Diskret Matematik

Oscar Palm

Oktober-December 2021

Contents

Chapter 1

Läsvecka 1

1.1 Kursintroduktion

Kurs-PM på Canvassidan
Alla lärare: Christian Johansson, Rolf Andréasson, Victor Ahlquist

Tenta den 14/01-2022
Två duggor under tentan

- Slutet av november, mitten av december

Kursinnehåll:

- Logik och mängdlära
- Kombinatorik
- Grafteori
- Talteori
- (Kryptering)

Kursens innehåll definieras av de delar av kursboken som listas i programmet (på canvas?)

Logik:
Induktion "Kunskap från observationer"

- Statistik
- Kommer ej beröras under kursens gång

Deduktion "Ny kunskap från etablerad kunskap med hjälp av logiska argument"

Satslogik:

- Grundläggande begreppet inom satslogik är så kallade Utsagor
- Utsaga
- – - En utsaga är ett påstående som kan definieras antingen som falskt eller sant
  – - Detta innebär inte att det är simpelt att definiera huruvida det är sant eller falskt, enbart att det är möjligt att definiera.

Êx.

- 1. Göteborg är Sveriges huvudstad - Falskt
- 2. 1 November 2021 är en måndag - Sant
- 3. Jag ljuger - Inte en utsaga; en paradox
- 4. ICA är öppet - Inte en utsaga; innehåller inte tillräckligt med information för bedömning

Kommentarer:

- Ibland behöver vardagliga påståenden preciseras för att kunna tolkas som en utsaga.
- Alternativt behöver vi bestämma ett sammanhang för att kunna tolka uttrycket som en utsaga.

Hur skapar vi formellt sett en utsaga?:

- Inom satslogiken utgår vi ifrån att vi har en samling ”utsagor” och att det finns någon form av uttryckbart sanningsvärde för dessa.

Vad satslogiken behandlar är ej enbart de enskilda utsagorna, detta görs i andra sammanhang, utan hur logiska relationer och slutsatser går att dra sinsemellan dem.

Logiska operatorer:

- Hur vi från våra existerande utsagor kan skapa nya.
- Konjunktion P∧ Q ”P och Q”
  – P∧ Q är sann om och endast om både P är sann och Q är sann
- Disjunktion $P \vee Q$ ”P eller Q”
  – $P \vee Q$ är sann om och endast om P är sann och/eller Q är sann
- Negation ¬ ”Inte P” ”Icke P”
  – $\neg P$ är sann om och endast om P är falsk

- Implikation $P \rightarrow Q$ "P implicerar Q" eller "P medför Q" eller "Om P, så Q"
  - Kan också tolkas som $\neg P \vee Q$
  - Ex. Om det är en björn, så kan den simma; dvs. Antingen är det inte en björn, eller så kan den simma?
- Ekvivalens $P \leftrightarrow Q$ "P är ekvivalent med Q"
  - P om och endast om Q
- Tautologier
  - En sammansatt utsaga beroende på ett antal ingående utsagor som alltid är sann oavsett sannngsvärdena på ingångsutsagorna, ex. $P \vee \neg P$
  - ex. modus ponens
  - Hur kan vi kontrollera huruvida en sammansatt utsaga är en tautologi?
    - Bruteforcemetod: sanningstabell
    - Mer elegant: Omformulera uttrycket med hjälp av de olika lagarna för boolesk algebra; ex. De morgans lag, absorptionslagarna ...

Logiska relationer

- Hur flertalet utsagors sanningsvärden påverkar relaterade.
- P implicerar Q logiskt om $P \rightarrow Q$ är sann; dvs. $P \rightarrow Q$
- P är logiskt ekvivalent med Q om $P \leftrightarrow Q$ är sann; dvs. $P \Leftrightarrow Q$
  - Säger att P och Q har samma sanningsvärde

OBS!!!

- Boken använder små bokstäver för utsagor i sanningstabeller.
- Bokens resonemang är att p står för en s.k. boolesk variabel medan P står för en utsaga.

1.2 Predikatlogik och mängdlära (också logiska argument)

Logiska argument

- Ett logiskt argument består av tre huvuddelar
  - Hypoteser: $H^1, H^2, ...H^n$ (Utsagor)
  - Slutsats: C utsaga
  - Tillsammans är dessa sammansatta av andra, mer primitiva utsagor.?
  - Så att $H^1, H^2, ...H^n \rightarrow C$ är en tautologi när vi expanderar H-utsagorna till de mer primitiva utsagorna

Predikatlogik och Mängdlära - Två sidor av samma mynt?
Mängder:

- En mängd är löst uttryckt en väldefinierad samling av objekt där inget objekt kan existera mer än en gång.
  - Exempelvis alla reella tal eller samtliga naturliga tal
- Viktigt: För varje tänkbart objekt x och varje tänkbar mängd M skall man kunna avgöra om x tillhör M eller ej (i alla fall teoretiskt)
  - DVS: "x tillhör M" är en utsaga
- skriver $x \in M, x \notin M$(strecket egentligen genom)
- om $x \in M$ så kallas x för ett element i M
- Två sätt att definiera en mängd:
  - Uppräkning: lista samtliga objekt i mängden
    - M=Sthlm,Gbg,Malmö
    - M=Samtliga heltal
    - Spelar ingen roll vilken ordning uppräkningen sker i eller hur många gånger ett specifikt element räknas upp
  - Predikat: Ett sätt att utöka satslogiken genom att använda sig av variabler
    - Ofta vill man använda sig av påståenden som beror på variabler
    - $P(x) : 10 \leftarrow x$
    - Q(y) : y ligger i Asien
    - Dessa är inte utsagor utan sanningsvärdet beror på vad variablerna har för värden
    - Kan även kallas för öppen utsaga
    - Anges ett specifikt värde för variablerna skapas en vanlig utsaga av predikatet

    - Kan även skapa en utsaga av predikatet med hjälp av kvantifiering

- Def. två mängder är lika:
    - Två mängder M och N är lika om de innehåller samma element
    - $x \in M \Leftrightarrow x \in N : \forall x$
    - skriver M=N

Kvantifiering

- Universell kvantifiering $\forall$
    - För alla heltal x gäller P
    - Skrivs $\forall x \in M : P(x)$
- Existensiell kvantifiering $\exists$
    - Det existerar heltal y där Q
    - Skrivs $\exists y \in M : Q(y)$
    - (Ibland skrivs $\exists!$ för att definiera att exakt ett) - Används ej inom denna kurs, just a fun fact
- $\exists$ samt $\forall$ kallas kvantorer
- Om mängd är underförstått kan man skriva $\forall x P(x)$ och skippa definiering av mängden.

Quiz

- $\forall x \exists y : x > y$: sant
- $\exists y \forall x : x > y$: falskt, det finns inget minsta tal
- Poäng: Ordningen på kvantifiering spelar roll när vi har olika kvantorer inblandade

Mängdnotation 2 - Predikat

- Givet ett universum U och ett predikat P(x) kan man definiera en mängd
- $M = \{x \in U | P(x)\}$ M består av alla x i U så att P(x) är sann

Mängder med egna beteckningar:

- Finns på papper
- För mängd M, avser —M— antalet element i mängden (M.length()), även #M

Mängdoperatorer och mängdrelationer

- Tänker oss alla mängder som en del av ett universum
- Relationer:
  - M=N om och endast om $x \in M \Leftrightarrow x \in N$
  - $M \subseteq N$ om och endast om $x \in M \rightarrow x \in N$ (Varje element i M är ett element i N)
- Viktigaste mängdoperatorerna:
  - Union $M \cup N = \{x | x \in M \vee x \in N\}$
  - Snitt $M \cup N = \{x | x \in M^x \in N\}$
  - Komplement $M^c = \{x | x \notin M\}$
  - Mängddifferens $M \backslash N =$ Där x finns i M men ej i N
  - Kartesisk produkt Kolla upp själv (s.47-48)

Räkneregler inom mängdläran:

- Identitet
  - $A \cap U = A$
  - $A \cup \emptyset = A$
- Dominans
  - $A \cup U = U$
  - $A \cap \emptyset = \emptyset$
- Namnlös
  - $A \cup A^c = U$
  - $A \cap A^c = \emptyset$
- Idempotens
  - $A \cup A = A$
  - $A \cap A = A$
- Dubbelt komplement
  - $(A^c)^c$
- Kommutativitet
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Associativitet

  - $(A \cup B) \cup C = A \cup (B \cup C)$
  - $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributivitet
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$
- deMorgan
  - $(A \cap B)^c = A^c \cup B^c$
  - $(A \cup B)^c = A^c \cap B^c$
- Namnlös
  - $A \backslash B = A \cap B^c$

Venndiagram

- Fina cirklar för att visa hur operatorer påverkar mängder

Potensmängd: Mängden av alla delmängder

1.3 Funktioner

Det finns en mängd olika regler vi kan använda oss av för att förenkla logiska uttryck; associativa, kommutativa, de Morgans osv...

- s. 13 o s.45

Funktioner

- En funktion $f : A \to B$ är en regel som för varje $a \in A$ tilldelar ETT element $f(a) \in B$
  - Det får dock existera ej av A tilldelade element i B
- Terminologi:
  - A kallas för f's definitionsmängd
  - B kallas för f's målmängd
  - Delmängden $f(A) = \{b \in B | \exists a \in A : f(a) = b\} \subseteq B$ kallas för f's värdemängd eller bild
    - Värdemängd="allt som träffas av f"
- $f : A \to B, g : C \to D$
  - $f = g$ om $A = C, B = D$ och $f(x) = g(x) \forall x \in A = C$
- Egenskaper hos funktioner:
  - f är injektiv om $\forall x, y \in A : x \neq y \to f(x) \neq f(y)$
    - Varje invärde genererar ett unikt utvärde, ex. $f(x) = x + 1$
  - f är surjektiv om $f(A) = B$, dvs värdemängden=målmängden
    - "f träffar allt i B"
  - f är bijektiv om den är både injektiv och surjektiv
- Operationer på funktioner:
  - Invers: Om $f : A \to B$ är bijektiv kan man definiera en funktion $f^{-1} : B \to A$ genom att göra f baklänges (bryta ut x)
  - Sammansatta funktioner:
    - $f : A \to B$
    - $g : B \to C$
    - kan skapa ny funktion $g \circ f : A \to C, g \circ f(x) = g(f(x))$
- Om $f : A \to B$ är bijektiv med invers $f^{-1} : B \to A$ så är $f \circ f^{-1} = id_B$ och $f^{-}1 \circ f = id_A$

Varning: f^{-1} är inte $\frac{1}{f(x)}$

Operatorer:

- En n-är operator på A är en funktion vars input är n element i A (ordnade) med output ett element i A
- Viktigaste fallen: $n = 2$, binär operator $x \times y \to A$
- $n = 1$, unär operator $x \to A$

1.4 Summor, produter och relationer

Summor och produkter:

- Ibland är det bättre att skriva en talföljd $a_1, a_2, ..., a_n$ mha ett index $a_i, i = 1, 2, ..., n$
- Samma sak med summor :
  - $a_1 + a_2 + ... + a_n$ kan skrivas som $\sum_{i=1}^{n} a_i$
- Fördelar:
  - Mer kompakt
  - Mer väldefinierat
- Nackdel: Möjligtvis mindre intuitivt
- Produkter kan skrivas på samma sätt
  - Använder $\prod$ istället för $\sum$
  - Ex. $\sum_{j=2}^{4} j^2 = 2^2 + 3^2 + 4^2 = 4 + 9 + 16 = 29$
  - $\prod_{k=3}^{5}(k-1) = 2 \times 3 \times 4 = 24$
- Variant
  - Ibland uttrycker man indexeringen med en mängd
  - Ex. $\sum_{j=2}^{4} j^2$ kan också skrivas $\sum_{j \in M} j^2, M = \{2, 3, 4\} = \{j | j = 2, 3, 4\}$

Relationer

- Def A,B två mängder. En relation R från A till B är en delmängd $R \subseteq A \times B$
- Kom ihåg $A \times B = \{(a, b) | a \in A, b \in B\}$
- Tänker $x \in A, y \in B$
- $(x, y) \in R$ tolkas som "x är relaterat till y"
- $(x, y) \notin R$ tolkas som "x är inte relaterat till y"
- Skriver oftast xRy istället för $(x, y) \in R$
- Ex.
  - $A = B = \mathbb{Z}$. Definiera en relation $R \subseteq \mathbb{Z} \times \mathbb{Z}$ som $(x, y) \in R \Leftrightarrow x \leq y$
  - $A = B = \{utsagor\}$, definiera $R \subseteq A \times A$ genom $(P, Q) \in R \Leftrightarrow P \rightarrow Q$

- $A = \{cities\}, B = \{countries\}$ $(x, y) \in R \Leftrightarrow xliggeriy$

- Visualisering (I don't know how to paint in latex =/) Exemplet var på en riktad graf? $R = \{(1,2),(1,1),(2,2),(3,3)\} \subseteq A \times A$

- Egenskaper hos relationer
  - $A = B$ från och med nu. R relation på A
  - R är :
    - *Reflexiv*: om xRx $\forall x \in A$
    - *Symmetrisk*: om $xRy \Rightarrow yRx$ $\forall x, y \in A$
    - *Antisymmetrisk*: om $(xRy \wedge yRx) \Rightarrow x = y$ $\forall x, y \in A$
    - *Transitiv*: om $(xRy \wedge yRz) \Rightarrow xRz$ $\forall x, y, z \in A$
    - *Partiell ordning*: om R är reflexiv, antisymmetrisk och transitiv
    - *Ekvivalensrelation*: om R är reflexiv, symmetrisk och transitiv
    - $A = \mathbb{Z}, R = \leq$
      - Reflexiv? Ja, $x \leq x$ $\forall x \in \mathbb{Z}$
      - Symmetrisk? Nej, $x \leq y \Rightarrow y \leq x$
      - Antisymmetrisk? Ja $(x \leq y \wedge y \leq x) \Rightarrow x = y$
      - Transitiv? Ja, $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$
      - Så $\leq$ är en partiell ordning
    - $A = \{utsagor\}, R =$ " $\Rightarrow$ "
      - $\forall u \in A$
      - Reflexiv? Ja, $u \Rightarrow u = true$
      - Symmetrisk? Nej, $(u \Rightarrow v) \Rightarrow (Q \Rightarrow P) \neq true$
      - Antisymmetrisk? Nej, $(P \Rightarrow Q \wedge Q \Rightarrow P) \Rightarrow P = Q \neq true$
      - Transitiv? Ja, $(P \Rightarrow Q \wedge P \Rightarrow S) \Rightarrow P \Rightarrow S = true$
      - Inte en partiell ordning
      - Inte en ekvivalensrelation
    - $P \rightarrow S$ är sant. Vill visa det utifrån $P \rightarrow Q$ sann och $Q \rightarrow S$ sann
      - Motsägelsebevis: $P \rightarrow S$ falsk ger P sann, S falsk.
      - $Q \rightarrow S$ sann och S falsk ger Q falsk, men då är $P \rightarrow Q$ falsk motsägelse.

- Ekvivalensrelationer
  - $A = \{cities\}$ definiera xRy som "x ligger i samma land som y"
    - Reflexiv: "x ligger i samma land som x"? Ja
    - Symmetrisk: "x ligger i samma land som y" medför "y ligger i samma land som x"? Ja
    - Antisymmetrisk: "x ligger i samma land som y" och "y ligger i samma land som x" medför "x är samma stad som y"? Nej

    - Transitiv: "x ligger i samma land som y" och "y ligger i samma land som z" medför "x ligger i samma land som z"? Ja
    - R är en ekvivalensrelation
  - Länderna kallas för ekvivalensklasser
    - R ekvivalensrelation på A. om $x \in A$ sätter vi $[x] = \{y \in A | xRy\}$
    - $[x]$ kallas för x:s ekvivalensklass
  - Egenskaper:
    - $x \in [x]$ (xRx ty R reflexiv)
    - $xRy \Leftrightarrow [x] = [y]$
    - x inte relaterad till y $\Leftrightarrow [x] \cap [y] = \emptyset$
  - Ex:
    - $A = \{cities\}$ R=ligger i samma land
    - Om x är en stad, $[x]$ = {alla städer som ligger i samma land som x}
    - ex. $[Oslo]$ = {alla städer i Norge}
  - Ett annat sätt att tänka kring ekvivalensrelationer; Partitioner:
    - Notation:
      - I indexmängd,$\forall i \in I$ har vi en mängd A_i
      - Vi definierar $\bigcup_{i \in I} A_i = \{x | \exists i : x \in A_i\}$
      - Unionen av alla A_i, för $i \in I$
    - En partition av en mängd B är en samling delmängder $A_i \subseteq B$ indexerade av en mängd I, så att
      - $B = \bigcup_{i \in I} A_i$
      - $A_i \cap A_j$ om $i \neq j$

Partitioner och ekvivalensrelationer är ekvivalent koncept:

- Om R är en ekvivalensrelation på B så är R:s ekvivalensklasser en partition av B.
- Om $B = \bigcup_{i \in I} A_i$ är en partition, så kan jag definiera en ekvivalensrelation R genom $xRy \Leftrightarrow$x och y ligger i samma cell A_i

Kommutativitet och associativitet

- Kommutativitet: En relation är kommutativ om $\forall x, y \in U : x * y = y * x$
- Associativitet: En relation är associativ om $\forall x, y, z \in U : x * (y * z) = (x * y) * z$
- Identitet: Ett element är en identitet för * om $a * e = e * a = a \ \forall a \in A$

Chapter 2

Läsvecka 2

2.1 Föreläsning 1 - Induktion, Rekursion, Summor

2.1.1 Uppvärmning:

Vad är $1+2+3+...+100$? $\sum_{n=1}^{100} n = 101 \times 50 = 5050$

2.1.2 Aritmetiska summor

En aritmetisk talföljd är en talföljd $a_1, a_2, ..., a_n$ där $a_2 - a_1 = a_3 - a_2 = a_4 - a_3 = ... = a_n - a_{n-1}$

Ex. $\sum_{n=1}^{100} n$, skillnaden d är 1.

Ex. $3, 7, 11, 15$, skillnaden d är 4.

Om $a_1, ..., a_n$ är en aritmetisk talföljd så kallas $a_1 + ... + a_n = \sum_{i=1}^{n} a_i$ för en aritmetisk talföljd.

För en aritmetisk summa gäller $\sum_{i=1}^{n} a_i = n \times \frac{a_1 + a_n}{2}$

2.1.3 Geometrisk talföljd

En talföljd $a_1, ..., a_n$ kallas geometrisk om $\frac{a_2}{a_1} = \frac{a_3}{a_2} = ... = \frac{a_n}{a_{n-1}}$

Ex. $2, 4, 8, 16, 32$, kvoten d är 2.

Ex. $4, 12, 36, 108$, kvoten d är 3.

Om $a_1, ..., a_n$ är en geometrisk talföljd kallas $\sum_{i=1}^{n} a_i$ för en geometrisk summa.

Om $c = \frac{a_2}{a_1} = ... = \frac{a_n}{a_{n-1}}$ och $c \neq 1$ så är $\sum_{i=1}^{n} a_i = a_1 \times \frac{c^n - 1}{c - 1}$

Varför? $a_1, a_2 = a_1 c, a_3 = a_1 c^2, ..., a_n = a_1 c^{n-1}$

$(c-1)\sum_{i=1}^{n} a_i = (c-1)(a_1 + a_1 c + a_1 c^2 + ... + a_1 c^{n-1}) = a_1(c-1)(1 + c + c^2 + ... + c^{n-1}) = a_1(c^n - 1)$

2.1.4 Induktion och Rekursion

- Rekursion är en definitionsteknik där man definierar en funktion/talföljd "steg för steg".
- Induktion är en bevisteknik där man bevisaren följd $P_1, P_2, ..., P_n$ av utsagor "steg för steg".
- $\mathbb{OBS}$! En oändlig talföljd $a_1, a_2, ...$ är samma sak som en funktion $f : \mathbb{Z}_+ \to \mathbb{R}$

$f : \mathbb{Z}_+ \to \mathbb{R}$ är rekursivt definierad om $\exists a \in \mathbb{Z}_+$ så att

1) $f(1), ..., f(a)$ är givna. (startvärden)

2) $\forall n \geq a + 1$ är $f(n)$ en funktion av $f(1), ..., f(a)$. (Rekursion)

$\mathbb{INTE}$ $\mathbb{BRA}$!, inte tillräckligt precis.

Problemet ligger i 2)
Kan jag använda olika funktioner för olika n?
Ser nästan ut så eftersom antalet argument växer.
Vilken typ av funktion får det vara?

$f : \mathbb{Z} \to \mathbb{R}$ är rekursivt definierad om $\exists a \in \mathbb{Z}_+$ och en funktion $h : \mathbb{R}^{a+1} \to \mathbb{R}$ så att

1. $f(1), .., f(a)$ är givna
2. $f(n) = h(f(n-a), f(n-a-1), ..., f(n-1), n)$
   $\forall n \geq a + 1$

Ex. $a = 1, h(x, y) = x \times y$
Om $f(1) = 1$ och $f(n) = h(f(n-1), n) = n \times f(n-1), n \geq 2$
Så $f(2) = f(1) \times 2 = 2, f(3) = f(2) \times 3, ..., f(n) = n!$
Ex. $a = 2$: Fibonacci-talföljden
$\{^{f(1)=1, f(2)=1}_{f(n)=f(n-1)+f(n-2), n\geq 3}\}$
$1, 1, 2, 3, 5, 8, 13, 21, ...$

Induktion

Låt $P_1, P_2, P_3, ...$ vara utsagor. (En utsaga P_n $\forall n \in \mathbb{Z}_+$)
Om:

1. P_1 är sann Kallas basfallet
2. $P_n \Rightarrow P_{n+1}$ $\forall n \in \mathbb{Z}_+$ Kallas induktionssteget
3. Så är P_n sann $\forall n \in \mathbb{Z}_+$

Tänk $P_1 \to P_2 \to P_3 \to P_4 \to ...$
Ex. Geometrisk summa, vill visa $1 + c + ... + c * n - 1 = \frac{c^n - 1}{c-1}$ $\forall n \in \mathbb{Z}_+$
Utsaga $P_n : \sum_{i=0}^{n-1} c^i = \frac{c^n - 1}{c-1}$, $n = 1, 2, 3, ...$

Basfall: Är P_1 sann?

$P_1 : \sum_{i=0}^{0} c^1 = \frac{c^n-1}{c-1} = 1$ är sann.

Induktionssteg: Vill visa $P_n \Rightarrow P_{n+1}$

DVS. om P_n är sann, så är P_{n+1} sann.

Antag att P_n är sann, dvs $1 + ... + c^{n-1} = \frac{c^n-1}{c-1}$

Vill visa P_{n+1} sann, dvs $1 + ... + c^{n-1} + c^n = \frac{c^n+1-1}{c-1}$

$1 + c + ... + c^{n-1} + c^n = \frac{c^n-1}{c-1} + c^n = \frac{c^n-1}{c-1} + \frac{(c-1)c^n}{c-1} = \frac{c^n-1+c^{n+1}-c^n}{c-1} = \frac{c^{n+1}-1}{c-1}$

Vilket är vad vi ville visa. Avslutar induktionssteget.

Enligt induktionsprincipen är P_n sann $\forall n \in \mathbb{Z}_+$.

Varianter:

Stark induktion, om:

1) P_1 sann
2) $P_1 \wedge ... \wedge P_n \Rightarrow P_{n+1}$
   $\forall n \in \mathbb{Z}_+$

Starkare induktionsantagande. Antar $P_1 \wedge ... \wedge P_n$, inte bara P_n

Fler basfall, om:

1) $P_1, ..., P_m$ är sanna
2) $P_1 \wedge ... \wedge P_n \Rightarrow P_{n+1}$
   $\forall n \geq m$

Så är P_n sann $\forall n \in \mathbb{Z}_+$

2.2 Föreläsning 2 - Kombinatorik

2.2.1 Fortsättning från föregående

Utsagor $P_1, P_2, ...$

Stark induktion med flera basfall:

1. $P_1, ..., P_m$ är samma för något m
2. $P_1 \wedge ... \wedge P_n \Rightarrow P_{n+1}, \forall n \geq m$

så är P_n sann $\forall n \in \mathbb{Z}_+$

Ex. Definiera $\begin{cases} a_0=0, a_1=1 \\ a_n=5a_{n-1}-6a_{n-2}, \forall n \geq 2 \end{cases}$

$a_0 = 0, a_1 = 1, a_2 = 5 \times 1 - 6 \times 0 = 5, a_3 = 5 \times 5 - 6 \times 1 = 19, ...$

Visa att $a_n = 3^n - 2^n$, för alla $n \geq 0$

Basfall: $a_0 = 0, f(0) = 3^0 - 2^0 = 0$ OK, $a_1 = 1, f(1) = 3^1 - 2^1 = 1$ OK

Induktionssteg:

Antag att $n \geq 2$ och att $a_k = f(k)\ \forall k < n$

Vi vill visa att $a_n = f(n)$

$a_n = 5a_{n-1} - 6a_{n-2} = 5fn - 1 - 6f(n-2) = 5 \times 3^{n-1} - 5 \times 2^{n-1} - 6 \times 3^{n-2} + 6 \times 2^{n-2}$

$= 3^{n-2}(9) - 2^{n-2}(4) = 3^{n-2} \times 3^2 - 2^{n-2} \times 2^2 = 3^n - 2^n$

Enligt induktionsprincipen är $a_n = 3^n - 2^n$

2.2.2 Andra bevistekniker

Kontrapositivt påstående

$(P \to Q) \Leftrightarrow (\neg Q \to \neg P)$

Ex. Vill visa (n^2 jämn $\to n$ jämn), n heltal

$n = 2m + 1 \Rightarrow n^2 = (2m + 1)^2 = 2(2m^2 + 2m) + 1 \neq$ jämn

Motsägelsebevis

$(\neg P \to Q \wedge \neg Q) \Rightarrow P$

Om antagandet att P är falsk leder till en motsägelse, så måste P vara sann.

2.2.3 Kombinatorik

Hur många sätt kan man göra saker på?

Multiplikationsprincipen

Antag att vi ska göra k stycken oberoende val och att dessa val individuellt kan göras på $n_1, n_2, ..., n_k$ olika sätt.

Då är antalet sätt de k valen kan göras på $\prod_{i=1}^{k} n_i$

Permutationer

Notera: om A är en mängd, skriver vi $|A|$ för antalet element i A
Låt a vara en mängd med $n$element.
En Permutation av r element i A ($o \leq r \leq n$) är en uppräkning $x_1, x_2, ..., x_r$av r olika element ur A där ordningen spelar roll.
Alternativ formulering: Vi väljer r element ur A, och ordningen spelar roll.
Hur många permutationer av r element ur A finns det?
Ex. Permutationer av 2 element ur $B = \{1, 2, 3\}$
Första talet: 1/2/3
Andra talet: ett av de 2 kvarvarande taken.
Totalt 6 permutationer.
Allmänt: Skall välja r element $x_1, ..., x_r$ ur A, $|A| = n$.
x_1 kan väljas på n olika sätt.
x_2 kan väljas på $n - 1$ olika sätt
x_3 kan väljas på $n - 2$ olika sätt
x_r kan väljas på $n - (r + 1)$ olika sätt
Slutsats: Permutationen $x_1, ..., x_r$ kan väljas på $n(n-1) \times (n-2) \times ... \times (n - r + 1) = \prod_{i=1}^{r}(n - i + 1)$ olika sätt.

Fakultetsfunktionen
$n! = 1 \times 2 \times ... \times n = \prod_{i=1}^{n} i$, $n \in \mathbb{Z}_+$
Ex. $4! = 1 \times 2 \times 3 \times 4 = 24$
Kan skriva om:
$n(n-1) \times ... \times n(n-r+1)$ är samma som
$\frac{n(n-1)\times...\times n(n-r+1)\times n(n-r)\times...\times 1}{n(n-r)\times n(n-r-1)\times...\times 1} = \frac{n!}{(n-r)!}$
Långsammare och svårare att räkna ut men kan skrivas mer kompakt
Om $r = n$ kan tänka på det som antalet sätt att ordna n element.

Kombinationer

En kombination av r element ur en mängd A är ett val av r olika element element ur A, där ordningen inte spelar roll.
Mer formellt: En kombination av r element ur A är en delmängd av A med r element.
Ex. Kombinationer av 2 element ur $B = \{1, 2, 3\}$ Hur många finns det?.
Det finns 6 permutationer men då ordningen inte spelar roll försvinner flertalet.
Varje kombination dyker up 2 ggr, dvs Antalet kombinationer$= \frac{Permutationer}{2} = \frac{6}{2} = 3$
Mer generellt:
$\frac{\frac{n!}{(n-r)!}}{r!} = \frac{n!}{r!(n-r)!}$
Allmänt: Hur många kombinationer av r element ur A finns det om $|A| = n$?

Kombinationer=$\frac{Permutationer}{r!}$

Uttrycket $\frac{n!}{r!(n-r)!}$ skrivs $\binom{n}{r}$, utläses ”n över r”, alternativt ”n välj r”.

Kallas för binomialkoefficienter.

Hur man räknar ut:

$\binom{7}{4} = \frac{7\times6\times5}{1\times2\times3} = 35$

$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!/r!}{r!(n-r)!/r!}$

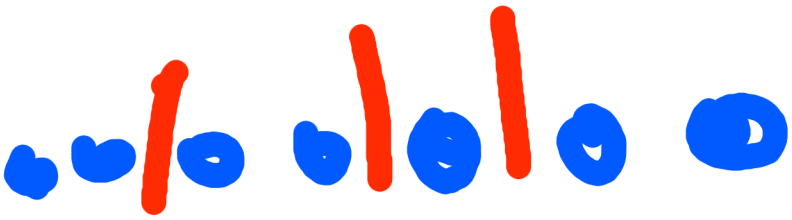
Chapter 3

Läsvecka 3

3.1 Föreläsning 1 - Problemlösning

3.1.1 Kombinatorisk problemlösning

På hur många sätt kan man fördela 7st likadana bollar i fyra lådor?



Om bollarna varit olika hade kunnat använda multiplikationsprincipen, ger 4^7 möjligheter.
En uppdelning är sekvens, med 7 bollar och 3st ”avdelare”.
På hur många sätt kan jag skapa en sådan sekvens?

- Har totalt 10 st symboler (7 bollar + 3 väggar)
- Kan göras på $\binom{10}{3}$ sätt och $\binom{10}{3} = \frac{10\times9\times8}{1\times2\times3} = 10 \times 3 \times 4 = 120$
- Slutsats: Man kan fördela n lika objekt i k olika lådor på $\binom{n+k-1}{k-1}$ sätt.n

Ex: Tre barn skall få 8 äpplen. På hur många sätt kan äpplena fördelas om

1. Det inte finns några restriktioner?
2. Alla skall få minst ett äpple?
3. Äldsta barnet skall få max 4 äpplen?

Svar:

1. $\binom{8+3-1}{3-1} = \binom{10}{2} = \frac{10\times9}{2} = \frac{90}{2} = 45$ sätt.
2. Ge barnen varsitt äpple först; $8 - 3 = 5$ äpplen kvar. $\binom{5+3-1}{3-1} = \binom{7}{2} = \frac{7\times6}{2} = \frac{42}{2} = 21$
3. Vänd på problemet, om äldsta ska få minst 5; ge 5 till äldsta och räkna: $\binom{3+3-1}{3-1} = \binom{5}{2} = \frac{5\times4}{2} = 10$ sätt.
   (Antalet sätt där äldsta$\leq$ 4)=(Antal sätt utan restriktioner)-(Antal sätt där äldsta$\geq$ 5)= $45 - 10 = 35$

3.1.2 Räkna saker på två sätt

$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$
Varför?
$\binom{n+1}{k}$ är antalet sätt vi kan välja k st tal ur $\{1, 2, ..., n + 1\}$
Vi kan också beräkna det på ett annat sätt:

- Antingen är $n + 1$ med eller inte.

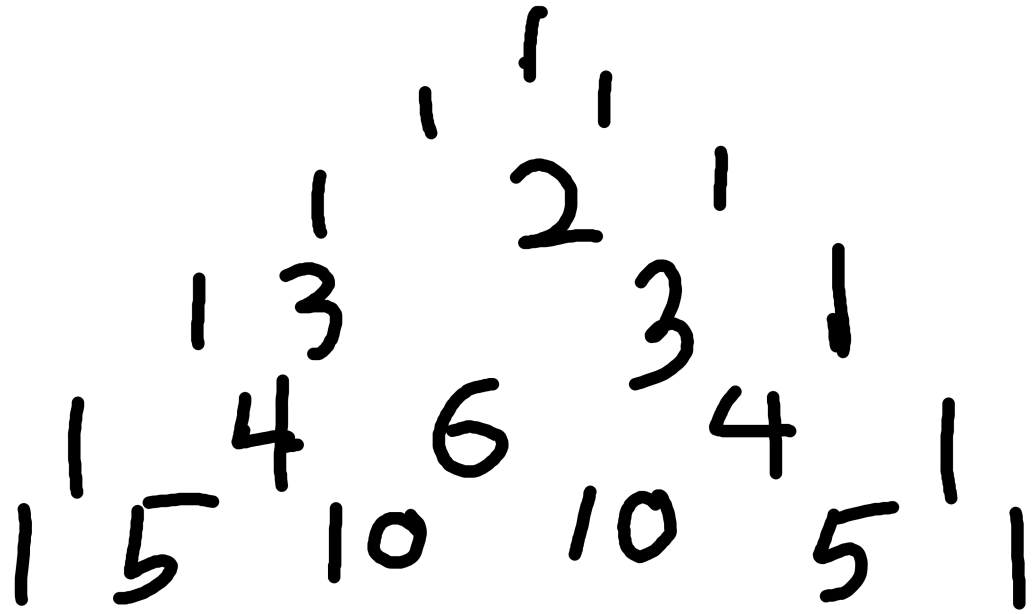
- Om $n+1$ inte är med: Alla k talen ska väljas från $\{1,2,...,n\}$, kan göras på $\binom{n}{k}$ sätt.
- On $n+1$ är med: resterande $k-1$ ska väljas från $\{1,2,...,n\}$, kan göras på $\binom{n}{k-1}$ sätt.

Totalt kan k tal väljas ur $\{1,2,...,n+1\}$ på $\binom{n}{k}+\binom{n}{k-1}$ sätt.

Alltså måste $\binom{n+1}{k}=\binom{n}{k}+\binom{n}{k-1}$.

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

Kan användas för att visualisera binomialkoefficienterna i Pascals triangel.



Tal nr k på rad nr n är $\binom{n}{k}$.

Binomialsatsen

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

$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$

kap. 6.14 i boken.

3.1.3 Lådprincipen (Pigeon hole principle)

Om $n + 1$ objekt placeras i n lådor så måste det finnas minst en låda med fler än 1 objekt i sig.

Ex. 25 elever går i en skolklass. Visa att minst tre st är födda i samma månad.
Existerar 25 elever och 12 månader.
Placerar vi 2 elever per månad (så utspritt det går) finns en elev kvar att placera, dvs. minst tre elever måste placeras i samma månad.

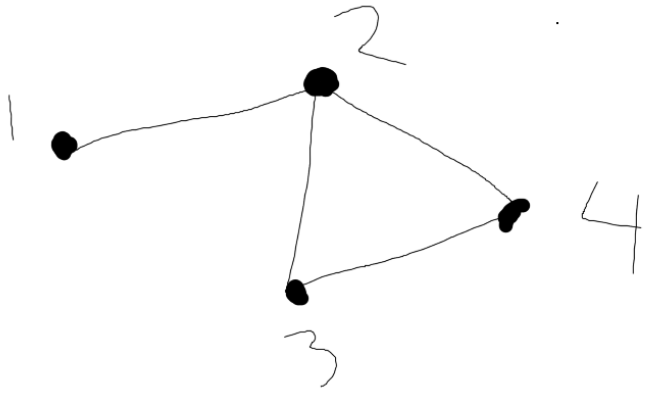
Ex. 40 personer går på en fest. Visa att minst två personer har skakat hand med lika många personer på festen.
Objekt: 40 pers; Lådor: Antalet personer de skakar hand med.
Om en person har skakat hand med 39 pers, så finns det ingen i låda 0. dvs. av de 40 lådorna kan enbart existera objekt i 39 av dem simultant, låda 0 och 39 är exklusiva.
Det kommer existera högst 39 icke-tomma lådor och exakt 40 objekt, dvs. enligt lådprincipen måste minst 2 objekt koexistera i en låda.

Ex. Fem personer skall stå i ett kvadratiskt rum med minst 2m mellan varje person, hur litet kan rummet vara?

3.2 Föreläsning 2 - Grafer och riktade grafer, träd

3.2.1 Grafer

Formellt: En graf består av en mängd V av noder (vertices) och en mängd $E \subseteq \{x, y| \subseteq x \neq y\}$ av kanter (edges).



- $V = \{1, 2, 3, 4\}$
- $E = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

Mellan varje par av noder får det finnas högst en kant.

.

Kapitel 1: 3, 4a, 6, 7abdfg, 8, 10, 11, 12, 17, 18

3.2.2 Delgrafer

$G = (V, E)$, $G' = (V', E')$ två grafer.

1. G' är delgraf till G om $V' \subseteq V$ och $E' \subseteq E$.
2. G' är inducerad delgraf till G om G' är en delgraf till G och om $\{x, y, \} \in E$ med $x, y \in V'$ så är $\{x, y\} \in E'$. ("om $x, y \in V'$ och det finns en kant mellan x och y i G så ligger den kanten också i G'")

Bipartitet och fullständiga delgrafer

- En graf kallas fullständig om det finns kanter mellan alla par av noder.
- En graf kallas bipartit om det finns en partition $V = A \cup B$, $A, B \neq \not{G}$ så att varje kant i G går mellan en nod i A och en i B.
- En graf kallas fullständigt bipartit om $\forall x \in A$, $\forall y \in B$ gäller att $\{x, y\} \in E$, dvs det finns en kant mellan x och y.

3.3 Föreläsning 3 - Vägar och cykler

3.3.1 Dugga

Första duggan är fredag 26/11 08:00-08:45
3 problem med 4p/problem.
4p = 1bonuspoäng
8p = 2 bonuspoäng.
Kom i god tid!

Övningsdugga kommer senast måndag.

3.3.2 Riktade grafer

Riktade grafer = grafer med pilar på kanterna.
Formellt: $G = (V, E)$
V = Mängd av noder.
$E \subseteq V \times V$ mängd av (riktade) kanter.
Graf: kanter är oordnade par $\{x, y\}$
Riktad graf: kanter är ordnade par (x, y)

Vi tillåter:

- Öglor
- Två kanter mellan två noder (om de går åt olika riktningar)

Vi tillåter inte:

- Mer än en riktad kant med samma start- och slutnod.

OBS! Formellt är en riktad graf med nodmängd V exakt samma sak som en relation på V.
Använde det när vi visualiserade relationer.

Liknande begrepp som för vanliga grafer

- Riktad väg - $v_0, v_1, ..., v_n \in V$ så att $(v_0, v_1), (v_1, v_2), ..., (v_{n-1}, v_n) \in E$
- Riktad cykel - Riktad väg $v_0, v_1, ..., v_n$ med $v_0 = v_n$ och där inga kanter upprepas.
- Starkt sammanhängande - G är starkt sammanhängande om det, för varje par av noder $x \neq y \in V$ finns en riktad väg som börjar i x och slutar i y.
- Sammanhängande - G är sammanhängande om dess underliggande graf är sammanhängande.

Underliggande grafen till en riktad graf

Två steg:

1. Ta bort pilarna.
2. Ta bort alla "öglor" och dubbla kanter.

3.3.3 Tillbaka till vanliga grafer

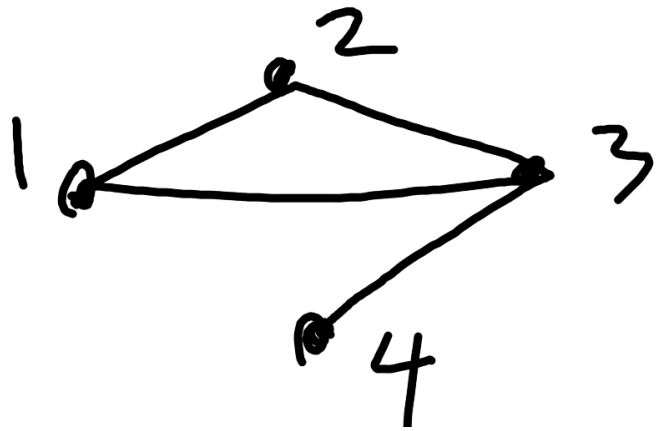
Träd: $G = (V, E)$ vanlig graf är ett träd om G är sammanhängande och inte innehåller några cykler.
Skog: $G = (V, E)$ Vanlig graf är en skog om G ej är sammanhängande men ej innehåller några cykler.

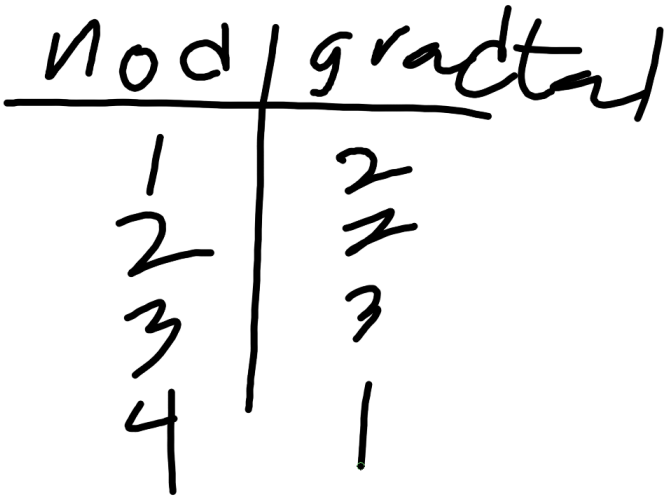
Två resultat om träd:

1. $G = (V, E)$ är ett träd $\Leftrightarrow$ G är sammanhängande och $|E| = |V| - 1$
2. $G = (V, E)$ är ett träd $\Leftrightarrow$ mellan varje par av noder $x, y \in V$ finns en unik väg från x till y

3.3.4 Gradtal

$G = (V, E)$ graf.
$x \in V$ nod.
Gradtalet för x i G är antalet kanter vars ena nod är x = Antalet noder i G som är länkade till x via en kant.
Skrivs d_x





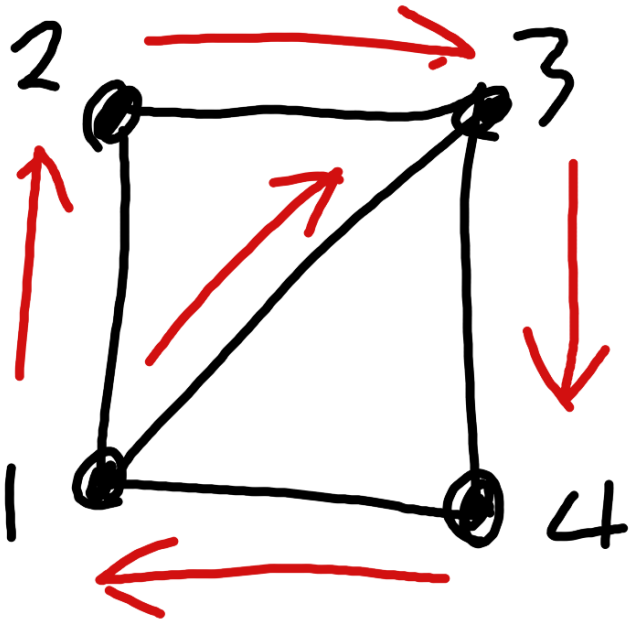
Summan 8, grafen har 4 kanter.

Sats: $G = (V, E)$ graf. Då är $\sum_{x \in V} d_x = 2 \times |E|$
Varför? Varje kant $\{v, w\} \in E$ bidrar med 1 till d_v och med 1 till d_w och med 0 till resterande gradtal. Varje kant bidrar alltså ned +2 till $\sum_{x \in V} d_x$
Följdsats: (7.3,7.4 i bok)

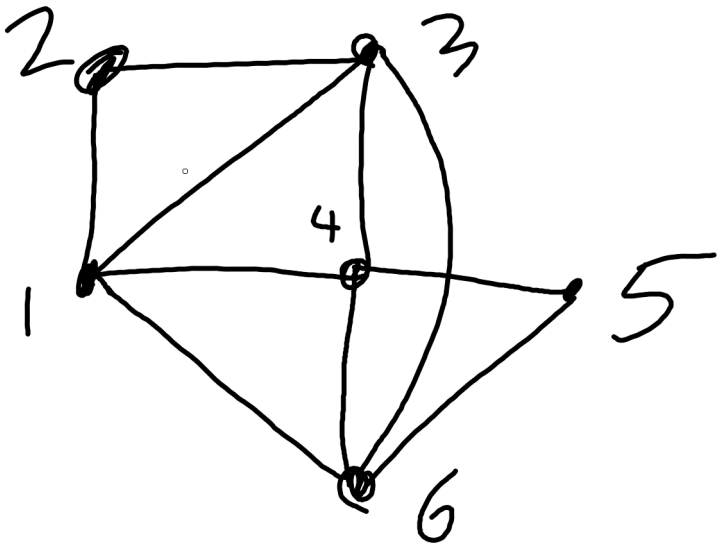
1. $\sum_{x \in V} d_x$ är ett jämt tal.
2. Antalet $x \in V$ med d_x är udda måste vara jämnt.

3.3.5 Eulervägar och Eulercykler

$G = (V, E)$ graf.
En Eulerväg i G är en väg i G som innehåller samtliga kanter i G exakt gång.
En Eulerväg som också är en cykel kallas för en Eulercykel.



1,2,3,4,1,3 är en Eulerväg, dock ej en Eulercykel.
(Finns ingen Eulercykel i grafen)



Har Eulercykel.

Hur vet man huruvida det existerar Eulercykel för en graf?
G har (minst) en Eulercykel $\Leftrightarrow$ alla gradtal i G är jämna.

Hur vet man huruvida det existerar Eulerväg för en graf?

Låt $x, y \in V, x \neq y$. G innehåller en Eulervåg som börjar i x och slutar i y $\Leftrightarrow d_x$ och d_y är udda och alla andra gradtal är jämna.

Hur kan man hitta Eulercykler?

Ett sätt: Hitta mindre cykler och lägg ihop dem.

3.4 Namnen spelar faktiskt roll

- P_n En väg
- C_n En cykel
- K_n En fullständig graf

Chapter 4

Läsvecka 4

4.1 Föreläsning 1 - Matriser

4.1.1 Vad är en matris?

En matris är en ”rektangulär tabell av tal”

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 3 & 2 & 1 \\ 5 & 8 & 3 \end{pmatrix} \quad \begin{pmatrix} 2 & 1 & 1 \\ 3 & 8 & \pi \\ e & 7 & 0 \\ 4 & 1 & \pi^2 \end{pmatrix}$$

2x2-matris 2x3-matris 4x3-matris

En matris har ett antal rader och ett antal kolumner/kolonner.
Om antalet rader är m och antalet kolumner är n så säger vi att vi har en $m \times n$-matris.
Allmän form:

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix} m \times n - matris$$

Alternativt:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & ... & a_{1,n} \\ a_{2,1} & a_{2,2} & ... & a_{2,n} \\ ... & ... & ... & ... \\ a_{m,1} & a_{m,2} & ... & a_{m,n} \end{pmatrix}$$ Om man behöver vara extra tydlig.

A_{ij}=talet på rad i och kolumn j = talet på plats (i, j)
$1 \leq i \leq m \quad 1 \leq j \leq n$

4.1.2 Räknesätt för matriser

Addition och subtraktion

Låt A och B vara två $m \times n$-matriser **OBS!** A och B är lika stora.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

Definition addition:

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

Definition subtraktion:

$$A - B = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} & \dots & a_{1n} - b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} - b_{m1} & a_{m2} - b_{m2} & \dots & a_{mn} - b_{mn} \end{pmatrix}$$

Multiplikation

Skalärprodukt:

- $a = \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix}$ kallas radvektor.
- $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ kallas kolumnvektor.

Skalärprodukten $a \bullet b$ definieras som

$a \bullet b = a_1b_1 + a_2b_2 + ... + a_nb_n = \sum_{i=1}^{n} a_ib_i$ och är ett tal(skalär), vilken kan ses som en 1×1-matris.

OBS! Skalärprodukten är endast definierad om de tär lika många tal i radvektorn som i kolumnvektorn.

En matris $A = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}$ kan vi tänka på A som mst radvektorer.

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \quad \begin{matrix} a_1 = \begin{pmatrix} a_{11} & \dots & a_{1n} \end{pmatrix} \\ a_2 = \begin{pmatrix} a_{21} & \dots & a_{2n} \end{pmatrix} \\ \vdots \\ a_m = \begin{pmatrix} a_{m1} & \dots & a_{mn} \end{pmatrix} \end{matrix}$$

Sats A $m \times n$-matris, B $n \times r$ och C $r \times s$-matris.

Då är $(AB)C = A(BC)$ (matrismultiplikation är associativ).

4.1.3 Tillämpning på riktade grafer

$G = (V, E)$, riktad graf med $V = \{1, 2, 3, \ldots, n\}$.

Def: Grannmatrisen $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$ $n \times n$-matris till G är definierad genom???

OBS! Från A kan man återskapa G, så A är ett sätt att representera G $A_{ij} = 1$ om det finns en riktad kant i G från i till j, 0 om det inte finns en riktad kant i G från i till j.

4.2 Seminarium

Problem 1: Hur många femsiffriga tal *utan nollor* finns det om

- a) exakt en siffra ska vara udda?

- b) minst tre siffror ska vara jämna och övriga siffror ska vara olika?

a) $\binom{4}{1}^4 \times 5^2$
b)$5 \times 4 \times \binom{5}{2} \times 4^3 + 5 \times \binom{5}{1} \times 4^4 + 4^5 = 20224$

Problem 2: Låt $n \geq 3$ vara ett udda tal. n stycken revolvermän står i en öken. Inga två revolvermän står på samma avstånd från varandra. Samtliga revolvermän drar sin revolver samtidigt och skjuter på den som står närmast, visa att minst en revolverman inte blir träffad.
Lösning: Induktion på n: $\overset{n=udda,\geq 3}{,3,5,7,\ldots}$
Basfall $n = 3$ Alltid ett par med minsta avstånd mellan varandra.
Induktionssteg:

- Antag att, för nst revolvermän som skjuter på varandra, så blir minst en person inte träffad.

- Vill visa samma påstående fast med $n + 2$st revolvermän.

- Än en gång existerar det två st revolvermän med kortaste avtåndet mellan sig, dessa skjuter varandra.

Problem 3: Låt $n \in \mathbf{Z}_+$ och låt $K_{1,n}$ vara den fullständiga bipartita grafen med $1 + n$ noder.
(a) för vilka n har $K_{1,n}$ en Eulerväg respektive en eulercykel?
(b) Om det inte finns en Eulercykel, vad är det minsta antalet kanter man behöver ta bort och/eller lägga till för att det skall finnas en Eulercykel? Den resulterande grafen skall fortfarande vara sammanhängande.

4.3 Googles PageRank-algoritm

Internet är en riktad graf

Noder är hemsidor

En ritad kant från X till Y är en länk på sidan X till sidan Y

4.3.1 Background

Gamla sökmotorer som Yahoo och Askjeeves hade svårt att sortera skräp från relevanta hemsidor.

PageRanks ide

Viktiga sidor ses som de med många refereringar från andra sidor.

4.3.2 Practical use

Om jag surfar på måfå genom att klicka på länkar, hur stor är sannolikheten att jag hamnar på sida X?

När sannolikheten ökar anses sidan mer relevant enligt PageRank.

Chapter 5

Läsvecka 5

5.1 Mål med talteori

Första målet: Visa att varje positivt heltal kan skrivas som en produkt av primtal på ett unikt sätt.

5.2 Delbarhet

Låt $a, b \in \mathbb{Z}$
Vi säger att a delar b om det finns ett $m \in \mathbb{Z}$ så att $b = a \times m$.
(Informellt: a delar b om antingen $a = 0 = b$ eller $\frac{b}{a}$ är ett heltal).

Skriver $a|b$ om a delar b, och $a \nmid b$ om $a$inte delar b.

Delarhet är en relation på $\mathbb{Z}$.
Några egenskaper:

1. $a|0 \ \forall a \in \mathbb{Z}$
2. $a|a \ \forall a \in \mathbb{Z}$
3. $(a|b \wedge b|c) \Rightarrow a|c \ \forall a, b, c \in \mathbb{Z}$
4. $0 \nmid a$ om $a \neq 0$
5. Låt $a, b, c \in \mathbb{Z}$. Då gäller $(a|b \wedge b|c) \Leftrightarrow (a|xb + yc \forall x, y \in \mathbb{Z})$

5.2.1 Bevis av 5

$\Leftarrow$
Antag att $a|xb + yc$ oavsett vad x & y är $(x, y \in \mathbb{Z})$
Om $x = 1$ och $y = 0$, så får jag $a|1 \times b + 0 \times c = b$, dvs $a|b$

Om $x = 0$ och $y = 1$, så får jag $a|0 \times b + 1 \times c = c$, dvs $a|c$
Så $a|b \wedge a|c$

$\Rightarrow$
Antag att $a|b$ och $a|c$, så $\exists m, n \in \mathbb{Z}$ så att $b = a \times m$ och $c = a \times n$
Om $x, y \in \mathbb{Z}$ så är $xb + yc = xam + yan = a(xm + yn) \Rightarrow a|xb + yc$

5.2.2 Delbarhet är reflexiv, transitiv och nästan antisymmetrisk

Om $a|b$ och $b|a$, då är antingen $a = b$ eller $a = -b$

Bevis

Fall 1: $a = 0$ $a|b \Rightarrow b = 0 \Rightarrow a = b$
Fall 2: $a \neq 0$ $a|b$ betyder $\exists m \in \mathbb{Z} : b = am$
$b|a$ betyder $\exists n \in \mathbb{Z} : a = bn$
Så $a = bn = amn \Rightarrow 1 = mn \Rightarrow m = n = 1$ eller $m = n = -1$

5.2.3 Restdivision

"Divisionsalgoritmen"
Låt $a \in \mathbb{Z}, b \in \mathbb{Z}_+$. Då finns unika $q_1 r \in \mathbb{Z}$ så att:
$a = qb + r$, med $0 \leq r < b$

q kallas för kvoten, r kallas resten.
q är det största heltalet så att $a - qb \geq 0$
Och r är då $a - qb$

5.2.4 Gemensamma delare

Def. $a, b \in \mathbb{Z}$, inte bägge 0.
En gemensam delare till a och b är ett tal $d \in \mathbb{Z}$ så att $d|a$ och $d|b$.

Ex 2 gemensam delare till 16 och 24
1 gemensam delare till 7 och 13
1 gemensam delare till a och b, $\forall a, b \in \mathbb{Z}$
-7 gemensam delare till 28 och 49
5 inte gemensam delare till 15 och 24

En gemensam delare d till a och b uppfyller:
$d \leq |a|$, så det finns alltid en största gemensamma delare till a och b.

Skrivs sgd(a, b) och är alltid positiv.

Ex:
$a = 4, b = 6$
4 har positiva delare $1, 2, 4$
6 har positiva delare $1, 2, 3, 6$
De gemensamma delarna är $1, 2$ och den största av dessa är 2.
dvs. sgd$(4, 6) = 2$

Om sgd$(a, b) = 1$ säger vi att a och b är relativt prima

Sats

1. Om $a \in \mathbb{Z}_+$så är sgd$(a, 0) = a$
2. $\forall a, b, n \in \mathbb{Z}$ så är sgd$(a + nb, b) =$ sgd(a, b)

Varför?

1. $a|a$ och $a|0$ så a är en gemensam delare till a & 0. Om $d|a$ så är $d \leq a$, så a måste vara största gemensamma delaren till a och 0.
2. Visar att (a, b) och $(a + nb, b)$ har exakt samma gemensamma delare. Då måste också sgd$(a, b) =$ sgd$(a + nb, b)$
   Om $d|a$ och $d|b$, så måste också $d|a + nb$ enligt (sats 5.4 del 5)
   Om $d|a + nb$ och $d|b$, så måste också $d|(a + nb) - nb$, dvs $d|a$

5.2.5 Euklides algoritm

$a, b \in \mathbb{Z}_+$. $a \geq b$

Genom upprepad division med rest får vi ?

$$
\begin{aligned}
a &= bq_1 + r_1,\ 0 \leq r_1 < b \\
b &= r_1q_2 + r_2,\ 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3,\ 0 \leq r_3 < r_2 \\
&\vdots \qquad\qquad \vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, \\
r_{n-1} &= r_nq_n,
\end{aligned}
$$

Varför fungerar Euklides algoritm?

Enligt sats 5.14 är:
sgd$(a, b) =$ sgd$(a - q_1b, b) =$ sgd$(r_1, b) =$ sgd$(r_1, b - q_2r_1) =$ sgd$(r_1, r_2) = \cdots =$ sgd$(r_{n-1}, r_n) =$ sgd$(r_{n-1} - r_nq_{n+1}, r_n) =$ sgd$(0, r_n) = r_n$

5.3 Bezouts identitet

Låt $a, b \in \mathbb{Z}$. Då finns det $m, n \in \mathbb{Z}$ så att $ma + nb = \text{sgd}(a, b)$.
m, n inte unika.

Kan hitta m och n mha Euklides algoritm.
sgd$(876, 204)$

$876 = 204 \times 4 + 60$
$204 = 60 \times 3 + 24$
$60 = 24 \times 2 + 12$
$24 = 12 \times 2$

Vill hitta $m, n \in \mathbb{Z}$ så att $876m + 204n = 12$.
$12 = 60 - 24 \times 2 = 60 - (204 - 60 \times 3) \times 2 = 60 - 2 \times 204 + 60 \times 6 = 7 \times 60 - 2 \times 204 = 7 \times (876 - 204 \times 4) - 2 \times 204 = 7 \times 876 - 28 \times 204 - 2 \times 204 = 7 \times 876 - 30 \times 204$.
$m = 7, n = -30$.
dvs:

$$12 = 876m + 204n = 7 \times 876 + (-30) \times 204$$

5.4 Linjära diofantiska ekvationer

Ekvationer av typen $ax + by = c$ där $a, b, c \in \mathbb{Z}$ är givna och vi söker $x, y \in \mathbb{Z}$
Ekvationer där man söker heltalslösningar kallas diofantiska.

Ex Vi hittade en lösning till $876x + 204y = 12$
$(x = 7, y = -30)$
$2x + 4y = 1$
Har inga lösningar med $x, y \in \mathbb{Z}$
$2x + 4y$ är alltid ett jämt tal oavsett x och y, 1 är dock udda.

$ax + by = c$ har lösningar $x, y \in \mathbb{Z}$ om och endast om $\text{sgd}(a, b) | c$
I exempel 2 är sgd$(2, 4) = 2$ och $2 \nmid 1$

Varför det stämmer

Sätt $d = \text{sgd}(a, b)$
Oavsett vad x och y är så gäller att $d | ax + by$, eftersom $d | a$ och $d | b$
Så om $d \nmid c$ kan det inte finnas några lösningar.

5.4.1 Generell lösning

Hur man kan lösa $ax + by = c$ om $d|c$

1. Beräkna $d = \text{sgd}(a, b)$ med Euklides algoritm.
2. Kontrollera att $d|c$.
3. Dela ekvationen med d.
4. Hitta en lösning till $ax + by = d$, dvs $\frac{a}{d}x + \frac{b}{d}y = 1$.
5. Multiplicera x, y med c/d.
6. Hitta alla lösningar.
   Om $ax + by = c$, då är $ax + by = ax_0 + by_0 \Rightarrow ax - ax_0 = by_0 - by \Leftrightarrow a(x - x_0) = b(y_0 - y)$.
7. Dela med d: $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$.
   Så $\frac{a}{d}|\frac{b}{d}(y_0 - y)$
   Eftersom $\text{sgd}(\frac{a}{d}, \frac{b}{d}) = 1$, så måste (senare!) $\frac{a}{d}|(y_0 - y)$, dvs $y_0 - y = \frac{a}{d} \times n$.
   $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) = \frac{b}{d}\frac{a}{d} \times n \Rightarrow x - x_0 = \frac{b}{d} \times n$.
   Så $x = x_0 + \frac{b}{d} \times n$ och $y = y_0 - \frac{a}{d} \times n$.

Så det finns en lösning $x_n, y_n)$ för varje $n \in \mathbb{Z}$ som ges av $x_n = x_0 + \frac{b}{d} \times n$, $y_n = y_0 - \frac{a}{d} \times n$.

5.5 Primtal

Ett heltal $p \geq 2$ kallas för ett primtal om 1 och p själv är de enda positiva heltalen som delar p.

Sats

Antag att $a|bc$ och att $\text{sgd}(a, b) = 1$. Då måste $a|c$.

Bevis

Bezouts identitet ger att $1 = ma + nb$ för några $m, n \in \mathbb{Z}$.
Så $c = 1 \times c = (ma + nb)c = mac = nbc$
Eftersom $a|mac$ och $a|nbc$(Eftersom $a|bc$) så måste $a|mac + bnc = c$.s

Följdsats 1

Låt p vara ett primtal och antag att $p|ab$ för några $a, b \in \mathbb{Z}$.
Då måste $p|a$ eller $p|b$.

Om $p|a$, då är vi klara.
Om $p \nmid a$ då är $\text{sgd}(ab, p) = 1$ eftersom 1 och p är de enda positiva delarna till

p.
Då kan vi tillämpa den föregående satsen och få att $p|b$.

Följdsats 2

Om p är ett primtal och $p|a_1, a_2, \cdots, a_n$, så måste $p|a_i$ för något $i \in \{1, \cdots, n\}$

Induktionssteg

Om $p|a_1, \cdots, a_{n-1}, a_n$, så måste $p|a_1 \times a_{n-1}$ eller $p|a_n$ (Enligt följdsats 1). Om $p|a_n$ är i klara.
Om $p|a_1 \times a_{n-1}$ så finns ett $i \in \{1, \cdots, n-1\}$ så att $p|a_i$, eligt induktionsantagandet. Så oavsett finns ett $i \in \{1, \cdots, n\}$ så att $p|a_i$.

Chapter 6

Läsvecka 6

6.1 Aritmetikens fundamentalsats

Låt $m \geq 2$ vara ett heltal. Då kan m skrivas på ett unikt sätt som $m = p_1 \times \cdots \times p_r$, där $p_1, \cdots p_r$ är primtal och $p_1 \leq \cdots \leq p_r$

Ex: $36 = 2 \times 2 \times 3 \times 3$
$10 = 2 \times 5$
$17 = 17$

6.1.1 Bevis

Först visar vi att det finns en primtalsfaktorisering, med stark induktion:

Basfall:
$m = 2$, $2 = 2$ är ett primtal.
Induktionssteg:
Säg att varje tal $k < m$ har en primtalsfaktorisering.
Om m är ett primtal är vi klara ($m = m$ är en primtalsfaktorisering).

Om m är ett sammansatt tal, så är $m = ab$ med $1 < a, 1 < b$ heltal.
Då är $a, b < m$, så $a = p_1, \times \cdots \times p_s$, $b = p_{s+1} \times \cdots \times p_r$ är produkter av primtal, så $m = ab = p_1 \times \cdots \times p_s \times \cdots \times p_r$ är en produkt av primtal.

Nu visar vi att primtalsfaktoriseringen är unik:

Induktion!
Basfall:
$m = 2$ kan bara skrivas på ett sätt som en produkt av primtal.
Induktionssteg:
Antag att resultatet stämer för alla $k < m$.
Antag att $m = p_1 \times \cdots \times p_r = q_1 \times \cdots \times q_s$ är två primtalsfaktorisering av m.

Säg att $p_1 \leq q_1$. Då gäller $p_1 | q_1 \times \cdots \times q_s$
Enligt Följdsats 2 måste $p_1 | q_i$ för något $i \in \{1, \cdots, s\}$.
Men $q_i$är ett primtal, så $p_1 = q_i$.
Vi har också $p_1 \leq q_1 \leq \cdots \leq q_s$, så om $p_1 = q_i$ så måste $p_1 = q_1$.
Då är $p_2 \times \cdots \times p_r = \frac{m}{p_1} = \frac{m}{q_1} = q_2 \times \cdots \times q_s$ och är $< m$,
så enligt induktionsantagandet är $r = s$ och $p_i = q_i \ \forall i \in \{2, \cdots, r = s\}$

6.2 Kongruenser

Idag är det tisdag, vilken veckodag är det om:

1. 6 dagar? - måndag
2. 10 dagar? - fredag
3. 106 dagar? - onsdag

Hur kan räkna?
Cykler om 7 dagar

1. 6 dagar framåt = 1 dag bakåt $\rightsquigarrow$ måndag
2. $10 = 7 + 3$, 10 dagar framåt = 3 dagar framåt $\rightsquigarrow$ fredag
3. $106 = 7 \times 15 + 1$, så 106 dagar franåt = 1 dag framåt $\rightsquigarrow$ onsdag

Matematiskt kan man ställa upp det såhär:
måndag-söndag representerar vi med $1 - 7$.
$tisdag = 2$.
1) $2 + 6 = 8 = 7 + 1$, 1=måndag.
2) $2 + 10 = 12 = 7 + 5$, 5=fredag.
3) $2 + 106 = 108 = 7 \times 15 + 3$, 3=onsdag.

Kallas resträkning modulo 7, alternativt kondgruensräkning modulo 7.
7 är "cykel", kallas modulus.

I andra exempel har man ett annat modulus, t.ex. 12 alt. 24 för klockan.

Rent matematiskt kan vi välja vilket heltal $n \in \mathbb{Z}_+$ som helst som modulus.
Kan betrakta två heltal som "samma" om deras differens är en multipel av n.

6.2.1 Matematisk beskrivning

Definition

Låt $n \in \mathbb{Z}_+$.
Vi definierar en relation "$\equiv$ modulo n" på $\mathbb{Z}$ genom att säga att

$a \equiv b$ modulo n om $n|a-b$ (dvs $a-b$ är en multipel av n)
Utläses "4 är kongruent med b modulo n"
Skrivs oftast $a \equiv b \bmod n$ eller $a \equiv b, (n)$

Exempel

1. Om $n = 7$, så är $8 \equiv 1 \bmod 7$ eftersom $8 - 1 = 7$ är en multipel av 7
2. $108 \equiv 3 \bmod 7$, eftersom $108 - 3 = 105 = 7 \times 15$ är en multipel av 7
3. $11 \not\equiv 3 \bmod 7$, eftersom $11 - 3 = 8$ inte är en multipel av 7 $\star$

6.2.2 Sats

Kongruens mod n är en ekvivalensrelation

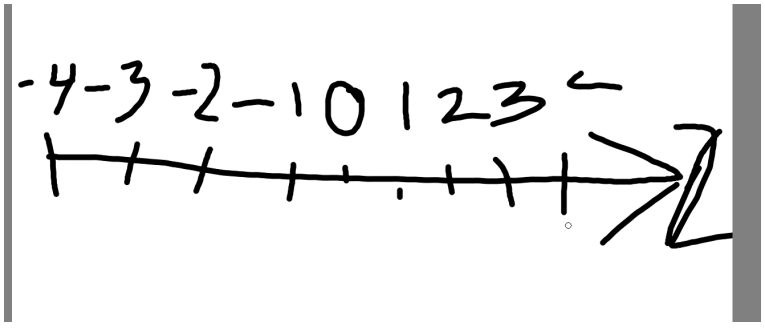
Bevis

Skall kontrollera att kongruens mod n är reflexiv, symmetrisk samtr transitiv.

- Reflexiv: $a \equiv a \bmod n$? ja, eftersom $a - a = 0$ och 0 delbart med n.
- Symmetrisk: Om $a \equiv b \bmod n$, så gäller $n|a-b$.
  Om $n|a-b$, så $n|(-1)(a-b) = b-a$, dvs. $b \equiv a \bmod n$.
- Transitiv: Antag att $a \equiv b \bmod n$ och $b \equiv c \bmod n$,
  dvs. $n|a-b$ och $n|b-c$. Då gäller $n|(a-b)+(b-c) = n|(a-c)$, dvs $a \equiv c \bmod n$.

6.2.3 Ekvivalensklasserna för kongruens mod n

Låt $a \in \mathbb{Z}$.
$[a] = \{b \in \mathbb{Z} | b \equiv a \bmod n\}$ är definitionen av ekvivalensklass.
Enligt divisionsalgoritmen finns en unik rest $r \in \mathbb{Z}$ $0 \leq r \leq n-1$ så att $a = n \times q + r$, dvs $a \equiv r \bmod n$.
$r \in [a]$ så $[a] = [r] = \{\cdots, r-2n, r-n, r, r+n, r+2n, \cdots\}$.



Ex. $n = 4$

6.3 Addition, subtraktion, multiplikation och division modulo n

Ekvivalensklasserna till relationen $\equiv$ mod n
Det finns n st olika kongruensklasser modulo n:
$[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n$
Ett tal $a \in \mathbb{Z}$ tillhör $[r]_n$, där r är resten vid division av a med n.
Dvs $a = q \times n + r, 0 \leq r < n$.

Def

$\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$, mängden av alla kongruensklasser modulo n.

6.3.1 Addition, subtraktion och multiplikation

$a, b, c, d \in \mathbb{Z}, n \in \mathbb{Z}_+$
Säg att $a \equiv c\ (n)$ och $b \equiv d\ (n)$.
Då är:

1. $a + b \equiv c + d\ (n)$
2. $a - b \equiv c - d\ (n)$
3. $a \times b \equiv c \times d\ (n)$

Exempel

6×9 mod 7?

- $6 \times 9 = 54 = 7 \times 7 + 5 \equiv 5\ (7)$
- $6 \times 9 \equiv (-1) \times 2 \equiv -2 \equiv 5\ (7)$

Varför är satsen sann?

1) Vill visa $a + b \equiv c + d\ (n)$, dvs $n|(a + b) - (c + d)$
Vi vet att $n|(a - c)$ och $n|(b - d)$
$(a + b) - (c + d) = a - c + b - d = (a - c) + (b - d)$, så $n|(a + b) - (c + d)$
2) och 3) görs på liknande sätt.

Exempel

Vilken veckodag är den 1 april 2022?
Idag: Onsdag 8 december 2021.
Dagar kvar mod 7:
$23 + 31 + 28 + 31 + 1 \equiv 2 + 3 + 0 + 3 + 1 = 9 \equiv 2\ (7)$
Det är en fredag. (Korrekt)

Definition

Vi definierar addition, subtraktion och multiplikation på $\mathbb{Z}_n$ genom

- $[a]_n + [b]_n = [a + b]_n$
- $[a]_n - [b]_n = [a - b]_n$
- $[a]_n \times [b]_n = [a \times b]_n$

Varför är den här definitionen OK?
Säg att $[a]_n = [c]_n$ och $[b]_n = [d]_n$, är då
$[a + b]_n = [c + d]_n$?
$[a - b]_n = [c - d]_n$?
$[a \times b]_n = [c \times d]_n$?
Ja! =)
$[a + b]_n = [c + d]_n \Leftrightarrow a + b \equiv c + d\ (n)$
$[a - b]_n = [c - d]_n \Leftrightarrow a - b \equiv c - d\ (n)$
$[a \times b]_n = [c \times d]_n \Leftrightarrow a \times b \equiv c \times d\ (n)$.

6.3.2 Division i $\mathbb{Z}_n$

Division i $\mathbb{Z}$ − normalt är $\frac{a}{b}$ inte ett heltal även om a och b är heltal.
Så det kommer inte fungera att göra på samma sätt som de andra räknesätten.
$\frac{[1]_3}{[2]_3} = [1/2]_3$, $[1/2]_3$ finns inte.

Vad är division?

$a, b \in \mathbb{Q}$ eller i $\mathbb{R}$.
$\frac{b}{a} = \frac{1}{a} \times b$ Division med a = Multiplikation med $\frac{1}{a}$
Vad är $\frac{1}{a}$? $\frac{1}{a}$ är ett tal x så $xa = 1$.
Med andra ord $\frac{1}{a}$ är lösningen (om den finns!) på $ax = 1$.
Om $a = 0$ har $ax = 1$ ingen lösning − går inte att dela med 0.

Givet $[a]_n\mathbb{Z}_n$, när kan vi lösa $[a]_n[x]_n = 1$?
Ex lös $[2]_3[x]_3 = [1]_3$, $[x]_3 = [2]_3$, $[2]_3 \times [2]_3 = [4]_3 = [1]_3$

Att lösa $[a]_n[x]_n = [1]_n$

Samma som $[ax - 1]_n = [0]_n$, dvs $n|(ax - 1)$, dvs $\exists y \in \mathbb{Z} : ax - 1 = ny$
$ax - 1 = ny \Leftrightarrow ax - ny = 1$, en linjär diofantisk ekvation!

$ax - ny = 1$ är lösbar enbart om $\text{sgd}(a, n)|1 \Leftrightarrow \text{sgd}(a, n) = 1$ och vi kan lösa den med hjälp av *Euklides algoritm*.
Vår formel för den allmänna lösningen till $ax - ny = 1$ ger att x är unik modulo n.

Definition

Låt $[a]_n \in \mathbb{Z}_n$.
Om $\text{sgd}(a, n) = 1$ så finns ett unikt $[x]_n \in \mathbb{Z}_n$ så att $[a]_n \times [x]_n = [1]_n$
$[x]_n$ kallas för inversen till $[a]_n$.

Ett heltal x med egenskapen $ax \equiv 1 \mod n$ kallas för en invers till a modulo n. Om a har en invers modulo n säger vi att a är inverterbar modulo n.

Exempel

4 är inverterbar mod 9, eftersom $\text{sgd}(4, 9) = 1$.
Hur hittar vi inversen till 4 mod 9? $\rightarrow$ Euklides algoritm!

$9 = 4 \times 2 + 1$
$4 = 1 \times 4$

Baklänges
$1 = 9 - 4 \times 2$
$1 \equiv 0 - 4 \times 2 \equiv (-2) \times 4 \ (9)$

Så $x = -2$ löser $4x \equiv 1 \ (9)$, dvs -2 är en invers till 4 mod 9.

OBS: $-2 \equiv 7$, så 7 också en invers till 4 mod 9, etc.

6.4 Linjära kongruensekvationer

Exempel

Lös $4x \equiv 3 \ (11)$
En lösning: Prova allt!
Mer systematiskt:
Vill multiplicera ekvationen med inversen till 4 (om existerande) mod 11, för att "få bort" 4an.
Får då $12x \equiv 9 \ (11)$
$12x \equiv x$ så $x \equiv 9 \ (11)$

6.5 Duggainfo

Är på fredag 08.00-08.45
Berör Kap 7 och kap 5 (t.om. primtal) exklusive kongruenser.

$$n = p_1^k \times p_2^k \times \cdots \times p_r^k$$
$$\phi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

6.6 Seminarium 3

6.6.1 Problem 1

Fråga

Hitta alla lösningar till ekvationen $8x + 2 \equiv 5 \mod 19$

Mitt svar

$x = [17]_n$

Christians svar

$8x + 2 \equiv 5$
$8x \equiv 5 - 2 = 3$
(Invertera 8)
$19 = 8 \times 2 + 3$
$8 = 2 \times 3 + 2$
$3 = 1 \times 2 + 1$
$2 = 2 \times 1$

$$1 = 3 - 2 = 3 - (8 - 2 \times 3) = 3 \times 3 - 8 = 3 \times (19 - 2 \times 8) - 8 = 3 \times 19 + (-7) \times 8$$

Invers till 8 mod 19:
(-7)

(Multiplicera ekvation med invers)
$(-7) \times 8x \equiv -21$
$x \equiv -21 \equiv 17$

6.6.2 Problem 2

Fråga

Hitta alla lösningar till ekvationen $6x \equiv 15 \mod 9$

Mitt svar

$$6x \equiv 15, (9)$$
$$6x \equiv 6, (9)$$
$$x = [1]_n, x = [4]_n, x = [7]_n$$
$$x = 1 + 3n$$

$x_k = 0, 1, 2, 3, 4, 5, 6, 7, 8$
$6x_k = 0, 6, 12, 18, 24, 30, 36, 42, 48$

Christians svar

$$6x \equiv 15 \equiv 6, (9)$$
$$6x \equiv 6, (9)$$

Kan inte bra dela med 6m $x \equiv 1$ (9) är en lösning men det är inte alla lösningar.
$6x \equiv 6$ (9) betyder att $9|6x - 6$, dvs $9y = 6x - 6$.
$6x - 9y = 6$, en linjär diofantisk ekvation.

$$6x - 9y = 6$$
$$2x - 3y = 2$$

Vi har två alternativ;
Alternativ 1:

- Lös $2x - 3y = 2$
- $x = y = (-2)$ ger en lösning.
- Alla lösningar ges av $(x_n, y_n) = (-2 + 3n, -2 + 2n)$
- $x \equiv (-2), (3)$, dvs $x \equiv 1, (3)$

Alternativ 2:

- $2x - 3y = 2 \Leftrightarrow 2x \equiv 2$ (3)
- 2 är inverterbar mod 3, 2 är sin egen invers.
- $2(2x) \equiv 2(2)$
- $x \equiv 4 \equiv 1$

Alternativ 3:

- $6x \equiv 6$ (9)
- Kan jag invertera 6 mod 9?

  Nej, för att $\text{sgd}(6, 9) = 3 \neq 1$
  Dela allt med 3, $\frac{6}{3}x \equiv \frac{6}{3}$ $(\frac{9}{3})$
  $2x \equiv 2$ (3) $\Rightarrow x \equiv 1$ (3)
- för $ax \equiv b$ (c) krävs $\text{sgd}(a, c)|b$ för en lösning.

6.6.3 Problem 3

Fråga

Hitta alla lösningar till ekvationerna:

(1) $x^2 \equiv 1 \bmod 8$

(2) $x^2 \equiv 3 \bmod 13$

(3) $x^2 - 6x + 6 \equiv 0 \bmod 13$, $x \in \mathbb{Z}$

Mitt svar

(1)
$$x = [1]_8, x = [3]_8, x = [5]_8, x = [7]_8$$

(2)
$$x = [4]_n, x = [9]_n$$

Christians svar

(1) Trial and error!

(2) Kan lösas isch som en andragradsekvation

$$x^2 \equiv 3, (13)$$
$$x^2 - 3 \equiv 0, (13)$$
$$x^2 - 16 \equiv 0, (13)$$
$$x^2 - 4^2 \equiv 0, (13)$$
$$(x + 4)(x - 4) \equiv 0, (13)$$

Eftersom 13 är ett primtal kan man resonera $(x+4)(x-4) \equiv 0 \Rightarrow x+4 = 0$, eller $x - 4 = 0$ (13)
$x \equiv -4$, $x \equiv 4$ (13)

(3) Hann inte med idag =/

6.7 Kinesiska restsatsen

6.7.1 Funny story?

En general har mellan 500 och 600 soldater,
Tidigare hade man delat in dem i grupper om 7 och då blev det 5 över.
Vid ett annat tillfälle hade man delat in dem i grupper om 15, och då blev det 3 över.

Så generalen funderar en liten stund och inser att de har 558 soldater.

x antalet soldater

(1) $x \equiv 5(7)$

(2) $x \equiv 3(15)$

Vad säger (1)?
$x \equiv 5, (7) \Leftrightarrow x = 7y + 5$ för något $y \in \mathbb{Z}$
Substituera $x = 7y + 5$ i (2):
$7y + 5 \equiv 3 \quad (15)$
$7y \equiv -2 \quad (15)$
Vill invertera 7 mod 15: $\quad 15 = 7 \times 2 + 1$
$7 = 1 \times 7$
$1 = 15 - 2 \times 7$ så $1 \equiv (-2) \times 7 \quad (15)$
$y \equiv 4 \quad (15)$ betyder $y = 15 + 4$, för något $z \in \mathbb{Z}$

Så $x = 7y + 5 = 7(15z + 4) + 5 = 105z + 28 + 5 = 105z + 33 \ \forall z \in \mathbb{Z}$
− Samtliga lösningar

6.7.2 What is it actually?

Låt $a, b \in \mathbb{Z}$ och $m, n \in \mathbb{Z}_+$ med $\text{sgd}(m, b) = 1$

$x \equiv 5 \quad (7)$
$x \equiv 3 \quad (15)$
Kan lösa ekvationssystemet.
Vad säger (1)
$x \equiv 5 \ (7) \Leftrightarrow x = 7y + 5$ för något $y \in \mathbb{Z}$
Om x_0 är en lösning så ges alla lösningar av $x_k = x_0 + mnk \qquad k \in \mathbb{Z}$

I exemplet ovan hade vi $m = 7, n = 15$ så $sgd(7, 15) = 1$ och $mn = 105$

6.7.3 Kinesiska restsatsen på fler än 2

Kan lösa system med fler ekvationer, så länge alla moduli är parvis relativt prima

1. $x \equiv 4, (10$
2. $x \equiv 5, (11)$
3. $x \equiv 2, (7)$

$sgd(10, 7) = sgd(10, 11) = sgd(7, 11) = 1$ Så skall gå att lösa.

(1) säger $x = 10y + 4$ för något $y \in \mathbb{Z}$

Substitution i (2) ger:
$x = 10y + 4 = 2, (7) \Leftrightarrow 3y + 4 = 2, (7) \Leftrightarrow 3y \equiv (-2), (7)$
Invertera 3 mod 7, (-2) är en invers.

Multiplicera med (-2)

$y \equiv (-2)3y \equiv (-2)(-2) \equiv 4 \quad (7)$ så $y = 7z + 4$ för något $z \in \mathbb{Z}$

Så $x = 10y + 4 = 10(7(z) + 4) + 4 = 70z + 44$

Substitution i (3):

$x \equiv 70z + 44 \equiv 5 \Leftrightarrow 4z + 0 \equiv 5 \quad (11)$

Får $4z \equiv 5 \quad (11)$

Invertera 4 mod 11, 3 är en invers. Multiplicera med 3.

$F \equiv 3 \times 4z \equiv 15 \equiv 4 \quad (11)$, så $z = 11k + 4$ för något $k \in \mathbb{Z}$

Så $x = 70z + 44 = 70(11k + 4) + 44 = 770k + 280 + 44 = 770k + 324 \quad k \in \mathbb{Z}$

Chapter 7

Läsvecka 7

7.1 Potenser mod n

$a^k \equiv ?$ (n)

7.2 Eulers ϕ-funktion

$n \in \mathbb{Z}_+$

$u(n) = \{[x]_n \in \mathbb{Z}_n | [x]_n \text{ är inverterbar}\} = \{[x]_n \in \mathbb{Z}_n | \text{sgd}(x, n) = 1\} \subseteq \mathbb{Z}_n$

7.2.1 Def

$\phi(n) = |u(n)$, dvs $\phi(n) =$ antalet tal i $\{1, \cdots, n\}$ som är relativt prima med n.

Ex

$\phi(1) = 1,$	$u(1) = \{[1]\}$	$\mathbb{Z}_1 = \{[1]\}$
$\phi(2) = 2,$	$u(2) = \{[1]_2\}$	$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$
$\phi(6) = 2,$	$u(6) = \{[1]_6, [5]_6\}$	$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6, \}$

7.3 Eulers sats

Om sgd$(a, n) = 1$, så är $a^{\phi(n)} \equiv 1$ (n).
För att vara användbar behöver vi kunna beräkna $\phi(n)$.

7.3.1 $\phi(n)$ för primtal

p primtal.
$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ $k \in \mathbb{Z}_+$

Varför?

Ska räkna antalet a mellan 1 och p^k som är relativt prima med p^k, dvs $\text{sgd}(a, p^k) = 1 \Leftrightarrow p \not| a$.
De a mellan 1 och p^k med $p|a$ är $p, 2p, 3p, \cdots, p^k = p^{k-1}p$, så de är $p^k - 1$ st.

Så antalet a med $p \not| a$ är $p^k - p^{k-1}$, så $\phi(p^k) = p^k - p^{k-1}$

Sats (5.54)

Om $\text{sgd}(m, n) = 1$, så är $\phi(mn) = \phi(m)\phi(n)$.
Varför?
$\phi(mn)$ = antalet a mellan 0 och $mn - 1$ som är relativt prima med mn.

Definiera en funktion

f:$\{0, 1, \cdots, mn-1\} \to \{0, 1, \cdots, m-1\} \times \{0, 1, \cdots, n-1\}$
Om $a \in \{0, 1, \cdots, mn-1\}$ så är $a = mq_1 + r_1$, $r \in \{0, 1, \cdots, m-1\}$
$a = nq_2 + r_2$, $r_2 \in \{0, 1, \cdots, n-1\}$

Vi sätter $f(a) = (r1, r2)$.

1) f är injektiv; Om $f(a) = f(b)$, så är $a \equiv b$ (m) och $a \equiv b(n) \Leftrightarrow a \equiv b(mn)$ enligt kinesiska restsatsen, så $a = b$ eftersom $a, b \in \{0, 1, \cdots, mn-1\}$

2) Säg att $f(a) = (r_1, r_2)$, Då är $\text{sgd}(a, mn) = 1 \Leftrightarrow \text{sgd}(r_1, m) = 1$ och $\text{sgd}(r_2, n) = 1$

Varför?
$\text{sgd}(a, mn) = 1 \Leftrightarrow \text{sgd}(a, m) = 1$ och $\text{sgd}(a, n) = 1 \Leftrightarrow \text{sgd}(r_1, m) = 1$ och $\text{sgd}(r_2, n) = 1$.
(Jämför med motiveringen till varför Euklides algoritm fungerar).

f ger en bijektion mellan $\{a | a \in \{0, 1, \cdots, mn-1\}, \text{sgd}(a, mn) = 1\}$ och $\{x | x \in \{0, 1, \cdots, m-1\}, \text{sgd}(x, m) = 1\}$ $x\{y | y \in \{0, 1, \cdots, n-1\}$, $\text{sgd}(y, n) = 1\}$
Så $\phi(mn) = \phi(m)\phi(n)$

Om $n = p_1^{e_1} \cdots p_r^{e_r}$, med p_i olika primtal och $e_i \geq 1$, så är $\phi(n) = \phi(p_1^{e_1} \cdots p_r^{e_r}) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r}) = (p_1^{e_1} p_r^{e_1 - 1}) \cdots (p_r^{e_r} - p_r^{e_{r-1}})$

7.4 Eulers sats - fortsättning

Om sgd$(a, n) = 1$ så är $a^{\phi(n)} \equiv 1$ (n)

7.4.1 Specialfall

p primtal.

1) Om $p \not| a$, så är $a^{p-1} \equiv 1$ (p).

2) $a^p \equiv a$ (p) för alla $a \in \mathbb{Z}$

7.4.2 Exempel

Vilken entalssiffra har $3^8 \times 77 + 2^{10} \times 121$?

Entalssiffra = rest vid division med 10.
$77 \equiv 7$ (10)
$121 \equiv 1$ (10)
3^8 $\phi(10) = \phi(2)\phi(5) = 1 \times 4 = 4$, så $3^8 = (3^4)^2 \equiv 1^2 \equiv 1$ (10)
2^{10} Kan inte använda Elers sats då sgd$(2, 10) = 2 \not\equiv 1$
$2^3 = 8 \equiv (-2)$ (10) så $2^{10} = 2^{3\times3+1} = (2^3)^3 \times 2 = -(-2) \times 2 \equiv 4$ (10)

$3^8 \times 77 + 2\ 10 \times 121 \equiv 1 \times 7 + 4 \times 1 \equiv 11 \equiv 1$ (10)

7.5 Public Key Cryptography

7.5.1 Symmetrisk kryptering

Inte saker som pgp och gpg

1) Metod (Substitutionsschiffer)

2) Parameter (Hur många steg framåt/bakåt i alfabetet vi rör oss)

7.5.2 Assymetrisk kryptering, Historisk kuriosa

På 70-talet kom assymetriska krypteringssystem som bygger på modulär aritmetik.
Kom två extra populära:

- Diffie-Hellman
- RSA (Rivest-Shamir-Adleman) (1977)

7.5.3 RSA

Alice vill kunna ta emot krypterade meddelanden:

1) Alice väljer två primtal p och q
och beräknar $N = pq$ och $\phi(N) = (p-1)(q-1)$

2) Alice väljer ett $a \in \{1, \cdots, N-1\}$ med $\text{sgd}(a, \phi(n)) = 1$
och beräknar ett b så att $ab \equiv 1 \bmod \phi(N)$

3) Alice skickar (N,a) (Public key) till de hon vill kommunicera med och behåller p, q, b och $\phi(N)$ hemliga.
Bob vill skicka ett krypterat meddelande till Alice.
$\rightsquigarrow$ gör om det till (flera) tal x.

4) Bob beräknar $y \equiv x^9 \bmod$ N och skickar y till Alice
y är det krypterade meddelandet.

5) Alice beräknar x genom $y^b \equiv x^{9b} \equiv x^{1+k\phi(N)} \equiv x \times (x^{\phi(N)})^k \equiv x \times 1^k \equiv x$ mod N

Varför fungerar det här?

Om jag vet N så kan jag primtalsfaktorisera N, beräkna $\phi(N)$ och beräkna b. dessa beräkningar är dock ganska tidskrävande.

För att knäcka RSA (dvs beräkna x utifrån y, N och a) så behöver jag i princip faktorisera $N = pq$. Om p och q är tillräckligt stora tar detta för lång tid för att vara värt det.

Ex Talet RSA-250 har 250 siffror (829 siffror binärt) faktoriserades 2020, tog motsvarande 2700 core years med en 2.1GHz-processor.

N rekommenderas ha $\geq$ 2048 siffror binärt för att klassas som säkert.

I praktiken använder man hybridsystem med både symmetrisk och assymetrisk kryptering.

Chapter 8

Begreppslista

8.1 Logik

8.1.1 Logiska operatorer

Sanningstabell				
p	q	$p \wedge q$	$p \vee q$	$\neg p$
F	F	F	F	S
F	S	F	S	S
S	F	F	S	F
S	S	S	S	F

p	q	$p \leftrightarrow q$	$p \rightarrow q$
F	F	S	S
F	S	F	S
S	F	F	F
S	S	S	S

- Konjunktion $P \wedge Q$ "P och Q"

  $P \wedge Q$ är sann enbart om både P och Q är sanna

- Disjunktion $P \vee Q$ "P eller Q"

  $P \vee Q$ är sann enbart om P och/eller Q är sann

- Negation $\neg P$ "Inte P" "Icke P"

  $\neg P$ är sann enbart om P är falsk

- Implikation $P \rightarrow Q$ "P implicerar Q" eller "P medför Q" eller "Om P så Q"

  Kan också tolkas som $\neg P \vee Q$

  Ex. Om det är en björn så kan den simma; dvs. Antingen är det inte en björn, eller så kan den simma.

- Ekvivalens $P \leftrightarrow Q$ "P är ekvivalent med Q"

  P om och endast om Q

- Tautologier

  En sammansatt utsaga beroende på ett antal ingående utsagor som alltid är sann, oavsett sanningsvärdena på ingångsutsagorna, ex. $P \vee \neg P$

8.1.2 Logiska relationer

- P implicerar Q logiskt om $P \to Q$ är sann; dvs $P \Rightarrow Q$
- P är logiskt ekvivalent med Q om $P \leftrightarrow Q$ är sann; dvs. $P \Leftrightarrow Q$

  P och Q har samma sanningsvärde

8.1.3 Logiska argument

Består av tre huvudkomponenter

- Hypoteser $H^1, H^2, \cdots, H^n$ (Utsagor)
- Slutsats C, Utsaga
- $H^1, H^2, \cdots, H^n \to C$ är en tautologi när vi expanderar H-utsagorna till mer primitiva utsagor.

8.2 Mängder

Mängd: En väldefinierad samling av objekt där inget objekt kan existera mer än en gång.

8.2.1 Fördefinierade mängder

- $\mathbb{Z}$: Alla heltal
- $\mathbb{N}$: Alla naturliga tal.
- $\mathbb{Z}_+$: Positiva heltal
- $\mathbb{Q}$: Rationella tal
- $\mathbb{R}$: Reella tal
- $\mathbb{C}$: Komplexa tal
- $\emptyset$: Tom mängd

8.2.2 Tillhörande

$x \in M$ x tillhör M
$x \notin M$ tillhör ej M

8.2.3 Kvantifiering

- $\forall$ Universell kvantifierare

  $\forall x \in \mathbb{Z} : x \lesseqgtr 0$ För alla heltal x är x större, mindre eller lika med 0

- $\exists$ Existensiell kvantifiering

  $\exists x \in \mathbb{Z} : x = 0$ Existerar minst ett heltal x med värde 0

8.2.4 Mängdrelationer

- $M = N$ enbart om $x \in M \Leftrightarrow x \in N$
- $M \subseteq N$ enbart om $x \in M \rightarrow x \in N$

8.2.5 Mängdoperationer

- Union $M \cup N = \{x | x \in M \vee x \in N\}$
- Snitt $M \cap N = \{x | x \in M^x \in N\}$
- Komplement $M^c = \{x | x \notin M\}$

- Mängddifferens $M \backslash N$ = Där x finns i M men ej i N
- Kartesisk produkt $a \times B = \{(a, b) | a \in A \text{ och } b \in B\}$

8.2.6 Räkneregler inom mängdläran

Identitet

$A \cap U = A$
$A \cup \emptyset = A$

Dominans

$A \cup U = U$
$A \cap \emptyset = \emptyset$

Namnlös

$A \cup A^c = U$
$A \cap A^c = \emptyset$

Idempotens

$A \cup A = A$
$A \cap A = A$

Dubbelt komplement

$(A^c)^c = A$

Kommutativitet

$A \cup B = B \cup A$
$A \cap B = B \cap A$

Associativitet

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

Distributivitet

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

deMorgan

$(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$

Namnlös

$A \backslash B = A \cap B^c$

8.3 Funktioner

Skrivs $f : A \to B$
A kallas f's definitionsmängd.
B kallas f's målmängd.
$f(A) = \{b \in B | \exists a \in A : f(a) = b\} \subseteq B$ kallas för f's värdemängd.

$f : A \to B$ tillderar ETT element $f(a) \in B$ $\forall a \in A$

8.3.1 Egenskaper hos funktioner

- f injektiv om $\forall x, y \in A : x \neq y \to f(x) \neq f(y)$
- f surjektiv om $f(A) = B$
- f bijektiv om både injektiv och surjektiv.

8.3.2 Operationer på funktioner

- Invers: Om $f : A \to B$ bijektiv kan definiera $f^{-1} : B \to A$ genom att bryta ut x
- Sammansatta funktioner: $f : A \to B$, $g : B \to C \Rightarrow g \circ f : A \to C$, $g \circ f(x) = g(f(x))$
- $f : A \to B$, $f^{-1} : B \to A \Rightarrow f \circ f^{-1} = id_B$, $f^{-1} \circ f = id_A$
- $f^{-1} \neq \frac{1}{f(x)}$

8.4 Summor och produkter

$a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{n} a_i$
$a_1 \times a_2 \times \cdots \times a_n = \prod_{i=1}^{n} a_i$

8.5 Relationer

A, B två mängder. Relation R från A till B delmängd $R \subseteq A \times B$

- $(x, y) \in R$ "x relaterat till y"
- $(x, y) \notin R$ "x inte relaterat till y"
- Skrivs oftast xRy istället för $(x, y) \in R$

8.5.1 Egenskaper hos relationer

R relation på mängd A
R är:

- Reflexiv; $xRx\ \forall x \in A$
- Symmetrisk; $xRy \Rightarrow yRx\ \forall x, y \in A$
- Antisymmetrisk; $(xRy \wedge yRx) \Rightarrow x = y\ \forall x, y \in A$
- Transitiv; $(xRy \wedge yRZ) \Rightarrow xRz\ \forall x, y, z \in A$
- Partiell ordning; Om R reflexiv, antisymmetrisk och transitiv.
- Ekvivalensrelation; Om R reflexiv, symmetrisk och transitiv.

8.5.2 Kommutativitet och associativitet

Kommutativitet: Relation R är kommutativ om $\forall x, y \in U : xRy = yRx$
Associativitet: Relation R associativ om $\forall x, y, z \in U : xR(yRz) = (xRy)Rz$
Identitet: element identitet för relation R om $aRe = eRa = a$, $\forall a \in A$

8.6 Talföljder

8.6.1 Aritmetisk talföljd

En talföljd kallas aritmetisk om $a_2 - a_1 = a_3 - a_2 = \cdots = a_n - a_{n-1}$
För en aritmetisk talföljd a gäller $\sum_{i=1}^{n} a_i = n \times \frac{a_1 + a_n}{2}$

8.6.2 Geometrisk talföljd

En talföljd kallas geometrisk om $\frac{a_2}{a_1} = \frac{a_3}{a_2} = \cdots = \frac{a_n}{a_{n-1}}$

$c = \frac{a_n}{a_{n-1}}$

För en geometrisk talföljd a gäller $\sum_{i=1}^{n} a_i = a_1 \times \frac{c^n - 1}{c - 1}$

8.7 Rekursion

$f : \mathbb{Z}_+ \to \mathbb{R}$ är rekursivt definierad om $\exists a \in \mathbb{Z}_+$ och en funktion $h : \mathbb{R}^{a+1} \to \mathbb{R}$ så att:

1. $f(1), \cdots, f(a)$ är givna
2. $f(n) = h(f(n-a), f(n-a-1), \cdots, f(n-1), n) : \forall n \geq a+1$

8.8 Bevistekniker

8.8.1 Induktion

Låt $P_1, P_2, \cdots, P_n$ vara utsagor.
Om:

1. P_1 är sann kallas basfallet.
2. $P_n \Rightarrow P_{n+1}$ $\forall n \in \mathbb{Z}_+$ kallas induktionssteget
3. Så är P_n sann $\forall n \in \mathbb{Z}_+$

8.8.2 Kontrapositivt påstående

$(P \to Q) \Leftrightarrow (\neg Q \to \neg P)$

8.8.3 Motsägelsebevis

$(\neg P \to Q \wedge \neg Q) \Rightarrow P$

8.9 Kombinatorik

8.9.1 Multiplikationsprincipen

Göra k st oberoende val, varje val kan göras på $n_1, n_2, \cdots, n_k$ sätt.
k val kan då göras på $\prod_{i=1}^{k} n_i$ sätt.

8.9.2 Permutationer

Permutationen $x_1, \cdots, x_n$ kan göras på $\prod_{i=1}^{r}(n-i+1) = \frac{n!}{(n-r)!}$

8.9.3 Fakultetsfunktionen

$n! = 1 \times 2 \times \cdots \times n = \prod_{i=1}^{n} i, n \in \mathbb{Z}_+$

8.9.4 Kombinationer

$Kombinationer = \frac{Permutationer}{r!} = \frac{n!}{r!(n-r)!} = \binom{n}{r}$

Man kan fördela n lika objekt i k olika lådor på $\binom{n+k-1}{k-1}$ sätt.
$\binom{n+k-1}{k-1} = \binom{n}{k} + \binom{n}{k-1}$

8.9.5 Binomialsatsen

$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

8.9.6 Lådprincipen

Om $n+1$ objekt placeras i n lådor existerar minst en låda med fler än 1 objekt.

8.10 Grafer

8.10.1 Formalia

En graf består av en mängd V(noder/vertices) och $E \subseteq \{x, y| \subseteq x \neq y\}$(kanter/edges)
Högst en kant per nodpar.

8.10.2 Delgrafer

$G = (V, E), G' = (V', E')$
G' delgraf till G om $V' \subseteq V$ och $E' \subseteq E$

8.10.3 Fullständig delgraf

En graf kallas fullständig om det finns kanter mellan alla par av noder.

8.10.4 Bipartitet

En graf kallas bipartit om det finns en partition $V = A \cup B,\ A, B \neq \not{G}$ så att varje kant i G går mellan en nod i A och en i B.

8.10.5 Fullständigt bipartit delgraf

En graf kallas fullständigt bipartit om $\forall x \in A$, $\forall y \in B$ gäller att $\{x, y\} \in E$, dvs det finns en kant mellan x och y.

8.10.6 Riktade grafer

Tre huvudskillnader mot icke-riktade grafer:

- Öglor är tillåtna (kant till och från samma nod)
- Får gå två kanter mellan samma nodpar (Om kanterna riktade åt olika håll)
- Kanten $a \to b$ är skild från $b \to a$

Riktad väg

$v_0, v_1, \cdots, v_n \in V$ så att $(v_0, v_1), (v_1, v_2), \cdots, (v_{n-1}, v_n) \in E$

Riktad cykel

Riktad väg $v_0, v_1, \cdots, v_n$ med $v_0 = v_n$ utan upprepade kanter.

Starkt sammanhängande

G starkt sammanhängande om för varje nodpar $(x, y) \in V, x \neq y$ finns riktad väg $x \to y$

Sammanhängande

G sammanhängande om underliggande graf är sammanhängande.

8.10.7 Konvertera riktad till sin underliggande graf

1. Konvertera kanter $a \to b$ till $a \leftrightarrow b$
2. Eliminera otillåtna kanter (dubletter, öglor)

8.10.8 Träd

Graf G träd om sammanhängande och fri från cykler.

8.10.9 Skog

Graf G skog om icke-sammanhängande men fri från cykler.

8.10.10 Gradtal

Gratalet d_x för noden x är antalet kanter från noden x

8.10.11 Eulervägar

En väg i G innehållande samtliga kanter exakt en gång.
Om det existerar noder x, y där $(d_x, d_y) \bmod 2 = (0, 0)$ medan resterande gradtal är jämna existerar Eulerväg mellan x och y

8.10.12 Eulercykel

En Eulerväg med samma start- och slutnod.

8.10.13 Grafbenämning

P

P_n En väg med n noder.

C

C_n en cykel med n noder.

K

K_n en fullständig graf med n noder.
$K_{n,m}$ en fullständig bipartit graf med n noder i ena biparten och m noder i andra.

8.11 Matriser

8.11.1 Formalia

Em matris med m rader (vertikalt) och n kolumner (horisontellt) kallas en $m \times n$-matris.

8.11.2 Addition och subtraktion

A och B två matriser av (samma storlek)

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

Addition

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

Subtraktion

$$A - B = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} & \cdots & a_{1n} - b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} - b_{m1} & a_{m2} - b_{m2} & \cdots & a_{mn} - b_{mn} \end{pmatrix}$$

8.11.3 Skalärprodukt

Radvektor

$$a = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Kolumnvektor

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Skalärprodukt

Då a radvektor och b kolumnvektor:

$$a \bullet b = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n = \sum_{i=1}^{n} a_i b_i$$

8.12 Delbarhet

8.12.1 Egenskaper

1. $a|0\ \forall a \in \mathbb{Z}$
2. $a|a\ \forall a \in \mathbb{Z}$
3. $(a|b \wedge b|c) \Rightarrow a|c\ \forall \mathbb{Z}$
4. $0 \not| a$ om $a \neq 0$
5. Låt $a, b, c \in \mathbb{Z}$. Då gäller $(a|b \wedge b|c) \Leftrightarrow (a|xb + yc,\ \forall x, y \in \mathbb{Z})$

Om $a|b$ och $b|a$ gäller antingen $a = b$ eller $a = (-b)$

8.12.2 Restdivision

Låt $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+$. Då existerar unika $q_1 r \in \mathbb{Z}$ så:
$a = qb + r$, $0 \leq r < b$

8.12.3 Gemensamma delare

Låt $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+$.
Gemensam delare till a och b ett tal $d \in \mathbb{Z}$ så $d|a$ och $d|b$.

8.12.4 Största gemensamma delare

Betecknas $d = \text{sgd}(a, b)$
Om $\text{sgd}(a, b) = 1$ är a och b relativt prima.

Sats

Om $a \in \mathbb{Z}_+$ så är $\text{sgd}(a, 0) = a$
$\forall a, b, n \in \mathbb{Z}$ är $\text{sgd}(a + nb, b) = \text{sgd}(a, b)$

8.12.5 Euklides algoritm

$a, b \in \mathbb{Z}_+$. $a \geq b$

Genom upprepad division med rest får vi ?

$$
\begin{aligned}
a &= bq_1 + r_1,\ 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2,\ 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3,\ 0 \leq r_3 < r_2 \\
&\vdots \qquad\qquad \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \\
r_{n-1} &= r_n q_n,
\end{aligned}
$$

8.13 Bezouts identitet

$\forall a, b \in \mathbb{Z}$, $\exists m, n \in \mathbb{Z}$ så $ma + nb = \text{sgd}(a, b)$.
Kan hitta m och n genom att köra Euklides algoritm baklänges.

8.14 Linjära diofantiska ekvationer

8.14.1 Formalia

Ekvationer av typen $ax + by = c$ där $a, b, c \in \mathbb{Z}$ är givna och vi söker $x, y \in \mathbb{Z}$
Ekvationen enbart lösbar om $d|c$ där $d = \text{sgd}(a, b)$

8.14.2 Generell lösning

1. Beräkna $d = \text{sgd}(a, b)$
2. Kontrollera att $d|c$
3. Hitta en lösning till $ax + by = d$, dvs $\frac{a}{d}x + \frac{b}{d}y = 1$
4. Multiplicera x, y med $\frac{c}{d}$
5. Hitta samtliga lösningar: Om $ax + by = c$, då är $ax + by = ax_0 + by_0 \Rightarrow ax - ax_0 = by_0 - by \Leftrightarrow a(x - x_0) = b(y_0 - y)$.
6. $x_n = x_0 + \frac{b}{d}n$, $y_n = y_0 - \frac{a}{d}n$