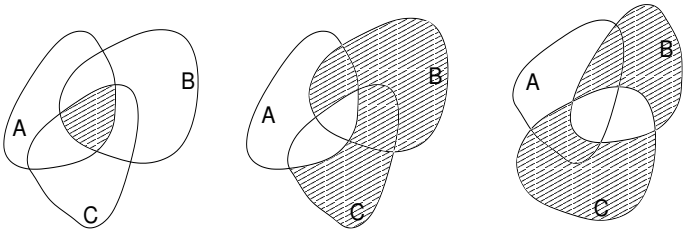
    b. Skriv upp de 4 första elementen i $A \cap B$

13. Visa de Morgans lagar : $(A \cup B)' = A' \cap B'$ och $(A \cap B)' = A' \cup B'$.

14. Visa distributiva lagarna för $\cap$ och $\cup$:

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

15. Tre mängder, A, B och C skär varann som i figurerna. Beskriv med mängdoperationer de markerade delmängderna av $A \cup B \cup C$



1.3 Predikatlogik

1.3.1 Öppna utsagor

Utsagor i matematisk text och datorprogram innehåller ofta *varibler* till exempel

$x > 3$

$x = y + 3$

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

if $x > 0$ **then** $x := x + 1$

Sådana utsagor kallas *öppna*. Deras sanningsvärde beror på vad man ersätter variablerna med. Fler exempel:

$x + 2 \geq 3$ (sann, då $x > 1$, falsk, då $x \leq 1$)

n är ett udda heltal (sann, då $n = \pm 1, \pm 3, \pm 5, \ldots$)

Om $P(x)$ är förkortning för "x är större än 3" så är till exempel $P(4)$ sann men $P(8/3)$ falsk. Om $Q(x, y, z)$ står för $x^2 + y^2 = z^2$ är $Q(3, 4, 5)$ och $Q(5, 12, 13)$ sanna men $Q(2, 3, 4)$ falsk.

Sanningsmängden för en öppen utsaga är mängden av de objekt för vilka utsagan gäller (är sann), dvs $\{x; P(x)$ är sann$\}$.

Utsagan "$x^2 \leq 4$" har sanningsmängden (eller *lösningsmängd en*) $\{x : -2 \leq x \leq 2\}$

I utsagan "x är större än 3" är variabeln x *subjekt* och "är större än 3" *predikat*, dvs egenskapen som x utsägs ha.

1.3.2 Kvantorer

Då man "sätter in" något i stället för variablerna i en öppen utsaga så att den blir meningsfull *sluter* man den. Öppna utsagor kan också slutas med *kvantorer* (kallas även *kvantifikatorer*. Vi använder i matematiken två kvantorer, existenskvantorn $\exists$ och universalkvantorn eller all-kvantorn $\forall$.

"Det finns ett tal x sådant att $x^2 = -1$."
Existenskvantorn motsvarar i vanligt språkbruk uttryck som "Det finns ett" i "Det finns ett x sådan att $P(x)$", "för minst ett" i "$P(x)$ gäller för minst ett x" och liknande. Formaliseras till

$$\exists x \ P(x)$$

"Alla däggdjur har päls."

Allkvantorn används i *allmänna utsagor* då man vill slå fast att en viss egenskap gäller för alla x under övervägande (i grundmängden): "$P(x)$ gäller för alla x."

$$\forall x \ P(x)$$

Man kan ha flera kvantorer, om man har flera variabler. "Alla har sett någon av filmerna " kan formaliseras $\forall x \ \exists y \ Q(x, y)$.

$\exists y \ \forall x \ Q(x, y)$ betyder däremot "Det finns en film som alla har sett." Kvantorernas ordning har alltså betydelse.

1.3.3 Negering av kvantifierade utsagor

Att inte alla x har egenskapen P innebär ju att något x inte har egenskapen P. Motsatsen till $\forall x\ P(x)$ är tydligen $\exists x\ \neg P(x)$. Formaliserat:

$$\neg(\forall x\ P(x)) \ \Leftrightarrow\ \exists x\ \neg P(x)$$

Att det inte är sant att det finns ett x med egenskapen $P(x)$ måste betyda att alla x saknar egenskapen $P(x)$. Motsatsen till $\exists x\ P(x)$ är således $\forall x\ \neg P(x)$. I formel:

$$\neg(\exists\ P(x)) \ \Leftrightarrow\ \forall x\ \neg P(x)$$

Exempel Motsatsen till "Alla Göteborgare talar fort och otydligt" är "Det finns en göteborgare som talar långsamt eller tydligt". Motsatsen till "Det finns ett tal som är större än 100" är "Alla tal är mindre än 100"

Övnigar

16. Formalisera följande utsagor med kvantorerna $\forall$ och $\exists$.

    a. Alla elever klarade tentan.

    b. Någon elev klarade alla prov.

    c. Alla prov klarades av någon elev.

    d. Alla präster är prostar.

    e. Ingen elev klarade alla prov.

    f. Högst 70 personer var där.

    g. Det finns ett tal som är större än eller lika med alla andra tal.

17. Formulera i positiv form motsatsen till utsagorna i föregående uppgift.

1.4 Teoriuppbyggnad

En (matematisk eller annan) teori brukar vara uppbyggd så att den från början består av ett antal utsagor som betraktas som sanna, så kallade *axiom*, från vilka andra sanna utsagor, *satser* eller *teorem*, härleds varefter nya sanna utsagor kan härledas och så vidare.

Det är viktigt att man kan kontrollera att en härledning, ett *bevis* är korrekt gjord. Ett bevis skall därför i princip kunna brytas ned i enkla härledningsmönster, så kallade *syllogismer* av vilka vi listar några i en tabell. ($\therefore$ betyder "alltså" och betcknar en giltig slutsats ur vad som står ovanför)

Regler för	*Införande*		*Elimination*
negation	$\dfrac{\neg(\neg p)}{\therefore p}$	$\dfrac{p}{\therefore \neg(\neg p)}$	$\dfrac{\begin{array}{c}\text{Antag } \neg p \\ \text{Då en motsägelse}\end{array}}{\therefore p}$
konjunktion	$\dfrac{\begin{array}{c}p \\ q\end{array}}{\therefore p \wedge q}$		$\begin{array}{c}p \wedge q \\ \hline \therefore p \\ \therefore q\end{array}$
disjunktion	$\dfrac{p}{\therefore p \vee q}$	$\dfrac{q}{\therefore p \vee q}$	$\dfrac{\begin{array}{c}p \vee q \\ p \Rightarrow r \\ q \Rightarrow r\end{array}}{\therefore r}$
implikation	$\dfrac{\begin{array}{c}\text{Antag } p \\ \text{Då } q\end{array}}{\therefore p \Rightarrow q}$		$\dfrac{\begin{array}{c}p \\ p \Rightarrow q\end{array}}{\therefore q}$
ekvivalens	$\dfrac{\begin{array}{c}p \Rightarrow q \\ q \Rightarrow p\end{array}}{\therefore p \Leftrightarrow q}$		$\begin{array}{c}p \Leftrightarrow q \\ \hline \therefore p \Rightarrow q \\ \therefore q \Rightarrow p\end{array}$

Kapitel 2

De hela talen

2.1 Delbarhetsegenskaper

Betrakta mängden av hela tal

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

med räknesätten addition, subtraktion och division definierade som vanligt (som i grundskolan).

Definition 2.1 *Heltalet a är* delare *till heltalet b om det finns ett heltal c så att $b = a \cdot c$*

Att a är delare till b skrivs $a|b$, "a delar b.

Ex. $17|51$, ty $51 = 17 \cdot 3$.
Ex. 28 har delarna $\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28$.

Definition 2.2 *Alla delare till ett heltal b utom ± 1 och $\pm b$ är* äkta delare

Ex. $\pm 2, \pm 4, \pm 7, \pm 14$ är äkta delare till 28.

Sats 2.1 *. Låt a ,b, c, d vara hela tal*

Om $a|b$ och $a|c$, så gäller $a|(b + c)$ och $a|b \cdot d$.

Om $a|b$ och $b|c$, så gäller $a|c$.

Bevis: Övning. □

Divisionsalgoritmen *Till heltalen a och b, där $b > 0$, finns entydigt bestämda heltal k och r, $0 \leq r < b$ så att*

$$a = b \cdot k + r$$

Talet k är *kvoten* och r *resten.*

Ex. $59 = 17 \cdot 3 + 8$.

Definition 2.3 *Ett* primtal *är ett heltal ≥ 2 som saknar äkta delare.*

M a o är ett primtal ett heltal ≥ 2, vars enda positiva delare är talet själv och 1.
. De första primtalen är $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$.
Det största kända primtalet (september 2003) är $2^{13466917} - 1$, ett s k mersenne-tal med 4053946 siffror.

Hjälpsats 2.2 *Om heltalet m inte är ett primtal, så är den minsta positiva äkta delaren till m ett primtal.*

Bevis: Bland de äkta positiva delarna finns en, d säg, som är minst. Om inte d vore primtal, hade d en äkta positiv delare d_1, som måste vara mindre än d. Eftersom d_1 då också måste dela m motsäger detta att d är den minsta positiva delaren. □

Beviset ovan är ett typiskt motsägelsebevis : Ur negationen till den utsaga p man vill bevisa följer en motsägelse. Alltså måste p gälla.
Beviset till nästa sats är ännu ett exempel på detta.

Sats 2.3 *(Euklides): Det finns oändligt många primtal.*

Bevis: Antag motsatsen, dvs att det bara finns ändligt många primtal. Låt P vara det största primtalet. Bilda talet

$$N = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot P + 1 = P! + 1$$

Den minsta positiva delaren d till N är ett primtal eller är N självt ett primtal . Men inget av talen $1, 2, \ldots, P$ kan vara delare till N, eftersom resten blir 1 då man dividerar N med dessa tal! Då måste d vara ett primtal som är större än P vilket motsäger att P är det största primtalet.
Alltså måste det finnas oändligt många primtal. □

Sats 2.4 *Varje heltal ≥ 2 kan delas upp i primtalsfaktorer*

Bevis: Låt n vara ett positivt heltal. Låt p_1 vara den minsta positiva delaren till n, som ju är primtal. Då finns n_1 så att $n = p_1 \cdot n_1$. Låt nu p_2 vara minsta positiva delaren till n_1 så att $n = p_1 \cdot p_2 \cdot n_2$ och så vidare. Processen måste sluta efter ändligt många steg, och då har vi $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m$, $\square$.

Att primfaktoruppdelningen är entydig visas längre fram.
Ex. $4179240 = 2^3 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 47$.
I programmmeringsspråk förekommer beteckningarna div och mod för kvoten respektive resten: $59 \operatorname{div} 17 = 3$ och $59 \bmod 17 = 8$

Att talen a och b har samma rest vid division med q skrivs

$$a \equiv b \pmod{q}$$

Ex. $59 \equiv 20 \equiv 7 \pmod{13}$

2.2 Räkning med rester

Sats 2.5 *Om heltalen a_1 och a_2 har resterna r_1 respektive r_2 vid division med heltalet q, så gäller*

$a_1 + a_2$ har resten $r_1 + r_2$ vid division med q

$a_1 \cdot a_2$ har resten $r_1 \cdot r_2$ vid division med q

$n \cdot a_1$ har resten $n \cdot r_1$ vid division med q (n heltal)

Bevis:

$a_1 = b_1 \cdot q + r_1$ och $a_2 = b_2 \cdot q + r_2 \Rightarrow a_1 + a_2 = (b_1 + b_2) \cdot q + r_1 + r_2$

$a_1 \cdot b_1 = (b_1 b_2 \cdot q + b_1 r_2 + b_2 r_1) q + r_1 \cdot r_2$

$n \cdot a_1 = n \cdot b_1 \cdot q + n \cdot r_1$. $\square$

Anmärkning Sats 2.5 innebär att om $a_1 \equiv a_2 \pmod{q}$ och $b_1 \equiv b_2 \pmod{q}$ så gäller

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{q} \\ a_1 \cdot b_1 &\equiv a_2 \cdot b_2 \pmod{q} \end{aligned}$$

Exempel 2.2.1 Vilken blir minsta icke-negativa resten, då

(a) $557 \cdot 283 + 355$ divideras med 7?

(b) $17^{29} + 13^{59}$ divideras med 7?

Lösning: Med $\equiv$-beteckningen kan vi jobba så här:

(a) $557{\cdot}283{+}355 = (80{\cdot}7{-}3)(40{\cdot}7{+}3){+}(50{\cdot}7{+}5) \equiv (-3)3{+}5 = -4 \equiv \underline{3} \pmod 7$.

(b)

$$17^{29} + 13^{59} = (2 \cdot 7 + 3)^{29} + (2 \cdot 7 - 1)^{59} \equiv 3^{29} + (-1)^{59} =$$

$$= 3^{3 \cdot 9} \cdot 3^2 - 1 = 27^9 \cdot 9 - 1 =$$

$$\{27 = 28 - 1 = 4 \cdot 7 - 1,\ 9 = 7 + 2\}$$

$$= (4 \cdot 7 - 1)^9 (7 + 2) - 1 \equiv (-1)^9 \cdot 2 - 1 =$$

$$= -2 - 1 = -3 = (-1)7 + 4 \equiv \underline{4} \pmod 7$$

2.3 Största gemensamma delaren

2.3.1 Euklides algoritm

Hur förkortar man bråk med stora täljare och nämnare, som till exempel $\frac{4179240}{573648}$? Vad vi egentligen söker är det största positiva heltalet som delar både täljare och nämnare, *största gemnsamma delaren*, SGD, till 4179240 och 573648. *Euklides algoritm* är en metod som sållar fram SGD genom upprepad användning av divisionsalgoritmen. Först ett exempel:

$$4179240 = 573648 * 7 + 163704$$

$$573648 = 163704 * 3 + 82536$$

$$163704 = 82536 * 1 + 81168$$

$$82536 = 81168 * 1 + 1368$$

$$81168 = 1368 * 59 + 456$$

$$1368 = 456 * 3$$

Den största gemensamma delaren är då 456, skrives $\mathbf{SGD}(4179240, 573648) = 456$ och $\frac{4179240}{573648} = 9165/1258$.

Med allmänna beteckningar blir det så här: Låt a och b vara positiva tal och sök $SGD(a, b)$. Divisionsalgoritmen ger

$$\begin{aligned} a &= b \cdot k_1 + r_1, & 0 \leq r_1 < b \\ b &= r_1 \cdot k_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2 \cdot k_3 + r_3, & 0 \leq r_3 < r_2 \end{aligned}$$

Processen måste ha ett slut (resterna avtar ju strängt)

$$r_{n-2} = r_{n-1} \cdot k_n + r_n, \qquad 0 \leq r_{n-1} < r_n$$

$$r_{n-1} = r_n \cdot k_{n+1}$$

Vi ser nu lätt att $r_n | r_{n-1} \Rightarrow r_n | r_{n-2} \Rightarrow \ldots \Rightarrow r_n | b \Rightarrow r_n | a$! r_n är alltså *gemensam* delare till a och b.
Antag att heltalet d delar både a och b. Eftersom $r_1 = a - b \cdot k_1$, måste d dela r_1, eftersom $r_2 = b - r_1 \cdot k_2$ måste d dela r_2 och så vidare. Vi finner till slut att d delar r_n. r_n är således den *största* gemensamma delaren.

2.3.2 Minsta gemensamma multipeln

Då vi vill addera två rationella tal söker vi ju efter den minsta gemensamma nämnaren, som ju är den *minsta gemensamma multipeln*, MGM, till nämnarna.
Låt a och b vara två heltal $\neq 0$. Vi bryter ut $SGD(a, b)$ ur båda talen och får

$$a = a_1 \cdot SGD(a, b), \quad b = b_1 \cdot SGD(a, b)$$

där $a_1 = a/SGD(a, b)$ och $b_1 = b/SGD(a, b)$. Då är

$$m = a_1 b_1 SGD(a, b) = \frac{a}{SGD(a, b)} \cdot b = \frac{ab}{SGD(a, b)}$$

en gemensam multipel till a och b eftersom både a och b delar detta uttryck. Att m också är den *minsta* gemensamma multipeln lämnas som en (kanske svår) övning.

Exempel 2.3.1 Beräkna $170/81168 - 5/1368$.

Lösning $SGD(81168, 1368) = 456$ (se ovan), så minsta gemensamma nämnaren är

$$MGM(81168, 1368) = \frac{81168 \cdot 1368}{456} = \frac{81168}{456} \cdot 1368 = 178 \cdot 3 \cdot 456$$

$$\frac{170}{81168} - \frac{5}{1368} = \frac{170}{178 \cdot 456} - \frac{5}{3 \cdot 456} = \frac{170 \cdot 3 - 5 \cdot 178}{178 \cdot 3 \cdot 456} = -5/1068$$

Hjälpsats 2.6 *Om a och b är heltal, finns två heltal x och y så att $SGD(a,b) = ax + by$*

Bevis: Gå baklänges i Euklides algoritm. □

Sats 2.7 *Om a och b är heltal och p primtal och $p|ab$ så måste $p|a$ eller $p|b$*

Bevis: Antag $p \not| a$ (annars var ju allt klart).Då är $SGD(p,a) = 1$.
Då finns heltal x och y så att $1 = px + ay$.
Då gäller $pbx + aby = b$.
Men $p \mid ab$ och $p \mid pbx$, alltså $p|b$. □

Hjälpsats 2.8 *Om $a_1, a_2, \ldots, a_n$ är heltal och p ett primtal och $p|a_1a_2 \cdots a_n$ så måste $p|a_k$ för något k, $1 \leq x \leq n$*

Bevis: Om inte $p|a_1$ måste $p|a_2 \cdots a_n$ enligt sats2.7.
Om inte heller $p|a_2$ måste $p|a_3 \cdots a_n$ osv. Efter högst n steg hittar vi a_k sådan att $p|a_k$. □

Nu kan vi visa den fullständiga satsen om uppdelning i primfaktorer av hela tal,

Sats 2.9 (Aritmetikens fundamentalsats) *Varje heltal $a \geq 2$ kan skrivas som en produkt av primtal på ett och endast ett sätt, bortsett från faktorernas ordningsföljd.*

Bevis: Enligt sats 2.4 på sid 19 kan a skrivas som en produkt av primtal. Antag att det går att göra på två sätt, så att

$$a = p_1p_2 \cdots p_m = q_1q_2 \cdots q_n, \ p_k \text{ och } q_i \text{ primtal}$$

Vi kan anta att $m \leq n$. Enligt lemma 2.8 måste $p_1|q_j$ för något j. Det måste innebära att $p_1 = q_j$, eftersom båda är primtal. Vi numrerar om så att q_j blir q_1 och dividerar båda led med $p_1 = q_1$:

$$p_2p_3 \cdots p_m = q_2q_3 \cdots q_n$$

Nu kan vi upprepa förfarandet, p_2 måste vara lika med någon ny q_2 och så vidare. Till slut är alla p_k slut och alla p_k är lika med varsitt q_j. Om det funnes några q_j kvar skulle vi ha

$$1 = q_{m+1} \cdots q_n$$

som är omöjligt eftersom alla primtalen $q_j \geq 2$. Av detta följer entydigheten. □

Vi är nu istånd att bevisa

Sats 2.10 (Satsen om rationella rötter) *Anta att talen $a_0, a_1, \ldots, a_n$ är heltal. En nödvändig förutsättning för att polynomet*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

skall ha en rationell *rot $\alpha = p/q$, där p och q är förkortat så långt det går, är att $p|a_0$ och $q|a_n$.*

Bevis: Antag att $f(p/q) = 0$. Multiplicera med q^n. Då gäller

$$q^n f(\frac{p}{q} = q^n \left(a_0 + a_1 \frac{p}{q} + a_2 \frac{p^2}{q^2} + \cdots + a_n \frac{p^n}{q^n} \right)$$

$$= a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0 \ .$$

Men då gäller

$$p(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1}) = -a_0 q^n$$

Det följer att $p|a_0 q^n$. Eftersom $p \not| q$ och därmed $p \not| q^n$ måste $p|a_0$ enligt sats 2.7 ovan. Att $q|a_n$ bevisas på liknande sätt. □

2.3.3 Diofantiska ekvationer

Diofantiska ekvationer, som har namn efter Diofantos som verkade i Alexandria omkring år 250 e Kr, är ekvationer där de "obekanta" förusättes vara heltal. Vi skall se hur man löser diofantiska ekvationer av typen

$$ax + by = c$$

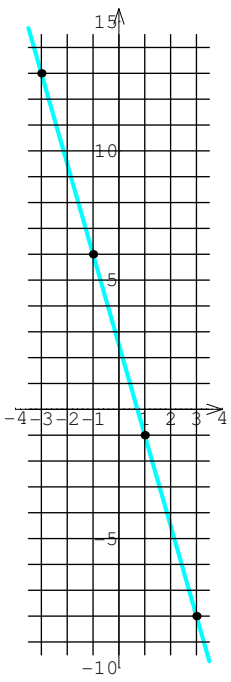
där a, b och c är hela tal och där man söker heltalen x och y.

Först konstaterar vi:

Faktum 2.1 *Om $SGD(a, b) \not| c$ så saknar den diofantiska ekvationen $ax + by = c$ lösningar.*

Bevis: Det följer av $SGD(a, b)|a \wedge SGD(a, b)|b \Rightarrow SGD(a, b)|ax + by \Rightarrow SGD(a, b)|c$. □

I en lösbar diofantisk ekvation kan vi alltså anta att $SGD(a, b) = 1$ (annars kunde vi ju dividera båda sidor med SGD), vilket ofta underförstås i fortsättningen.



Faktum 2.2 *Om x_1, y_1 löser $ax + by = c$, så ges samtliga lösningar av*

$$x = x_1 - bm; \quad y = y_1 + am$$

där m är vilket heltal som helst.

Bevis: Det ger nämligen $ax + by = a(x_1 - bm) + b(y_1 + am) = ax_1 + by_1 + abm - abm = c$.
Om $x = x_1 + u$ och $y = y_1 + v$ är en annan lösning gäller $ax + by = a(x_1 + u) + b(y_1 + v) = c = ax_1 + by_1$, varav följer $au + bv = 0$, dvs $au = -bv$. Det innebär att $a|v$ (eftersom $a \not| b$), dvs $v = a \cdot m$ för något m. Då är $au = -b \cdot a \cdot m$ och alltså $u = -b \cdot m$. □

Exempel 2.3.2 Lös den diofantiska ekvationen $7x + 2y = 5$.
Lösning: Vi hittar ganska lätt en lösning: $x_1 = 1$ och $y_1 = -1$.
Alla heltalslösningar till $7x + 2y = 5$ ges då av

$$x = 1 - 2m \text{ och } y = -1 + 7m$$

Se också figuren i marginalen för en geometrisk tolkning.

I nästa exempel visar vi en metod för att hitta en lösning som bygger på Euklides' algoritm.

Exempel 2.3.3 : Sök alla heltal x, y sådana att $17x + 39y = 2$
Lösning: Euklides algoritm ger:
$39 = 2 \cdot 17 + 5$; $17 = 3 \cdot 5 + 2$; $5 = 2 \cdot 2 + \underline{\underline{1}}$. Ur det får vi:
$\underline{\underline{1}} = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 3 \cdot 5) = -2 \cdot 17 + 7 \cdot 5 = -2 \cdot 17 + 7(39 - 2 \cdot 17) = -16 \cdot 17 + 7 \cdot 39$,dvs
$17(-16) + 39 \cdot 7 = 1$ och alltså $17(-16 \cdot 2) + 39(7 \cdot 2) = 2$ Samtliga lösningar kan skrivas:

$$x = -32 - 39m; \quad y = 14 + 17m$$

Exempel 2.3.4 : Bullarna kostar 4 kr och wienerbröden 5 kr. Per köpte bullar och wienerbröd för sammanlagt 47 kr. Hur många bullar och hur många wienerbröd köpte Per?

Lösning: Om x är antalet bullar och y är antalet wienerbröd får vi den diofantiska ekvationen $4 \cdot x + 5 \cdot y = 47$.
Vi bryter ut gemensamma faktorer. Men $SGD(4, 5) = 1$ så det finns inga.
Så söker vi en lösning till ekvationen $4 \cdot x + 5 \cdot y = 1$ Den har enligt 2.6 en lösning som kan beräknas med hjälp av Euklides algoritm, men vi

finner lätt lösningen $x = -1,\ y = 1$.
En lösning till ekvationen $4 \cdot x + 5 \cdot y = 47$ är då $x_0 = -47,\ y_0 = 47$.
Den fullständiga lösningen till den ursprungliga ekvationen $4 \cdot x + 5 \cdot y = 47$ är då

$$x = -47 + 5 \cdot m,\ y = 47 - 4m$$

Både x och y måste vara ickenegativa heltal: $-47 + 5 \cdot m \geq 0 \Leftrightarrow m \geq 47/5 \Leftrightarrow m \geq 10$ och $-47 + 4m \leq 0 \Leftrightarrow m \leq 47/4 \Leftrightarrow m \leq 11$.
Vi får $10 \leq m \leq 11$ så m är antingen 10 eller 11. Då vi sätter in dessa m-värden i lösningen finner vi att Per antingen köpte
3 bullar och 7 wienerbröd eller 8 bullar och 3 wienerbröd.

2.3.4 Olika talsystem

Vanligtvis skriver vi heltal i 10-systemet. ex vis $67532 = 6 \cdot 10^4 + 7 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0$. För att omvandla 67532 i basen 10 till basen 7 använder vi divisionsalgoritmen upprepade gånger.

$$\begin{aligned} 67535 &= 9647 \cdot 7 + 6 \\ 9647 &= 1378 \cdot 7 + 1 \\ 1378 &= 196 \cdot 7 + 6 \\ 196 &= 28 \cdot 7 + 0 \\ 28 &= 4 \cdot 7 + 0 \\ 4 &= 0 \cdot 7 + 4 \end{aligned}$$

Genom successiv insättning får vi då

$$(67535)_{10} = (((((4 \cdot 7 + 0) \cdot 7 + 0) \cdot 7 + 6) \cdot 7 + 1) \cdot 7 + 1) \cdot 7 + 6$$

$$= 4 \cdot 7^6 + 0 \cdot 7^5 + 0 \cdot 7^4 + 6 \cdot 7^3 + 1 \cdot 7^2 + 6 \cdot 7^0 = (400616)_7$$

I schemat ovan kan man alltså finna svaret genom att läsa resterna nerifrån och upp! Man kan göra på ett annat sätt också: Skriv upp alla potenser av den nya basen 7 som är mindre än 67535

$$7^0 = 1,\ 7^1 = 7,\ 7^2 = 49,\ 7^3 = 343,\ 7^4 = 2401,\ 7^5 = 16807$$

och använd divisionsalgoritmen igen:

$$67535 = 4 \cdot 16807 + 307,\quad 307 = 6 \cdot 49 + 13,\quad 13 = 1 \cdot 7 + 6$$

$$67535 = 4 \cdot 7^5 + 0 \cdot 7^4 + 0 \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7^1 + 6 \cdot 7^0 = (400616)_7$$

Basen 7 som vi använt här som exempel förekommer nog sällan i tillämpningar. Vanliga baser är 10 (decimala), 2 (binära), 8 (oktala) och 16 (hexadecimala tal).

Blandade uppgifter till kapitel 2

18. XOR. Bilda det nya logiska konnektivet Δ genom ekvivalensen

$$(p\Delta q) \Leftrightarrow [(p \vee q) \wedge (\neg(p \wedge q))]$$

   a. Stämmer det att $(p\Delta q) \Leftrightarrow [(p \wedge (\neg q)) \vee (q \wedge (\neg p))]$?

   b. Kontrollera att $[(p\Delta q) \wedge r] \Leftrightarrow [(p \wedge r)\Delta(q \wedge r)]$ är en giltig logisk formel.

19. Visa att om a är ett udda tal så är $a^2 - 1$ delbart med 8.

20. Visa att $n^3 - n$ alltid är delbart med 6.

21. a. $SGD(315, 56)$

   b. $MGM(96, 144)$

   c. $SGD(12259, 3887)$

   d. $SGD(428571, 126577)$

22. a. Skriv $(4711)_{10}$ binärt, oktalt och hexadecimalt.

   b. Skriv $(ABCD)_{16}$ decimalt.

23. Vilken blir resten, då 207^{65} divideras med 13?

24. Visa att $11^{2n} + 5^{2n+1} - 6$ är delbart med 4 för alla heltal n

25. Vilka av talen 589, 661 och 899 är primtal?

26. Visa att $42^{2001} \equiv 1 \pmod{13}$

27. (Euklides algoritm gäller för polynom också!) Ekvationerna

$$x^3 - 6x^2 + 11x - 6 = 0 \text{ och } x^3 - 7x^2 + 12x - 6 = 0$$

   har en gemensam rot. Bestäm denna rot.

28. Sök gemensamma nollställen till

$$x^4 - 4x^3 - x^2 + 16x - 12 \text{ och } x^4 - 5x^3 - 3x^2 + 17x - 10$$

29. Vilken veckodag är det den 10 september 2219? Den 23 september 2002 är en måndag.

30. Visa att $4|(n+1)^3 + (n-1)^3$ för alla heltal n

31. Visa att ett positivt tal är delbart med 9 då och endast då talets siffersumma är delbar med 9.

32. Visa att det inte finns något heltal x sådant att $4|x^3 - 2$.

33. Lös de diofantiska ekvationerna

    a. $5x + 6y = 113$.

    b. $13x + 7y = 576$ där $x > 0$ och $y > 0$.

34. Vid en föreställning kostade barnbiljetterna 35 kr st och vuxenbiljetterna 45 kr st. Biljettintäkterna var exakt 10 000 kr. Hur många barnbiljetter kan högst ha sålts?

35. Bestäm de värden på n mellan 1111 och 3333 som satisfierar kongruenssystemet

$$\begin{cases} n \equiv 10 \pmod{11} \\ n \equiv 100 \pmod{101} \end{cases}$$

Kapitel 3

Induktion och rekursion

3.1 Induktionsprincipen

Vi studerar nu de *naturliga* talen, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ och det användbara *induktionsaxiomet*

Exempel 3.1.1 [De udda talens lag.]

Vi bildar summor av de udda talen från 1 och uppåt:

$$1 + 3 = 4$$
$$1 + 3 + 5 = 9$$
$$1 + 3 + 5 + 7 = 16$$
$$1 + 3 + 5 + 7 + 9 = 25 = 5^2$$

Vi kan inte låta bli att lägga märke till att summan i vart och ett av de uppräknade fallen blir lika med kvadraten på antalet termer i summan. Är det alltid så? Vi gissar att svaret är ja och resonerar som följer för att bevisa vår förmodan.

Låt p vara ett naturligt tal. Om summan av de p första naturliga talen verkligen vore $= p^2$, vad händer om vi lägger till nästa udda tal? Efter viss tankemöda inser vi att det $p + 1$:a udda talet är $2p + 1$ som vi adderar:

$$p^2 \ + \ 2p + 1$$

Enligt kvadreringsregeln är ju detta lika med $(p+1)^2$. Vi har alltså visat:

Om summan av de p första udda talen är p^2, så är summan av de $p + 1$ första udda talen $(p + 1)^2$.

Men vi vet ju att $1 + 3 = 2^2$. Därmed vet vi enligt vad vi just visat ($p = 2$) att $1 + 3 + 5 = 3^2$ och därmed att $1 + 3 + 5 + 7 = 4^2$ och föjaktligen $1+3+5+7+9 = 5^2$ och därmed ... Vi kan härleda oss fram till naturligt tal n som helst och visa att $1+3+5+7+\cdots+2n-1 = n^2$.

Att detta sätt att resonera är riktigt tycker väl de flesta. I gängse matematisk teori tillfogar vi den så kallade *induktionspricipen* som ett axiom, vi formulerar den så här

Axiom 3.1 (Induktionsprincipen.) *Låt $P(n)$ vara en öppen utsaga sådan att*

$P(n_o)$ *är sann för ett heltal* n_0 *(basfall)*

$P(n) \Rightarrow P(n+1)$ *för alla heltal* $n \geq n_0$ *(induktionssteg)*

$P(n)$ *är då sann för alla heltal* $\geq n_0$.

Anm. Induktionsprincipen kan formuleras med logiska symboler:

$$[P(0) \wedge (\forall n : P(n) \Rightarrow P(n+1))] \Rightarrow \forall n : P(n)$$

Vi går nu igenom vårt exempel igen lite mer systematiskt.

Visa att för alla hela tal $n \geq 1$ gäller

$$1 + 3 + 5 + 7 + \ldots + 2n - 1 = n^2$$

Bevis: (Induktion)

Basfall: Om $n = 1$ är uttrycken på båda sidor om likhetstecknet $= 1$, Så formeln stämmer för $n = 1$.

Induktion: Låt oss utgå från att formeln verkligen gäller för något heltal $n \geq 1$, dvs för just detta n gäller $1 + 3 + 5 + 7 + \ldots + 2n - 1 = n^2$ (induktionsantagandet)
I så fall gäller

$$1 + 3 + 5 + 7 + \ldots + 2(n+1) - 1$$

$$= \underbrace{1 + 3 + 5 + 7 + \ldots + 2n - 1}_{n^2} + 2(n+1) - 1 =$$

{använd induktionsantagandet}

$$= n^2 + 2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2$$

Dvs om formeln gäller för heltalet n så gäller den också för heltalet $n+1$.

Ur induktionsprincipen följer då att formeln gäller för $\mathbb{N} \ni n \geq 1$. □

Exempel 3.1.2 Visa att $2^n \geq n^2$ för $n \geq 4$.

Bevis:

Basfall: För $n = 4$ betyder det att $2^4 \geq 4^2$ och det är ju sant ty $16 \geq 16$!

Induktion: Nu gör vi antagandet (induktionsantagandet) att $2^n \geq n^2$ är sant för något $n \geq 2$.
Vänsterledet i motsvarande formel för $n + 1$ är då

$$2^{n+1} = 2 \cdot 2^n = 2^n + 2^n \geq \{\text{Nu använder vi induktionsantagandet}\}$$

$$\geq n^2 + n^2 = n^2 + n \cdot n \geq n^2 + 4n \geq n^2 + 2n + 8 > n^2 + 2n + 1 = (n+1)^2$$

Vi har då visat att om $2^n \geq n^2$ och $n \geq 4$, så följer $2^{n+1} \geq (n+1)^2$, dvs det vi skulle bevisa gäller även för heltalet $n + 1$

Enligt induktionspricipen gäller formeln för alla $n \geq 4$. □

Exempel 3.1.3 Visa att $\boldsymbol{D}x^n = n \cdot x^{n-1}$ för $n \in \mathbb{N}$.
Bevis:

Basfall: $VL_0 = \boldsymbol{D}\, x^0 = \boldsymbol{D}\, 1 = 0 = 0 \cdot x^{0-1} = 0 = HL_0$!

Induktion: Antag att $\boldsymbol{D}\, x^p = p \cdot x^{p-1}$ för något heltal $p \geq 0$. Då deriverar vi x^{p+1} genom att använda formeln för derivatan av en produkt:

$$\boldsymbol{D}\, x^{p+1} = \boldsymbol{D}\, x \cdot x^p = 1 \cdot x^p + x\boldsymbol{D}\, x^p$$

$$= x^p + x \cdot p \cdot x^{p-1} = x^p + p \cdot x^p = (p+1)x^p$$

som är rätt uttryck för n=p+1.

Enligt induktionsaxiomet gäller då $\boldsymbol{D}x^n = n \cdot x^{n-1}$ för alla naturliga tal. □

3.1.1 Övningar på induktionsbevis

36. Visa att

$$2 \cdot 6 + 3 \cdot 7 + \ldots + (n+1)(n+5) = \frac{n(2n+7)(n+7)}{6} \text{ , för } n \geq 1$$

Bevisa med induktion eller på annat sätt (övn 37–44)

37. $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ för alla heltal $n \geq 1$.

38. $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$ för alla heltal $n \geq 1$.

39. $\sum_{k=0}^{n} k\, 2^{-k} = 2 - (n+2)2^{-n}$ för alla heltal $n \geq 1$.

40. $\sum_{k=n}^{2n} k = \frac{3n(n+1)}{2}$ för alla heltal $n \geq 1$.

41. $7^n + 3^{n+1}$ är delbart med 4 för alla heltal $n \geq 1$.

42. $8^n - 7n - 1$ är delbart med 49 för alla heltal $n \geq 1$.

43. $2^n \geq n^3$ för alla heltal $n \geq 10$.

44. $e^x > \frac{x^n}{n!}$för $x > 0$ och alla heltal $n \geq 1$.
($n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$)

3.2 Rekursiva följder och procedurer

Exempel 3.2.1 Fibonaccitalen. År 1201 publicerade Fibonacci (Lionardo di Pisa 1180–1250) en lärobok i matematik, Liber Abbacci, där följande problem rörande kaninavel formulerades.

Vi gör föjande antaganden:

Kaniner har evigt liv.

Kaniner får sina första ungar vid (exakt) två månaders ålder.

Varje månad ger varje vuxet kaninpar upphov till ett nytt kaninpar.

Vi införskaffar ett kaninpar månad 0 som månad 2 får två ungar som utgör utterligare ett kaninpar. Vi följer uvecklingen månad för månad.

månad	antal kaninpar
0	1
1	1
2	2
3	3
4	5
5	8
6	13

Man inser att antalet kaninpar en viss månad är lika med antalet par en månad tidigare plus antalet par två månader tidigare det vill säga

$$x_n = x_{n-1} + x_{n-2} \text{ för } n \geq 2$$

där y_n är antalet kaninpar månad n.

Övning.

45. Diskutera varför fibonaccis följd är väldefinierad genom utsagan: $x_0 = 1$ och $x_1 = 1$ och $x_n = x_{n-1} + x_{n-2}$ för $n \geq 2$

Fibonaccis följd säges vara definierad *rekursivt*, det vill säga värdet av en ny term beror på ett entydigt sätt av de föregående.

Exempel 3.2.2 ***n***! Vi gör en rekursiv definition av $n!$:

$$0! = 1$$
$$(n+1)! = n! \cdot (n+1) \text{ för } n \geq 1$$

Till exempel är $5! = 5 \cdot 4! = 5 \cdot 4 \cdot 3! = 5 \cdot 4 \cdot 3 \cdot 2! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = \underline{\underline{120}}$

$$\begin{aligned} 5! &= 5 \cdot 4! \\ 4! &= 4 \cdot 3! \\ 3! &= 3 \cdot 2! \\ 2! &= 2 \cdot 1! \\ 1! &= 1 \cdot 0! \\ 0! &= 1 \\ 1! &= 1 \cdot 1 = 1 \\ 2! &= 2 \cdot 1 = 2 \\ 3! &= 3 \cdot 2 = 6 \\ 4! &= 4 \cdot 6 = 24 \\ 5! &= 5 \cdot 24 = \underline{\underline{120}} \end{aligned}$$

Rekursiva procedurer kan användas vid programmering. Här är en pascal-rutin för att beräkna n!

```
function fak(n : integer) : integer;
  begin;
    if n = 0 then fak := 1
      else fak:= n*fak(n - 1)
  end
```

3.2.1 Rekursiva definitioner

Exempel 3.2.3 Textsträngar Låt en mängd av tecken vara given. Datatypen *sträng* kan då definieras så här

(i) Den tomma strängen, "", är en sträng.

(ii) Om t är ett tecken och $\boldsymbol{s}$ är en sträng så är $\boldsymbol{st}$ en sträng.

Exempelvis är "abc" en sträng.
Bevis: "abc" är enstäng $\Leftarrow$ "ab" är en sträng $\wedge$ "c" är ett tecken $\Leftarrow$"a" är en sträng $\wedge$"b" är ett tecken $\Leftarrow$"" är en sträng $\wedge$ "a" är ett tecken □

3.3 Linjära rekurrensekvationer

Att lösa en *rekurrensekvation* innebär att man ur en given rekursionformel härleder ett "slutet uttryck" för den n:te termen.

3.3.1 Homogena linjära rekurrensekvationer av första och andra ordningen med konstanta koefficienter

Nu behandlar vi ekvationer av typerna

$x_{n+1} + a\,x_n = 0$, av första ordningen

$x_{n+2} + p\,x_{n+1} + q\,x_n = 0$, andra ordningen.

Vi löser först $x_{n+1} + a\,x_n$

$$x_n = (-a)x_{n-1} = (-a)^2 x_{n-2} = (-a)^3 x_{n-3} = \cdots = (-a)^n x_0$$

Lösningenär alltså

$$x_n = C \cdot (-a)^n$$

där C är en konstant.

För att lösa en andra ordningens ekvation ansätter vi en liknande lösning $x_n = C \cdot \lambda^n$ och får

$$x_{n+2}+p\,x_{n+1}+q\,x_n = C\cdot\lambda^{n+2}+p\cdot C\cdot\lambda^{n+1}+C\cdot q\cdot\lambda^n = C\cdot\lambda^n(\lambda^2+p\cdot\lambda+q) = 0$$

Vi kan då dra slutsatsen att λ är en lösning till den *karakteristiska ekvationen*

$$\lambda^2 + p \cdot \lambda + q = 0$$

I själva verket ger detta all lösningar, enligt följande sats som vi meddelar utan bevis.

Sats 3.1 *Låt λ_1 och λ_2 vara lösningarna till karakteristiska ekvaationen $\lambda^2 + p \cdot \lambda + q = 0$. Då kan samtliga lösningar till rekurrensekvationen $x_{n+2} + p\, x_{n+1} + q\, x_n = 0$ skrivas*

$C_1 \cdot \lambda_1^n + C_2 \cdot \lambda_2^n$ *om* $\lambda_1 \neq \lambda_2$

$(A \cdot n + B)\lambda^n$ *om* $\lambda_1 = \lambda_2 = \lambda$

där $A,\ B,\ C_1$ och C_2 är konstanter.

Exempel 3.3.1

a. Ekvationen $x_{n+2} - 4x_{n+1} - 5x_n = 0$ har karakteristiska ekvationen $\lambda^2 - 4\lambda - 5 = 0$ med rötterna $\lambda_1 = -1$ och $\lambda_2 = 5$. Alla lösningar kan då skrivas $\underline{\underline{x_n = C_1(-1)^n + C_2 \cdot 5^n}}$, där C_1 och C_2 är godtyckliga reella tal.

b. $x_{n+2} - 4x_{n+1} + 4x_n = 0$ har karakteristiska ekvationen $\lambda^2 + 4\lambda + 4 = 0$ med dubbelroten $\lambda = 2$. Lösningarna är $\underline{\underline{x_n = (An + B) \cdot 2^n}}$, där A och B är fria konstanter.

Exempel 3.3.2 Ge den lösning till $x_{n+2} - 2x_{n+1} + 3x_n = 0$, för vilken $x_0 = 0$ och $x_1 = 3$.

Lösning. Karakteristiska ekvationen är $\lambda^2 - 2\lambda + 3 = 0$ med rötterna 1 och 2. Lösningen är $x_n = C \cdot 1^n + D \cdot 2^n = C + D \cdot 2^n$, där vi skall bestämma C och D.Insättning av startvärdena ger

$$\begin{cases} C + D = 0 \\ C + 2 \cdot D = 3 \end{cases}$$

som ger $C = -3, D = 3$, dvs $\underline{\underline{x_n = 3 \cdot 2^n - 3}}$.

Vi ger ett exempel där karakteristiska ekvationen har komplexa rötter.

Exempel 3.3.3 Lös $x_{n+2} - x_{n+1} + x_n = 0,\ x_0 = 0,\ x_1 = 1$.

Lösning. Karakteristiska ekvationen är $\lambda^2 - \lambda + 1 = 0$, om har de konjugerat komplexa rötterna $\dfrac{1 \pm i \cdot \sqrt{3}}{2}$, på polär form $\cos \pi/3 \pm i \cdot \sin \pi/3$. Vi får på samma sätt som tidigare

$$x_n = A \cdot \left(\frac{1 + i \cdot \sqrt{3}}{2} \right)^n + B \cdot \left(\frac{1 - i \cdot \sqrt{3}}{2} \right)^n$$

Insättning av startvärdena ger

$$\begin{cases} x_0 = A + B = 0 \text{ dvs } B = -A \\ x_1 = A \cdot \left(\frac{1+i\cdot\sqrt{3}}{2} - \frac{1-i\cdot\sqrt{3}}{2} \right) = A \cdot i \cdot \sqrt{3} = 1 \\ A = \frac{1}{i\cdot\sqrt{3}},\ B = -\frac{1}{i\cdot\sqrt{3}} \end{cases}$$

Vi sätter in dessa värden på A och B och använder de Moivres formel.

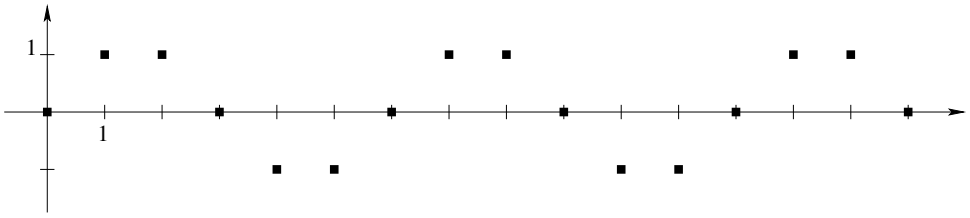
$$x_n = \frac{1}{i\sqrt{3}}\big((\cos\pi/3 + i\cdot\sin\pi/3)^n - (\cos\pi/3 - i\cdot\sin\pi/3)^n\big)$$

$$= \frac{1}{i\sqrt{3}}(\cos n\pi/3 + i\cdot\sin n\pi/3 - \cos n\pi/3 + i\cdot\sin n\pi/3)$$

$$= \frac{1}{i\sqrt{3}}(2i\sin n\pi/3) = \frac{2\sin n\pi/3}{\sqrt{3}}$$

Eftersom $\sin(n\pi/3) = 0,\ \sqrt{3}/2,\ \sqrt{3}/2, 0,\ -\sqrt{3}/2,\ -\sqrt{3}/2, 0,\ \sqrt{3}/2, \ldots$ för $n = 0, 1, 2, 3, 4, 5, \ldots$, ges x_n av följden

$$0, 1, 1, 1, -1, -1, 0, 1, 1, 0, 1 \ldots \text{ för } n = 0, 1, 2, 3, \ldots$$



3.3.2 . . . och inhomogena

En inhomogen rekurrensekvation ser ut så här

$$x_{n+2} + p\,x_{n+1} + q\,x_n = g_n$$

där g_n är något uttryck i n.
För att lösa sådana gör man på följande sätt

(i) Bestäm den allmänna lösningen x_{hn} till den *homogena* ekvationen $x_{n+2} + p\,x_{n+1} + q\,x_n = 0$.

(ii) Bestäm *en* lösning, *partikulärlösning* ,x_{pn} till den inhomogena ekvationen.

Addera sedan sedan dessa lösningar. $x_n = x_{hn} + x_{pn}$ ger samtliga lösningar till $x_{n+2} + p\,x_{n+1} + q\,x_n = g_n$.

Hur man hittar partikulärlösningarna är ett kapitel för sig, men grundregeln är att de är av samma typ som högerledet, eventuellt multiplicerad med ett polynom i n. Man får pröva sig fram.

Exempel 3.3.4 Lös r-ekvationen $x_{n+2} - 4x_{n+1} - 5x_n = n$.

Lösning. Homogena ekv har lösningarna (se exempel 3.3.1)

$$x_{hn} = C_1(-1)^n + C_2 \cdot 5^n$$

För att få en partikulärlösning ansätter vi $x_n = x_{pn} = an + b$, får

$$x_{n+2} - 4x_{n+1} - 5x_n = a(n+2) + b - 4a(n+1) - 4b - 5an - 5b = -8an - 2a - 8b = n$$

för alla n. Identifiering ger $a = -1/8, b = -a/4 = 1/32$, så $x_{pn} = -n/8 + 1/32$.
De fullständiga lösningen är

$$x_n = x_{hn} + x_{pn} = \underline{\underline{C_1(-1)^n + C_2 \cdot 5^n - n/8 + 1/32}}$$

Exempel 3.3.5 Lös $x_{n+2} - 4x_{n+1} - 5x_n = 5^n$.

*Lösning.*Då vi söker en partikulärlösning noterar vi att högerledet 5^n är en lösning till den homogena ekvationen, varför ansättningen $x_{pn} = C \cdot 5^n$ inte duger (som den annars skulle ha gjort). Vi trappar upp ansättningen till $x_{pn} = C \cdot n \cdot 5^n$ och får

$$x_{n+2} - 4x_{n+1} - 5x_n = C(n+2)5^{n+2} - 4C(n+1)5^{n+1} - 5C \cdot n \cdot 5^n$$

$$= C5^n(25n - 20n - 5n + 50 - 20) = C \cdot 30 \cdot 5^n = 5^n$$

Då blir $C = 1/30$, $x_{pn} = n/30 \cdot 5^n$ och ekvationens lösning är

$$x_n = x_{hn} + x_{pn} = \underline{\underline{C_1(-1)^n + (C_2 + \frac{n}{30}) \cdot 5^n}}$$

Några övningar på rekursion.

46. Följden a_n är bestämd genom villkoren $a_1 = \sqrt{2}$, $a_{n+1} = \sqrt{2 + a_n}$ för $n = 1, 2, 3, \ldots$.
    Visa att a) $a_n < 2$, b)$a_{n+1} > a_n$ för alla $n \geq 1$.

47. Gör en rekursiv definition av

    a. a^n, där a är ett tal$\neq 0$ och n är ett naturligt tal.

    b. $\sum_{k=0}^{n} a_k$, där $n \in \mathbb{N}$.

48. Låt $f_0, f_1, f_2, \ldots$ vara fibonaccitalen. Visa att

$$f_0^2 + f_1^2 + \cdots + f_n^2 = f_{n+1}f_n$$

    för alla naturliga tal n

49. Lös differensekvationerna med startvillkor

    a. $2x_{n+1} = 3x_n,\ x_0 = 3$

    b. $x_{n+2} = 5x_{n+1} - 6x_n,\ x_0 = x_1 = 1$

    c. $x_{n+2} - 5x_{n+1} + 6x_n = 2,\ x_0 = 0,\ x_1 = 1$

    d. $x_{n+2} - 3x_{n+1} + 2x_n = 2^{n+1},\ x_0 = x_1 = 1$

50. †Ge en sluten formel för fibonaccitalen.

Kapitel 4

Kombinatorik

Vi fortsätter nu med mängdläran och konsten att beräkna antalet element i olika mängder.

4.1 Dirichlets lådprincip

Sats 4.1 (Dirichlets lådprincip) *Om $n+1$ objekt placeras i n fack kommer minst ett fack att innehålla minst två objekt.*

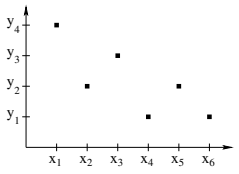
Beviset lämnas som övning.

Exempel 4.1.1 I en grupp med 8 personer måste det finnas minst två som är födda samma veckodag.

Exempel 4.1.2 Välj 101 tal bland talen $1, 2, \ldots 200$. Visa att det bland de valda talen finns två tal a och b sådana att $a|b$.

Lösning: Varje heltal kan skrivas $2^k \cdot y$, där y är ett udda tal. Det finns bara 100 udda tal mellan 1 och 200, så det finns (minst) två av de 101 valda talen som har samma y. Det mindre av dessa två delar då det större.

Exempel 4.1.3 Låt f vara en funktion sådan att D_f har $n+1$ element och V_f har högst n element. Då finns ett funktionsvärde som antas för två olika element i definitionsmängden, dvs funktionen kan inte vara inverterbar.



Övningar

51. På parkeringsplatsen står 1 001 bilar. Visa att sifferdelen i bilnumret är lika hos minst två av bilarna.
52. En stad i Sverige har 149 300 invånare. Vi delar in människorna i staden i grupper där alla har de fyra sista siffrorna i personnumret lika. Hur stor måste den största av dessa grupper minst vara?

4.2 Antalet element i ändliga mängder

Låt M vara en mängd. Om M har n element, skriver vi $|M| = n$.

Exempel 4.2.1

$$|\{a, c\}| = 2$$
$$|\{1, 3, 2, 1\}| = 3$$
$$|\emptyset| = 0$$
$$|\{m; m \in \mathbb{N} \ \wedge \ (m < 100)\}| = 100$$

Övning.

53. a. Visa att $|A \cup B| = |A| + |B| - |A \cap B|$.

    b. Ge en liknande formel för $A \cup B \cup C$.

4.2.1 n-tiplar

En *n-tipel* består av n objekt, som inte behöver vara olika, och där varje objekt har ett eget ordningsnummer mellan 1 och n. Vi skriver en n-tipel så här $(x_1, x_2, x_3, \ldots, x_n)$

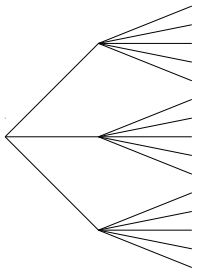
En 2-tipel är ett *ordnat par*, (x, y).

Ett annat namn för n-tipel ät *lista.*

Exempel 4.2.2

$$\text{(Gunnar, Helge, Ellinor)} \neq \text{(Helge, Ellinor, Gunnar)}$$

$$(1, 2, 3) \neq \{(1, 2, 3)\} \neq \{1, 2, 3\}$$



4.2.2 Multiplikationspricipen

Exempel 4.2.3 Antag att man skall göra två val och att i det första valet finns 3 olika alternativ och vid det andra valet finns 5 olika alternativ. Antal möjligheter att göra de två valen sammantaget är då $3 \cdot 5 = 15$ (Se figur.). I detta fall $3 \cdot 5 = 15$ valmöjligheter.

Resonemanget i exemplet ovan generaliseras till *multiplikationsprincipen*, som säger att vid n st val där varje val har n_k olika alternativ $k = 1, 2, ..., n$, så är antalet olika sätt som de n st valen sammantaget kan göras på ($\prod$ är tecknet för produkt)

$$n_1 \cdot n_2 \cdot \ldots \cdot n_n = \prod_{k=1}^{n} n_k$$

Exempel 4.2.4 Antalet möjliga sätt att tippa en stryktipsrad med 13 matcher är $3^{13} = 1\,594\,323$

Exempel 4.2.5 Antalet sätt att tippa alla 13 matcherna fel är $2^{13} = 8192$

Exempel 4.2.6 I en förening med 17 medlemmar skall väljas en ordförande, en sekreterare och en kassör. På hur många sätt kan detta teoretiskt gå till?

Lösning: Ordföranden kan väljas på 17 sätt. För varje val av ordförande kan sekreteraren väljas bland de återstående 16 föreningsmedlemmarna. För var och en av dessa $16 \cdot 17$ möjligheter finns sedan 15 medlemmar att välja kassören bland. Valet att välja denna grupp om tre kan ske på $17 \cdot 16 \cdot 15$ olika sätt.

Exempel 4.2.7 Hur många n-tipler med idel olika element kan man bilda ur en mängd med n element? Dvs på många sätt kan vi ordna n olika objekt i följd?
– Vi resonerar som förut, första komponenten kan väljas på n sätt, andra på $n-1$ sätt, och så vidare. Den n:te och sista kan bara väljas på ett sätt Enligt multiplikationsprincipen kan vi bilda

$$n \cdot (n-1) \cdots 2 \cdot 1 = n!$$

ordningsföljder.

Övning.

54. Om vi har siffrorna 1,2,4,5 och 7, hur många tresiffriga tal kan man bilda a) Om varje siffra kan återanvändas, b) om varje siffra bara får användas en gång, c) om talet skall vara udda med olika siffror?

4.2.3 Permutationer

Ett urval av k st olika element i en viss ordning ur en mämgd med n element kallas en *permutation av k element ur n givna.* Som i exempel 4.2.6 kan man visa att antalet permutationer av k element bland n givna är

$$P(n,k) = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

Ett specialfall är $k = n$, då alltså hela mängden skall ordnas eller ordnas om. Man talar då bara om en *permutation* av de n elementen. Antalet permutationer av n element är

$$P(n,n) = n(n-1)\ldots 3 \cdot 2 \cdot 1 = n!$$

Exempel 4.2.8 Mängden $\{a, b, c\}$ kan permuteras på $3! = 6$ sätt, nämligen

$$abc$$
$$acb$$
$$bac$$
$$bca$$
$$cab$$
$$cba$$

Exempel 4.2.9 Hur många textsträngar med alla tecken olika kan man bilda av tecknen ABCDE?

Lösning:

Antal tecken	antal strängar	
0	$5!/(5-0)! =$	1
1	$5!/(5-1)! =$	5
2	$5!/3! = 5 \cdot 4 =$	20
3	$5!/2! = 5 \cdot 4 \cdot 3 =$	60
4	$5!/1! = 5 \cdot 4 \cdot 3 \cdot 2 =$	120
5	$5!/0! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 =$	120
	Summa	326

4.2.4 Kombinationer och binomialkoefficienter

Om M med ett ändligt antal, n, element och k ett naturligt tal som är $\leq n$, hur många olika delmängder till M med k element kan man bilda? Eller, uttryckt på ett annat sätt, hur många *kombinationer* av k element av n finns det?

Frågeställningen är annorlunda jämfört med föregående delavsnitt om permutationer. I en delmängd (kmbination) fäster vi ju inget avseende vid ordningsföljden, $\{a, b, c\}$ är ju samma mängd som $\{c, a, b\}$.

Vi resonerar som följer. Först beräknar vi antalet permutationer av k element ur de givna n. Det blir $n(n-1)\cdots(n-k+1) = \dfrac{n!}{(n-k)!}$ stycken. Men vissa av dessa är ju bara omordningar av varandra och representerar samma delmängd. Varje delmängd representeras då av $k!$ olika omordningar. Vi måste då dividera med $k!$ och får svaret

$$\text{Antalet sätt att välja } k \text{ element bland } n = \frac{n!}{k!(n-k)!}$$

Definition 4.1 $\binom{n}{k}$ *är antalet delmängder med* k *element ur en mängd med* n *element.*

Enligt ovan gäller

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{4.1}$$

Talet $\binom{n}{k}$ kallas också *binomialkoefficient*

Exempel 4.2.10 En förening med 17 medlemmar (samma som i exempel 4.2.6) skall välja en styrelse om tre personer, som själva fördelar arbetsuppgifterna mellan sig. På hur många sätt kan detta ske?

Lösning: Nu är ordningsföljden likgiltig. Styrelsen kan väljas på

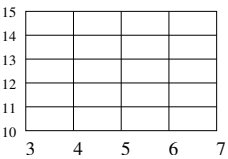
$$\binom{17}{3} = \frac{17!}{3!\,14!} = \frac{17\cdot 16\cdot 15\cdot \cancel{14}\cdot \cancel{13}\cdots \cancel{2}\cdot 1}{\cancel{14}\cdot \cancel{13}\cdots \cancel{2}\cdot 1\cdot 3\cdot 2\cdot 1} = \frac{17\cdot 16\cdot 15}{3\cdot 2} = 680$$

olika sätt.

Exempel 4.2.11 Hur många olika pokerhänder finns det?

Lösning: En pokerhand består av 5 kort valda bland 52 kort. Det finns alltså $\binom{52}{5} = 52\cdot 51\cdot 50\cdot 49\cdot 48/(5\cdot 4\cdot 3\cdot 2) = 2\,598\,960$ pokerhänder.

Exempel 4.2.12 Åke skall gå från hörnet Third ave/E 39 st till hörnet Fifth ave/E 34 st. På hur måga sätt kan han gå utan att gå omvägar?



Lösning: Åke måste gå sammanlagt 9 delsträckor (mellan två korsningar). 5 av dem måste gå söderut, de kan väljas på $\binom{9}{4} = \frac{9\cdot 8\cdot 7\cdot 6}{4\cdot 3\cdot 2\cdot 1} =$ 126 olika sätt, dvs det finns = 126 olika vägar.

4.3 Binomialteoremet

4.3.1 Egenskaper hos binomialkoefficienter

Vi ger några grundläggande samband för binomialkoefficienterna $\binom{n}{k}$

$$\binom{n}{0} = \binom{n}{n} = 1 \tag{4.2}$$

$$\binom{n}{k} = \binom{n}{n-k} \tag{4.3}$$

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{4.4}$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \tag{4.5}$$

Bevis. Dessa samband kan bevisas med hjälp av den numeriska formeln 4.1, men vi väljer att visa dem med hjälp av definition 4.1 ovan genom så kallade *kombinatoriska resonemang.*

Ekv 4.2: Antalet delmängder med 0 element är 1. Bara den tomma mängden $\emptyset$ har 0 element. Det finns också en och endast en delmängd med n element, grundmängden M själv.

Ekv 4.3: Till varje delmängd A med k element finns en annan med $n-k$ element, nämligen de element i M som inte tillhör A, så antalet delmängder med $n-k$ element måste vara lika många som de med k element.

Ekv 4.4: Om vi skall välja ut k element ur en grundmängd med $n+1$ element kan vi gå tillväga så att vi fixerar ett viss element x i grundmängden. Delmängderna med k valda element är av två slag:

(a) dels de som innehåller x , de övriga $k-1$ skall väljas bland de övriga n, det kan ske på $\binom{n}{k-1}$ sätt

(b) dels de som inte innehåller x då skall vi välja alla k bland de övriga n på $\binom{n}{k}$ sätt.

Detta ger formel 4.4.

Ekv 4.5: Vänstra ledet ger totala antalet delmängder. Att högra ledet också gör det inses genom att man för varje element i M har 2 möjligheter, antingen tas elementet med i urvalet eller också inte. Enligt multiplikationspricipen har vi 2^n valmöjligheter för de n elementen i grundmängden. □

Pascals triangel

Sambanden 4.2 och 4.4 ger tillsammans en rekursionsformel för binomialkoefficienterna. Vi arrangerar dem i ett triangulärt schema enligt

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ & & & \dots & & & \end{array}$$

och då vi tillämpar rekursionsformeln får vi Pascals triangel:

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\ & & & & & \dots & & & & & \end{array}$$

Exempel 4.3.1 På hur många sätt kan man få exakt 11 rätt av 13 på stryktips?

Lösning: De feltippade matcherna kan väljas på $\binom{13}{2}$ sätt. Var och en av dem kan vara fel på två sätt. Vi får svaret $\binom{13}{2} \cdot 2 \cdot 2 = 13 \cdot 12/2 \cdot 2 = 312$ sätt.

4.3.2 Binomialteoremet

Vi känner till kvadreringsregeln:

$$(x+y)^2 = x^2 + 2xy + y^2$$

och kanske också regeln för $(x+y)^3$:

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

Nu ger vi en allmän formel för $(x+y)^n$ där n är ett godtyckligt heltal ≥ 0. Vi skriver

$$(x+y)^n = (x+y)(x+y)\cdots(x+y) \qquad (n \text{ faktorer})$$

Då vi multiplicerar ihop dessa termer måste vi välja ett x eller ett y ur varje faktor. Vi får en summa av 2^n produkter $x^j y^k$ där $j+k=n$, alltså en summa av termer $x^{n-k}y^k$ där $0 \leq k \leq n$. En sådan term uppstår genom att vi väljer y ur k av parenteserna och x ur de övriga. Det kan för varje k ske på $\binom{n}{k}$ sätt så antalet termer av typen $x^{n-k}y^k$ är $\binom{n}{k}$ Detta ger det viktiga binomialteoremet:

Sats 4.2 (Binomialteoremet) *Om n är ett naturligt tal så gäller*

$$\begin{aligned}(x+y)^n &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k \\ &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n\end{aligned}$$

Vi ger några exempel:

Exempel 4.3.2

$$\begin{aligned}(a+b)^4 &= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4 \\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\ (x-1)^7 &= x^7 - 7x^6 + 21x^5 - 35x^4 + 35x^3 - 21x^2 + 7x + 1 \\ (x^2+2y)^5 &= x^{10} + 10x^8y + 40x^6y^2 + 80x^4y^3 + 80x^2y^4 + 32y^5\end{aligned}$$

Exempel 4.3.3 Bestäm koefficienten för x^{22} i $(2+x^2)^{16}$.

Lösning: Termen som innehåller $x^{22} = (x^2)^{11}$ är den med index $k = 11$, dvs

$$\binom{16}{11}2^{16-11}x^{22} = \binom{16}{5}2^5x^{22}$$

så svaret är

$$\binom{16}{5}2^5 = \frac{16\cdot 15\cdot 14\cdot 13\cdot 12}{5\cdot 4\cdot 3\cdot 2}32 = 4368\cdot 32 = 139776$$

Övningar på kombinatorik

55. Beräkna $\binom{10}{3}$, $\binom{12}{8}$ och $\binom{100}{98}$

56. Utveckla

    a. $(s-r)^3$

    b. $(x^2+2)^5$

57. Hur många $n-$siffriga tal ($n \geq 2$) kan bildas med siffrorna 1 och 2 om talen skall innehålla minst en etta och minst en tvåa?

58. Tre personer får välja två skivor var ur en samling på 10 olika skivor. På hur många sätt kan det gå till?

59. På hur många sätt kan 6 personer bilda

    a. en kö?

    b. en ring?

60. På hur många sätt kan $2n$ fotbollslag mötas i en spelomgång?

61. På hur många sätt kan man få en "full hand" i poker, dvs exakt tre kort i en valör (av tretton) och ett par av en annan valör?

62. I en grupp på 12 personer skall väljas en kommitté på 5 personer. A och B ställer som villkor att om den ena skall vara med i kommittén så skall den andra också vara med. Hur många olika kommittéer är möjliga?

63. Finns det någon konstant term i utvecklingen av $\left(\frac{x^2}{2} + \frac{32}{x^8}\right)^{20}$? Bestäm den i så fall.

64. Visa formel 4.5 genom att utveckla $(1+1)^n$.

65. Visa att $\binom{n}{k}\binom{n-k}{j} = \binom{n}{j}\binom{n-j}{k}$, om $j + k \leq n$.

66. Bevisa att $\binom{2n}{2} = 2\binom{n}{2} + n^2$.

67. Visa att $\sum_{k=0}^{n} \binom{n}{k} 2^k = 3^n$.

4.4 Oändliga mängder

4.4.1 Uppräkneliga mängder

Definition 4.2 *Mängden M är* uppräknelig *om varje element $x \in M$ kan ges ett eget naturligt tal.*

Exempel 4.4.1 De naturliga talen $\mathbb{N}$ är självklart uppräknelig.

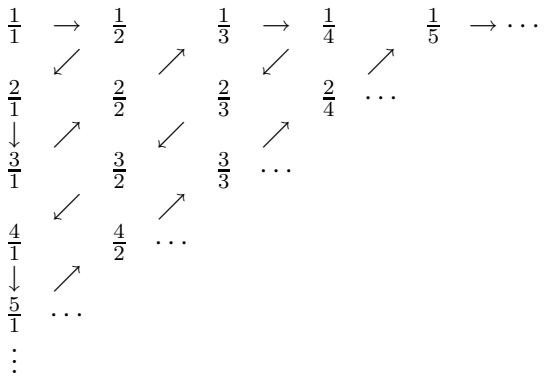
Exempel 4.4.2 $\mathbb{Z}$, mängden av hela tal är uppräknelig. En uppräkning är

$$0 \to -1 \to 1 \to -2 \to 2 \to -3 \to 3 \to -4 \to 4 \to \cdots$$

Exempel 4.4.3 De jämna talen är uppräkneliga eftersom man kan låta det n:te jämna talat vara $2n$

I själva verket är varje delmängd av en uppräknelig delmängd uppräknelig. Men det finns andra.

Exempel 4.4.4 Mängden av rationella tal är uppräknelig. Det kan vi visa genom att skriva upp de positiva rationella talen i ett schema och räkna upp dem som pilarna visar:



Här är ju samma tal med flera gånger, men det gör ju inte saken sämre.

Övningar.

68. Visa att mängden av möjliga datorprogram är uppräknelig.

69. Är {Möjliga läroböcker} uppräknelig?

4.4.2 Icke uppräkneliga mängder

Ordet "diskret" i sammanställningen "diskret matematik" betyder ändlig eller uppräknelig. Alla oändliga mängder är inte uppräkneliga, det finns olika grader av oändlighet.

Vi inför nu bereppet *kardinaltal*. För en ändlig mängd M är kardinaltalet $= |M|$, antalet element i mängden.
$|\mathbb{N}| = \aleph_0$ är kardinaltalet för de naturliga talen och därmed för varje uppräknelig mängd.[1] $|\mathbb{R}| = \aleph_1$ är kardinaltalet för de reella talen. Det visar sig att $\aleph_1 > \aleph_0$!

Sats 4.3 *De reella talen kan inte räknas upp.*

Innan vi bevisar detta (med Cantors diagonalbevis) noterar vi att varje reellt tal mellan 0 och 1 kan skrivas som ett oändligt decimalbråk. Framställningen är entydig om inte talet får avslutas med idel 9:or. Exempelvis

$$\begin{aligned} 1/7 &= 0.142857142857142857142857142857142857142857142857142857\cdots \\ \sqrt{2}/2 &= 0.707106781186547524400844362104849039284835937688474\cdots \\ \pi/4 &= 0.785398163397448309615660845819875721049292349843776\cdots \\ 1/e &= 0.367879441171442321595523770161460867445811131031767\cdots \end{aligned}$$

[1] $\aleph$, "alef" är första boxtaven i det hebreiska alfabetet.

Här följer Cantors diagonalbevis[2].

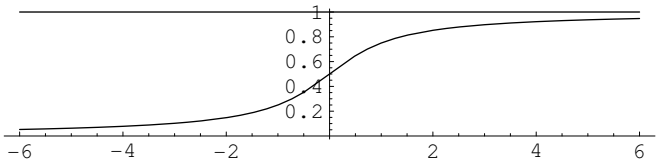
Bevis: Varje reellt tal mellan 0 och 1 kan entydigt representeras som ett oändligt decimaltal om vi kräver att inget sådant avslutas med idel nior. Antag nu att det finns en uppräkning av de reella talen mellan 0 och 1 med hjälp av de positiva heltalen. Vi får då en lista av decimalutvecklingar

$$\begin{aligned} A_1 &= 0, a_{11}a_{12}a_{13}a_{14}\ldots \\ A_2 &= 0, a_{21}a_{22}a_{23}a_{24}\ldots \\ A_3 &= 0, a_{31}a_{32}a_{33}a_{34}\ldots \\ A_4 &= 0, a_{41}a_{42}a_{43}a_{44}\ldots \\ &\ldots \end{aligned}$$

där alla talen är olika och där varje reellt tal mellan 0 och 1 finns med. Vi ska nu visa att det finns åtminstone ett reellt tal $A = 0, a_1a_2a_3a_4\ldots$ mellan 0 och 1 som inte är med i listan. Sätt nämligen $a_i = 1$ om $a_{ii} = 0$ och $ai_{=}0$ annars. Då är $A \neq A_i$ för alla i eftersom den i:e decimalen i utvecklingarna av A och A_i är olika. Därmed är beviset klart. □

Genom att avbilda $\mathbb{R}$ på $\{x; 0 < x < 1\}$ genom den omvändbara funktionen

$$y = 1/2 + \frac{1}{\pi}\arctan x$$



ser vi att $\mathbb{R}$ innehåller lika många tal som intervallet $(0, 1)$, dvs

$$|\mathbb{R}| = \aleph_1 \ .$$

En fråga som man kan ställa sig är om det finns någon mängd som är mäktigare än heltalen men mindre mäktig än de reella talen. Denna fråga kallas kontinuumproblemet. Cantors förmodande i början på nittonhundratalet, kontinuumhypotesen, var att så inte var fallet. Gödel visade på trettiotalet att denna hypotes inte kunde motbevisas och 1963 visade Paul Cohen att den inte kunde bevisas heller.

[2]se http://www.maths.lth.se/query/answers/q97-3.html

Svar till övningsuppgifterna

1. Om jag inte tar bussen regnar det inte.

2. a. $\neg p$

   b. $l \wedge v$

   c. $a \Rightarrow b$

   d. $\neg(sv \Rightarrow so)$

3. Den som syndar sover inte.

4. a. S

   b. S

   c. F

   d. S

   e. S

   f. S

5. a.

p	q	$(p \vee \neg q) \Rightarrow q$
S	S	S
S	F	F
F	S	S
F	F	F

   b.

p	q	$(p \Rightarrow q) \vee (q \Rightarrow p)$
S	S	S
S	F	S
F	S	S
F	F	S

6. $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$
   Antag F
   S F
   S S S Ⓕ
   S
   Ⓢ

7. $(\neg q \Rightarrow \neg p) \Leftrightarrow (p \Rightarrow q)$
   F S F S S S F
   S F F S S F F
   F S S S F S S
   S S S S F S F

8. $[(p \Rightarrow q) \wedge (\neg p \Rightarrow q)] \Rightarrow q$ är en tautologi.

9. a. $(b \wedge s) \Rightarrow (\neg m)$

   b. $(f \vee n) \Leftrightarrow t$

   c. $(\neg l) \wedge (\neg d)$

   d. $(x^2 + x = 6) \Leftrightarrow [(x = 2) \vee (x = -3)]$

10. a. Tautologi

    b. Inte en tautologi.

11. $\{a, b, c, d, 1, 2, 3, 4\}$

12. a. $\{1, 5, 8, 9, 11, 13, 14, 17, 20, 21\}$

    b. $\{5, 17, 29, 41\}$

15. a. $A \cap B \cap C$

    b. $(B \cup C) \cap (A' \cup C')$

    c. $(B \cup C) \cap (B' \cup C')$

16. a. $\forall x\ K(x)$

    b. $\exists x \forall p\ Q(x, p)$

    c. $\forall p \exists x\ Q(x, p)$

    d. $\forall x\ P(x)$

    e. $\neg[\exists x \forall p\ Q(x, p)]$

    f. $\neg[\exists x(x > 70) \wedge \text{Närv}(x)]$ (?)

    g. $\exists t \forall x\ t \geq x$

17. a. Någon elev blev underkänd på tentan.
    b. Alla elever blev underkända på något prov.
    c. Det fanns ett prov där alla elever underkändes.
    d. Det finns en präst som inte är prost.
    e. Någon elev klarade alla prov.
    f. Minst 71 personer var där
    g. Vilket tal man än väljer, finns det att annat tal som är större.

21. a. 7
    b. 288
    c. 299
    d. 407

22. a. $(4711)_{10} = (1001001100111)_2 = (11147)_8 = (1267)_{16}$.
    b. $(ABCD)_{16} = (43981)_{10}$.

23. 12

25. $19 \cdot 31$, primtal, $29 \cdot 31$.

27. SGD är $x - 1$. Den gemensamma roten är x=1.

28. Gemensamma nollställen är $x = -2$ och $x = 1$

29. Fredag.

33. a. $x = 1 + 6n,\ y = 18 - 5n$

b. $x = 5 + n \cdot 7, y = 73 - n \cdot 13$, $n = 0, 1, 2, 3, 4, 5$

34. Högst 278.

35. $n = 2221$ och $n = 3332$.

45. Det följer ur induktionsprincipen.

47. a. $a^0 = 1$ och $a^n = a \cdot a^{n-1}$ om $n \geq 1$.
    b. $\sum_{k=0}^{0} a_k = a_0$; $\sum_{k=0}^{n} a_k = a_n + \sum_{k=0}^{n-1} a_k$ om $n \geq 1$.

49. a. $x_n = 3 \cdot (3/2)^n$
    b. $x_n = 2^{n+1} - 3^n$
    c. $x_n = 1 - 3 \cdot 2^n + 2 \cdot 3^n$
    d. $x_n = 3 + (n-2)2^n$

50. $\dfrac{\left(-\left(1-\sqrt{5}\right)^{1+n} + \left(1+\sqrt{5}\right)^{1+n}\right)}{2^{1+n}\sqrt{5}}$

52. Minst 15 personer.

53. b. $|A| + |B| + |C|$
    $-|A \cap B| - |A \cap C| - |B \cap C|$
    $+|A \cap B \cap C|$

54. a. $5^3 = 125$
    b. $5 \cdot 4 \cdot 3 = 60$
    c. $3 \cdot 4 \cdot 3 = 36$

55. 120, 495, 4950

57. $2^n - 2$ stycken

58. På 18 900 sätt.

59. a. 720
    b. 120

60. $(2n-1)(2n-3)(2n-5)\cdots 3$

61. $13 \cdot 12\binom{4}{3}\binom{4}{2} = 3744$

62. 372

63. 16

69. Ja, om vi enbart ser till texten.