Contents

1 Aritmetisk talföljd

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

Ex:

1,2,3...,100 Skillnaden är 1

3,7,11,15,19,... Skillnaden är 4

Om $a_1, a_2, ..., a_n$ är en aritmetisk talföljd så kallas $a_1, a_2, ..., a_n = \sum_{i=1}^{n} ai$ för en aritmetisk summa. För en aritmetisk summa gäller $\sum_{i=1}^{n} ai = n \cdot \frac{a_1 \cdot a_n}{2}$ där n är antalet termer.

En talföljd $a_1, a_2, ..., a_n$ 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 är 2

$4, 12, 36, 108$ Kvoten är 3

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

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

Varför?

$a_1, a_2 = a_1 c, a_3 = a_1 c^2, ..., a_n = a_1 c^{n-1}$ så $(c-1) \sum_{i=1}^{n} ai = (c-1)(a_1 + a_1 c + a_1 c^2 + ... + a_1 c^{n-1}) = a_1 (c-1)(1 + c + c^2 + ... + c^{n-1}) = a_1 (-1 + c - c + c^2 - c^2 + ... - ... - c^{n-1} + c^n) = a_1 (c^n - 1)$

2 Induktion och Rekursion

- Rekursion är en definitionsteknik där man definierar en funktiontalföljdetc "steg för steg"
- Induktion är en bevisteknik där man bevisar en följd $P_1, P_2, ...$ av utsagor steg för steg

OBS! En oändlig taföljd $a_1, a_2, ...$ är samma sak som en funktion $f : \mathbb{Z}_+ \to \mathbb{R}$
"Def" (4.7 i boken)
$f : \mathbb{Z}_+ \to \mathbb{R}$ är en 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 $f(1), ..., f(n-1)$. ("rekursion") (Dålig förklaring...)

INTE BRA!!! 2) är inte tillräckligt precis
Problement i 2):

- Kan jag använda olika funktioner för olika n?
- Ser nästan ut så eftersom aantalet argument växer
- Vilken typ av funktion får det vara?

Def
$f : \mathbb{Z}_+ \to \mathbb{R}$ är rekursivt definierad om $\exists a \in \mathbb{Z}_+$ och en funkiton $h\mathbb{R}^{a+1} \to$ 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)=xy
Om $f(1) = 1$ så är $f(n) = h(f(n-1), n) = n \cdot f(n-1), n \geq 2$
Så $f(2) = f(1) \cdot 2 = 2, f(3) = f(2) \cdot 3 = 6,$
$f(4) = f(3) \cdot 4 = 24, ... f(n) = n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$

Ex
a=2 : Fibonacci-talföljden
$f(1) = 1, f(2) = 1; \quad f(n) = f(n-1) + f(n-2), n \geq 3$
Alltså blir det 1,1,2,3,5,8,13,...

2.1 Induktion

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

1. P_1 är sann, och —— kallas basfallet

2. $P_n \Rightarrow P_{n+1} \forall n \in \mathbb{Z}_+$ —— kallas induktionsteget

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

Tänk $P_1 \rightsquigarrow P_2 \rightsquigarrow P_3 \rightsquigarrow P_4$ ...
Ex
Geometrisk summa, $c \neq 1$
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,...

2.2 Induktionssteg

Vill visa $P_n \Rightarrow P_{n+1}$, n godtyckligt
Dvs, om P_n sann, så är P_{n+1} sann Antag P_n sann, dvs $1 + ... + c^{n-1} = \frac{c^n - 1}{c-1}$ —— induktionsantagande
Vill visa P_{n+1} sann, dvs $1 + ... + c^{n-1} + c^{\lceil n \rceil} = \frac{c^{n+1} - 1}{c-1}$
$1 + c + ... + c^{n-1} + c^n = \frac{c^n - 1}{c-1} + \frac{(c-1)c^n}{c-1} = \frac{c^n - 1 + c^{n+1} - c^n}{c-1} = \frac{c^{n+1} - 1}{c-1}$
vilket är vad vi ville visa. Avslutar vi med induktionsteget. Enligt induktionsprincipen är P_n sann $\forall n \in \mathbb{Z}_+$

2.3 Varianter

P_1, P_2, P_3, utsagor
Stark induktion
om

1. P_1 sann

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

3. så är P_n sann för alla $n \in \mathbb{Z}_+$

Starake induktionsantagande. Antar $P_1 \wedge ... \wedge P_n$, inte bara P_n
Variant 2: Fler basfall
Om

1. $P_1, ..., P_m$ är sanna

2. $P_1 \wedge ... \wedge P$ SKRIVA AV SAXEN HÄR

$P_1, P_2, ...$ Stark induktion med flera basfall
Om

1. $P_1, ..., P_m$ är sanna för något m, och

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
$a_0 = 0, a_1 = 1$
$a_n = 5 \cdot a_{n-1} - 6 \cdot a_{n-2}$ för $n \geq 2$
$a_0 = 0, a_1 = 1, a_2 = 5 \cdot 1 - 6 \cdot 0 = 5, a_3 = 5 \cdot 5 - 6 \cdot 1 = 19, ...$
Visa att $a_n = 3^n - 2^n =: f(n)$ för alla $n \geq 0$
(Stark) induktion:

Basfall: $a_0 = 0, f(0) = 3^0 - 2^0 = 0$ ok!
$a_1, f(1) = 3^1 - 2\ ^1 = 1$ ok!
Induktionssteag: Antag att $n \geq 2$ och att $a_k = f(k) \forall k \leq n$.
Vi vill visa att $a_n = f(n)$.
$a_n ?5an - 1 - 6a_{n-2} = 5f(n-1) - 6f(n-2) = 5(3^{3-1} - 2^{n-1}) - 6(3^{n-2} - 2^{n-2}) = 5 \cdot 3\ ^{n-1} - 5 \cdot 2^{n-1} - 6 \cdot 3^{n-2} + 6 \cdot 2^{n-2} = 5 \cdot 3^{n-1} - 6 \cdot 3^{n-2} - 5 \cdot 2^{n-1} + 6 \cdot 2n - 2 = 3^{n-2}(15-6) - 2^{n-2}(10-6) = 3^n - 2^n = f(n)$
Enligt induktionsprincipen är $a_n = 3^n - 2^n \forall n \in N$

2.4 Andra bevistekniker

Kontrapositivt påstående: $(P \to Q) \Leftrightarrow (\neg Q \to \neg P)$
Ex
Vill visa (n^2 jämn $\to$ n jämn), n heltal
Bättre att visa (n udda $\to$ n^2 udda) $n = 2m + 1 \Rightarrow n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$ vilket är udda
Motsägelsebevis $(\neg P \to Q \wedge \neg Q) \Rightarrow P$
"Om antagande att P är falsk leder till en motsägelse, så måste P vara sann".

3 Kombinatorik

Hur många sätt kan man göra saker på?

3.1 Multiplikationsprincipen

Antag att vi ska göra k stycken oberoende val och att valen individuellt kan göras på $n_1, n_2, ..., n_k$ sätt. Då är antalet sätt de k valen kan göras på $n_1 n_2 ... n_k = \prod_{i=1}^{k} n_i$
Ex
INFOGA BILD
På hur många sätt kan jag gå från A till D (utan att gå från höger till vänster)?
Från A till B: 3 val (3 broar)
Från B till C: 2 val (2 broar)
Från C till D: 4 val (4 broar)

Valen är oberoende, så enligt multiplikationsprincipen finns det $3 \cdot 2 \cdot 4 = 24$ sätt att gå från A till D.

3.2 Permutationer

Notation 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 ($0 \leq r \leq n$) är en uppräkning $x_1, x_2, ..., x_r$ av r olika element 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	Andra talet
1	2,3
2	1,3
3	1,2

6st 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 $n(n-1)(n-2)...(n-r+1) = \prod_{i=1}^{r}(n-r+1)$ olika sätt.
Fakultetsfunktionen: $n! = 1 \cdot 2 \cdot ... \cdot n = \prod_{i=1}^{r} i, n \in \mathbb{Z}_+$

O!=1 **Ex** $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Om r=n, kan tänka på det som antalet sätt att ordna n element.

3.3 Kombinationer

En kombination av r element ur en mängd A är ett val av r olika 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?

Första talet	Andra talet
1	2,3
2	1,3
3	1,2

Vi får (1,2), (1,3), (2,1), (2,3), (3,1), (3,2). Varje kombination dyker upp två gånger som en permutation i det här fallet. Alltså är antalet kombinationer 3, då antalet permutationer var 6 och vi får delmängderna $\{1, 2\}, \{1, 3\}, \{2, 3\}$.

Varför blev det just 2 i detta fallet? 2=2!, antalet sätt man kan ordna 2 element!
Allmänt: Hur många kombinationer av r element ur A finns det om $|A| = n$?
$Antaletkombinationer = \frac{Antaletpermutationer}{antaletvisattordnarelement} = \frac{n(n-1)...(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}$
Om r=n, kan tänka på det som antalet sätt att ordna n element.
Uttrycket $\frac{n!}{r!(n-r)!}$ skrivs $\binom{n}{r}$, utläses "n över r", eller "n välj r".
Kallas för binomialkoefficienter.

Ex

$\binom{7}{4} = \frac{7!}{4!3!} = \frac{5040}{24 \cdot 6} = 35$
$\binom{7}{4} = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} = 35$ "välja 4 element av 7"
$\binom{7}{3} = 35$ "ta bort 3 element ur 7"

4 Kombinatorisk problemlösning

På hur många sätt kan man fördela 7 st likadana bollar i fyra lådor?
Infoga bild 1
Om bollarna hade varit olika hade man kunnat använda multiplikationsprincipen, vilket ger 4^7 möjligheter.
Infoga bild 2
En uppdelning är en sekvens, med 7 bollar och 3 "väggar". På hur många olika sätt kan jag skapa en sådan sekvens? Har totalt 10 symboler (7 bollar + 3 väggar) varav 3 är väggar.
Kan göras på $\binom{10}{3}$ sätt, och $\binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 10 \cdot 3 \cdot 4 = 120$
Slutsats: Man kan fördela n lika objekt i k lådor på $\binom{n+k-1}{k-1}$ sätt.
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?

Lösning

1. Samma som innan, kan göras på $\binom{8+3-1}{3-1} = \binom{10}{2} = \frac{10 \cdot 9}{1 \cdot 2} = 45$ sätt
2. Först ger vi alla varsitt äpple. Vi har då 5 st äpplen kvar, som skall fördelas på tre barn. Samma som innan, kan göras på $\binom{5+3-1}{3-1} = \binom{7}{2} = 21$
3. Vi vänder på problemet På hur många sätt kan äpplena fördelas om äldsta barnet skall få minst 5 äpplen?
   Ge 5 äpplen till ädlsta barnet, och sen delar vi ut resterande 3 äpplena, kan göras på $\binom{3+3-1}{3-1} = \binom{5}{2} = \frac{5 \cdot 4}{1 \cdot 2} = 10$

(Antalet sätt där äldsta får ≤ 4)=(Antalet sätt utan restriktioner)-(antalet där äldsta får ≥ 5)=45-10=35 sätt

4.1 Räkna saker på två sätt

Sats (6.13 i boken) $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$
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 kan väljas från {1,2,...,n}, kan göras på $\binom{n}{k}$ sätt.
  Om n+1 är med: Resterande k-1 tal skall väljas från {1,2,...,n}, kan göras på $\binom{n}{k-1}$ sätt.
  Så totalt kan k tal 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 avändas för att visualisera binomialkoefficienterna i Pascals triangel.
  Infoga bild 3
  Tal nr k i rad nr n är $\binom{n}{k}$.

Binomialsatsen (6.14 i boken) $(x+y)^n = \sum_{k=0}^{h}\binom{n}{k}x^k \cdot y^{n-k}$
$(x+y)^2 = x^2 + 2xy + y^2, (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$
Lådprincipen (pigeonhole principle) Om n+1 objekt placeras i n lådor så måste det finnas minst en låda med minst två objekt i.
Ex 25 elever går i en skolkass. Visa att minst tre st är födda samma månad.
Lösning: Finns 25 elever och 12 månader
$2 \cdot 12 = 24$ vilket är mindre än 25, så då måste det finnas minst en månad som tre elever måste vara födda i.
Ex
40 personer går på fest. Visa att minst två personer har skakat hand med lika många personer.
Lösning
"Objekt": 40 personer
"Lådor": Antalet personer de skakat han med
lådor: 0,1,2,3,...,39
Om en person har skakat hand med 39 pers, så finns det ingen som skakat hand med 0 personer.
Om "lådan" 39 inte är tom, så är "lådan" 0 tom. Så det kommer vara högst 39 icke-tomma "lådor", och vi kan tillämpa Lådprincipen.
Ex
Fem personer skall stå i ett kvadratiskt rum med minst 2 m mellan varje person. Hur litet kan rummet vara?
Lösning
Ett sätt: Infoga bild 4
Går det göra med ett mindre rum?
Nej

5 Grafer

Formellt En graf består av en mängd V av node (vertices) och en mängd $E \subseteq \{\{x, y\} \subseteq v | x \neq y\}$ av kanter (edges).
Infoga bild 1
Till bilden: V={1,2,3,4}, E={{1,2}, {2,3}, {2,4}, {3,4}}
$\{x, y\} \in$ E tolkas som "det finns en kant mellan x och y"
Mellan vare par av noder får det finnas högst en kant. Också inte tillåtet med "öglor".
Notation Skriver G=(V,E) för en graf.
Ex
Fyra noder

1. BILDERRR
2. BILD 2 i flera mindre pls

5.1 Vägar och cykler

En väg i en graf G=(V,E) är en sekvens $V_0, V_1, ..., V_n$ av noder så att det finns en kant mellan $V_i och V_{i+1}$ för $i = 0, 1, ..., n-1$
En cykel är en väg $V_0, V_1, ..., V_n$ där $V_0 = V_n$ och inga kanter upprepas.
Ex
INFOGA BILD 3
En graf är sammanhängande om det finns en väg mellan varje par av noder. **Ex**
INFOGA BILD 4

5.2 Isomorfa grafer

Övning Vilka av dessa grafer är lika med varandra?

1. INFOGA BILD 5 del 1
2. del 2
3. etc

Svar:
1) och 2)? Ja, de är lika
1) och 3)? Nej, exempelvis har 1) en kant mellan 1 och 2 men i 3) finns ingen kan mellan 1 och 2. Däremot är 1) och 3) lika om jag byter namn på nod 1 och nod 4 i 3)
Två grafer som ör "lika om man byter namn på noderna" kallas isomorfa (och räknas ibland som samma graf).
Formellt $G_1 = (V_1, E_1)$ och $G_2 = (V_2, E_2)$ grafer, G_1 och G_2 är isomorfa om det finns en bijektion $f : V_1 \to V_2$ så att $\{x, y\} \in E_1 \leftrightarrow \{f(x), f(y)\} \in E_2$. Funktionen f kannas för en isomorfi

Ex
PICTURE TIME dags för bild 6
Intuitivt
bild 6 del 2
Formellt
Definiera en funktion $f : \{1,2,3,4\} \to \{a,b,c,d\}$ där $\{1,2,3,4\} = V_1$ och $\{a,b,c,d\} = V_2$
$f(4) = a, f(2) = b, f(1) = c, f(3) = d$
Vi hade också kunnat reflektera grafen, och definierat en isomorfi g genom $g(3) = a, g(1) = b, g(2) = c, g(4) = d$
Infoga bild 7

5.3 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 $\{x,y\} \in V'$, 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')

Bild 8 tack :)))

5.4 Grafer med namn

BIIIIIIIILD 9
En graf kallas fullständig om det finns kanter mellan alla par av noder.
Infoga bild 10
En graf kallas bipartit om det finns en partition $V = A \cup B$, $A, B \neq \emptyset$ så att varje kant i G går mellan en nod i A och en i B. Den kallas för fullständig 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.
INFOGA BILD 11
Infoga bild 12 del 1
Bilden ovan visar en graf som är bipartit, inte fullständigt bipartit (finns ingen kant mellan 1 och 5 exempelvis)
infoga bild 12 del 2
Bilden ovan visar en graf som är fullständigt bipartit
Infoga bild 12 del 3
Bilden ovan visar en icke bipartit graf
Annat sätt att tänka
En graf är bipartit om man kan färga noderna röda och gröna så att varje kant går mellan en röd och en grön nod.

5.5 Riktade grafer

Grafer med pilar på kanterna
Formell G=(V,E) där V=mängd av noder och $E \subseteq V \times V$ mängd av kanter
(x, y) tolkas som ${}_x\cdot \curvearrowright \cdot_y$ där x är startnod och y är slutnod
I en graf är kanter oordnade på {x,y}
I en riktad graf är kanter ordnade på {x,y}

Vi tillåter "öglör", eller grafor som sluts som en ögla
Vi tillåter inte Mer än en riktad kant med samma start och slutnod
INFOGA BILD 1 11-19
OBS! Formellt är en riktad graf med nodmängd V samma sak som en relation på V. Använd det när ni visualiserar relationer

5.6 Liknande begrepp som för vanliga grafer

Riktad väg $v_0, v_1, ...v_n \in V$
$(v_0, v_1), (v_1, v_2), ...(v_{n-1}, v_n) \in E$
INFOGA BILD 2 11-19

Riktad cykel Riktad väg $v_0, v_1, ..., v_n$ med $V_0 = V_1$ och där inga kanter upprepas

G=(V,E) är starkt sammanhängande om det, för varje par av noder $x \neq y : V$ finns en riktad väg som börjar i x och slutar i y

5.7 Undedrliggande grafen till en riktad graf

Steg 1 Ta bort pilarna
Steg 2 Ta bort öglor och dubbletter på kanter
INFOGA BILD 3 11-19
En riktad graf kallas för sammanhängande om dess underliggande graf är sammanhängande.

6 Tillbaka till vanliga grafer

6.1 Träd

G=(V,E) vanlig graf är ett träd om G är sammanhängande och inte innehåller några cykler
INFOGA BILD 4 11-19

6.1.1 Två resultat om träd

Sats 7.7 i boken G=(V,E) är ett träd $\Leftrightarrow$ G är sammanhängande och $|E| = |V|-1$.

Sats 7.6 i boken G=(V,E) är ett träd om och endast om en unik väg enkel

väg mellan varje par av noder.
Enkel väg = väg där inga kanter upprepas
(Idé: Om det finns två vägar mellan x och y så finns det en cykel)

6.2 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
INFOGA BILD 5 11-19 del 1
Nod Gradtal
1 2
2 2
3 3
4 1
Summa 8, grafen har 4 kanter
INFOGA BILD 5 11-19 del 2

Nod Gradtal
1 1
2 3
3 4
4 2
5 2
Summa 12, grafen har 6 kanter
Sats G=(V,E) graf. Då är $\sum_{x \in V} d_x = 2 \cdot |E|$
Varför? Varje kant $\{v, w\} \in E$ bidrar med 1 till d_v och med 1 till d_w och med 0 till alla andra gradtal. Alltså bidrar varje kant med 2 till $\sum_{x \in V} d_x$

Följdsats (7.3+7.4 i boken)

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

6.3 Eulervägar och Eulercyklar

G=(V,E) graf
Def: En Eulerväg i G som innehåller varje kant i G exakt en gång.
En Eulerväg som också är en cykel kallas för en Eulercykel.
INFOGA BILD 6 11-19 del 1
Nod Gradtal
1 3
2 2
3 3

4 2
Sats 7.11 i boken G har (minst) en Eulercirkel $\Leftrightarrow$ all gradtal i G är jämna. INFOGA BILD 6 11-19 del 2
Nod Gradtal
1 4
2 2
3 4
4 4
5 2
6 4

Sats 7.12 i boken Låt $\{x, y\} \in V, x \neq y$. G innehåller en Eulerväg som börjar i x och slutar i y $\Leftrightarrow$ d_x är udda, och alla andra gradtal är jämna.

6.4 Hur kan man hitta Eulercykler?

Ett sätt: Hitta mindre cykler och lagg ihop dem.
Börja med att bryta ut en mindre cykel från grafen, exempelvis vägen 1,2,3,1 i förra grafen, ta bort kanterna i cykeln ifrån grafen.
Hitta en ny cykel och repitera tills du har fått flera olika cyklar, om man fortsätter på förra exemplet får man {1,2,3,1}, {1,4,6,1} och {3,4,5,6,3}
Vad som återstår nu är att lägga ihop de mindre cyklarna. Utifrån de cyklarna i exemplet får vi 1,2,3,1=1,4,6=6,5,4,5,6,=6,1 vilket är en Eulercykel

7 Matriser

En matris är en "rektangulär tabell av tal".

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

En matris har ett antal rader och ett antal kolumner (eller kolonner). Om antalet rader är m och antal kolumner är n så säger vi att vi har en $m \times n$-matris.

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

alternativt A $= \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}$ om vi behöver vara extra tydliga

a_{ij}= talet på rad i och kolumn j = talet på plats (i,j)

7.1 Räknesätt för matriser

7.1.1 Addition och subtraktion

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

$$\mathrm{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}$$

$$\mathrm{B} = \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m,1} & b_{m,2} & \dots & b_{m,n} \end{pmatrix}$$

$$\text{Def: } A + B = \begin{pmatrix} a_{1,1} + b_{1,1} & b_{1,2} + b_{1,2} & \dots & a_{1,n} + b_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} + b_{m,1} & a_{m,2} + b_{m,2} & \dots & a_{m,n} + b_{m,n} \end{pmatrix}$$

$$\text{Def: } A - B = \begin{pmatrix} a_{1,1} - b_{1,1} & b_{1,2} - b_{1,2} & \dots & a_{1,n} - b_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} - b_{m,1} & a_{m,2} - b_{m,2} & \dots & a_{m,n} - b_{m,n} \end{pmatrix}$$

7.1.2 Multiplikation

Skalärprodukt:

$\underline{a}=\begin{pmatrix} a_1 & a_2 & ... & a_n \end{pmatrix}$
radvektor, $1 \times n$-matris
$\underline{b}=\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ kolumnvektor, $n \times 1$-matris

Skalärprodukten $\underline{a} \cdot \underline{b}$ definieras som
$\underline{a} \cdot \underline{b} = a_1b_1 + a_2b_2 + \ldots + a_nb_n = \sum_{i=1}^{n} a_ib_i$

$\underline{a} \cdot \underline{b}$ är ett tal (skalär), vilket kan ses som en 1×1-matris

OBS! Skalärprodukten är endast definierad om det är lika många tal i tadvektorn som i kolumnvektorn.

Ex

$\begin{pmatrix} 1 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -2 \\ 0 \end{pmatrix} = 1 \cdot 2 + 2 \cdot (-2) + 1 \cdot 0 = -2$

$\begin{pmatrix} 8 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 8 \end{pmatrix}$ är inte definierat!

En matris $A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix}$ kan vi tänka på A som m st redvektorer,

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

Liknande: $B=\begin{pmatrix} b_{1,1} & b_{1,2} & ... & b_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m,1} & b_{m,2} & ... & b_{m,n} \end{pmatrix}$ $m \times r$-matris kan skrivas som

$B= \begin{pmatrix} \underline{b_1} & \underline{b_2} & \ldots & \underline{b_r} \end{pmatrix}$ där $b_1 = \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix}$, $b_2 = \begin{pmatrix} b_{12} \\ \vdots \\ b_{n2} \end{pmatrix}$, $\ldots$, $b_r = \begin{pmatrix} b_{1r} \\ \vdots \\ b_{nr} \end{pmatrix}$

Ex

$$\begin{pmatrix}1 & 2\\4 & 3\end{pmatrix}\begin{pmatrix}8 & 1\\-5 & 6\end{pmatrix} = \left(\begin{pmatrix}1 & 2\\4 & 3\end{pmatrix}\left(\begin{pmatrix}8\\-5\end{pmatrix}\begin{pmatrix}1\\6\end{pmatrix}\right)\right) = \begin{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\cdot\begin{pmatrix}8\\-5\end{pmatrix} & \begin{pmatrix}1 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\6\end{pmatrix}\\ \begin{pmatrix}4 & 3\end{pmatrix}\cdot\begin{pmatrix}8\\-5\end{pmatrix} & \begin{pmatrix}4 & 3\end{pmatrix}\cdot\begin{pmatrix}1\\6\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\cdot 8+2\cdot(-5) & 1\cdot 1+2\cdot 6\\4\cdot 8+3\cdot(-5) & 4\cdot 1+3\cdot 6\end{pmatrix} =$$
$$\begin{pmatrix}-2 & 13\\17 & 22\end{pmatrix}$$

Ex

$$\begin{pmatrix}1 & 0\\2 & 1\end{pmatrix}\begin{pmatrix}3 & 4 & 0\\2 & 0 & 1\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix}\cdot\begin{pmatrix}3\\2\end{pmatrix} & \begin{pmatrix}1 & 0\end{pmatrix}\cdot\begin{pmatrix}4\\0\end{pmatrix} & \begin{pmatrix}1 & 0\end{pmatrix}\cdot\begin{pmatrix}0\\1\end{pmatrix}\\ \begin{pmatrix}2 & 1\end{pmatrix}\cdot\begin{pmatrix}3\\2\end{pmatrix} & \begin{pmatrix}2 & 1\end{pmatrix}\cdot\begin{pmatrix}4\\0\end{pmatrix} & \begin{pmatrix}2 & 1\end{pmatrix}\cdot\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\cdot 3+0\cdot 2 & 1\cdot 4+0\cdot 0 & 1\cdot 0+0\cdot 0\\2\cdot 3+1\cdot 2 & 2\cdot 4+1\cdot 0 & 2\cdot 0+1\cdot 1\end{pmatrix} =$$
$$\begin{pmatrix}3 & 4 & 0\\8 & 8 & 1\end{pmatrix}$$

OBS! $\begin{pmatrix}3 & 4 & 0\\2 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\2 & 1\end{pmatrix}$ är inte definierat

Ordning spelar roll! Ex:

$$\begin{pmatrix}8 & 1\\-5 & 6\end{pmatrix}\begin{pmatrix}1 & 2\\4 & 3\end{pmatrix} = \begin{pmatrix}8\cdot 1+1\cdot 4 & 8\cdot 2+1\cdot 3\\(-5)\cdot 1+6\cdot 4 & (-5)\cdot 2+6\cdot 3\end{pmatrix} = \begin{pmatrix}12 & 19\\19 & 8\end{pmatrix} \neq \begin{pmatrix}-2 & 13\\17 & 22\end{pmatrix} =$$
$$\begin{pmatrix}1 & 2\\4 & 3\end{pmatrix}\begin{pmatrix}8 & 1\\-5 & 6\end{pmatrix}$$

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

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

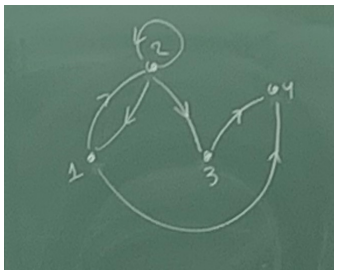
7.2 Tillämpning på riktade grafer

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

Def Grannmatrisen A = $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ $n \times n$-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

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$



Sats Antalet riktade vägar i G av längd k frpn nod i till nod j ges av talet på plats (i,j) i matrisen
$A^k = AA \dots A$, k ggr, där A är grannmatrisen till G

8 Talteori (kap 5)

Teorin flr heltalen $\mathbb{Z}$
Första målet Visa att varje positivit heltal kan skrivas som en produkt av primtal på ett unikt sätt.

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

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

Ex
$a \mid b$ ty $4 = 2 \cdot 2$, $3 \mid 2$ ty $12 = 3 \cdot 4$
$5 \nmid 24$ då $5m \neq 24 \forall m \in \mathbb{Z}$
$0 \mid 0$ ty $0m = 0 \forall m \in \mathbb{Z}$
Delbarhet är en relation på $\mathbb{Z}$.

8.1 Några egenskaper (5.4 i boken)

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

Bevis av 5)
$\Leftarrow$: Antag att $a \mid xb + yc$ oavsett vad x och y är $(x, y \in \mathbb{Z})$
Om $x = 1$ och $y = 0$, så får jag $a \mid 1 \cdot b + 0 \cdot c = b$, dvs $a \mid b$.
Om $x = 0$ och $y = 1$, så får jag $a \mid 0 \cdot b + 1 \cdot c = c$, dvs $a \mid c$.
Så $a \mid b \wedge a \mid c$.

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

Delbarhet är reflexiv, transitiv och ”nästan asymmetrisk”.

8.2 Sats 5.7

Om $a \mid b$ och $b \mid a$, då är antingen $a = b$ eller $a = -b$.

8.2.1 Bevis

Fall 1: $a = 0$: $a \mid b \Rightarrow b = 0 \Rightarrow a = b = -b$.
Fall 2: $a \neq 0$: $a \mid b$ betyder $\exists m \in \mathbb{Z} : b = am$
$b \mid a$ betyder $\exists n \in \mathbb{Z} : a = bn$,
så $a = bn = amn \Rightarrow 1 = mn \Rightarrow m = n = 1$ eller $m = n = -1$
$m = n = 1$ ger $a = bn = b$, $m = n = -1$ ger $a = bn = -b$ v.s.b

8.3 Division med rest

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

Ex $17 = 3 \cdot 5 + 2$ som är skriven på formen $a = q \cdot b + r$

q är det största heltalet så att $a - qb \geq 0$.
Och r är då $a - qb$.

8.4 Gemensamma delare

Def: $a, b \in \mathbb{Z}$, då varken a eller b är =0
En Gemensam delare till a och b är ett $d \in \mathbb{Z}$ så att $d \mid a$ och $d \mid b$.

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

En gemensam delare d till a och b uppfyller (om $a \neq 0$)

- $d \leq |a|$, så det finns alltid en störstagemensamma 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
så de positiva gemensamma delarna är 1 och 2, och sgd(4,6)=2

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

8.5 Sats (5.14)

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)

8.5.1 Varför?

1. $a \mid a$ och $a \mid 0$ så a är en gemensam delare till a och 0. Om $d \mid a$ så är $d \leq a$, så måste a 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 $d \mid a$ och $a \mid b$, så måste också $d \mid a + nb$ enligt sats 5.4 (del 5).
   Om $d \mid a + nb$ och $d \mid b$, så måste också $d \mid (a + nb) - nb$, dvs $d \mid a$ v.s.b

8.6 Euklides algoritm

$a, b \in \mathbb{Z}_+$. $a \geq b$. Genom upprepad division med rest får vi

$a = bq_1 + r_1$, $0 \leq r_1 < b$
$b = r_1q_2 + r_2$, $0 \leq r_2 < r_1$
$r_1 = r_2q_3 + r_3$, $0 \leq r_3 < r_2$
$\vdots$
$r_{n-2} = r_{n-1}q_n + r_n$,
$r_{n-1} = r_nq_{n+1} + r_{n+1}$

Slutar när resten är 0. Då är $sgd(a, b) = r_n$. (Sista resten som inte är 0)

Ex
Hitta sgd(16,24)
$24 = 16 \cdot 1 + 8$
$16 = 8 \cdot 2$, så sgd(16,24)=8
Hitta sgd(7,15)
$13 = 7 \cdot 1 + 6$
$7 = 6 \cdot 1 + 1$ så sgd(7,13)=1
$6 = 1 \cdot 6$

8.6.1 Varför funkar Euklides algoritm?

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

Ex a=876, b=204
$876 = 204 \cdot 4 + 60$ $\quad 60 = 24 \cdot 2 + 12$ $\quad 24 = 12 \cdot 2$ så sgd(876, 204)=12.
$204 = 60 \cdot 3 + 24$

9 Aritmetikens fundamentalsats

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

Ex:

$36 = 2 \cdot 2 \cdot 3 \cdot 3$ $\quad$ $10 = 2 \cdot 5$

$17 = 17$

Bevis:

Först $n \leq ar$ vi att det finns en primtalsfaktorisering, med strak induktion:

Basfall:

$m = 2$, $2 = 2$ är ett primtal

Induktionssteget:

Säg att varje tal $k < m$ har en primtalsfaktorisering. Om m är ett primtal är vi klara ($m = m$ är

SKRIV UTIFRÅN BILDER

10 Kongruenser

Idag är det tisdag. VIlken veckodag är det om:

1. 6 dagar? (Måndag)
2. 10 dagar? (Fredag)
3. 106 dagar? (Onsdag)

Hur kan man räkna? Cykler av 7 dagar

1. 6 dagar framåt = 1 dag bakåt -¿ Måndag
2. 10 = 7 + 3, 10 dagar framåt = 3 dagar framåt -¿ Fredag
3. $106 = 7 \cdot 15 + 1$, så 106 dagar framåt = 1 dag framåt -¿ Onsdag

Matematiskt kan man ställa upp det så här: Måndag-Söndag representerar vi med 1 till 7.
Tisdag = 2.

1. $2 + 6 = 8 = 7 + 1$,, 1 = Måndag
2. $2 + 10 = 12 = 7 + 5$, 5 = Fredag
3. $2 + 106 = 108 = 7 \cdot 15 + 3$, 3 = Onsdag

kallas restträkning modulo 7 eller kongruensräkning modulo 7. 7 är "cyckel", kallas modulus. I andra exempel har man ett annat modulus, t.ex 12 eller 24. Rent matematiskt kan vi välja vilket heltal $n \in \mathbb{Z}_+$ som helst som modulus. Jag vill betrakta två hetlal som "samma" om deras differens är en multipel av n.

Hur? Ekvivalensrelation.
Def: Låt $n \in \mathbb{Z}_+$. Vi definierar en relation "$a \equiv b$ modulo n" på $\mathbb{Z}$ om $n \mid a - b$ (dvs $a - b$ är en multipel av n)
Utläses "a är kngruent med b modulo n". Skrivs oftast $a \equiv b \bmod n$ eller $a \equiv b\ (n)$
Ex:

1. Om $n = 7$, så är $8 \equiv 1\ (7)$ eftersom $8 - 1 = 7$ är en multipel av 7.
   Också $108 \equiv 3\ (7)$, eftersom $108 - 3 = 105 = 7 \cdot 15$ är en multipel av 7.
   Däremot är $11 \not\equiv 3\ (7)$, eftersom $11 - 3 = 8$ inte är en multipel av 7

Sats Kongruens mod n är en kvivalensrelation.

Bevis Skall kolla att kongruens mod n är reflexiv, symmetrisk och transitiv.
Reflexiv $a \equiv a \bmod n$? ja, eftersom $a - a = 0$, som är delbart med n
Symmetrisk Om $a \equiv b \bmod n$, så gäller $n \mid a - b$, om $n \mid a - b$,
så $n \mid (-1)(a - b) = n \mid b - a$, dvs $b \equiv a \bmod n$
Transitiv Antag att $a \equiv b \bmod n$ och $b \equiv c \bmod n$, dvs $n \mid a - b$ och $n \mid b - c$.
Då gäller $n \mid (a - b) + (b - c) = n \mid a - c$, dvs $a \equiv c \bmod n$

10.1 Hur ser ekvivalensklasserna för kongruens mod n ut?

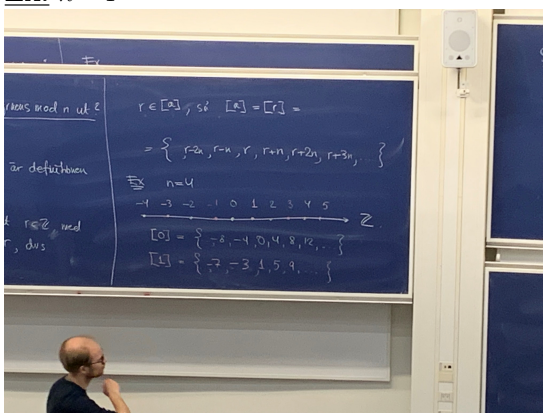
Låt $a \in \mathbb{Z}$.

$[a] = \{b \in \mathbb{Z} \mid b \equiv a \bmod n\}$ är definitionen av en ekvivalensklass

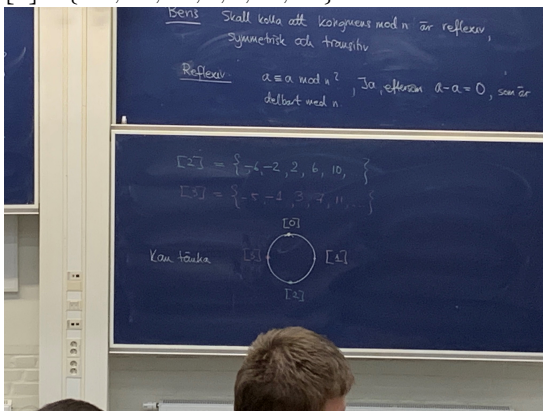
Enligt divisionsalgoritmen finns ett unikt $r \in \mathbb{Z}$ med $0 \leq r \leq n-1$ så att $a = nq + r$ dvs $a \equiv r \bmod n$

$r \in [a]$, så $[a] = [r] = \{\ldots, r-2n, r-n, r, r+n, r+2n, \ldots\}$

Ex: $n = 4$



$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$
$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$
$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$
$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$



10.2 Add, sub, multi och divi modulo n

Ekvivalensklasserna till relationen ≡ mod n.

Det finns n st olika kongruensklasser modulo n:

$[0]_{[n]}, [1]_{[n]}, [2]_{[n]}, \ldots, [n-1]_{[n]}$

Ett tal $a \in \mathbb{Z}$ tillhör $[r]_n$, där r är resten vid division av a med n. (dvs $a = q \cdot n + r$,

$+ \leq r \leq n$)
Def: $\mathbb{Z}_{\ltimes} = \{[0]_{[}n], [1]_{[}n], \ldots, [n-1]_{[}n]\}$, mängden av alla kongruensklasser modulo n.

10.2.1 Addition, subtraktion och multiplikation

Sats (5.38) $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{Z}_+$
Säg att $a \equiv c\ (n)$ och $b \equiv d\ (n)$. Då är

1. $a + b \equiv c + d$
2. $a - b \equiv c - d$
3. $ab \equiv cd$

Ex: $6 \cdot 9$ mod 7?
$6 \cdot 9 = 54 = 7 \cdot 7 + 5 \equiv 5\ (7)$
$6 \cdot 9 \equiv (-1) \cdot 2 \equiv -2 \equiv 5\ (7)$

Varför är satsen sann?

1. Vill visa $a + b \equiv c + d\ (n)$, dvs $n \mid (a + b) - (c + d)$.
   Vet att $n \mid a - c\ (= a \equiv c\ (n))$ och $n \mid b - d\ (b \equiv d\ (n))$.
   $(a + b) - (c + d) = (a - c) + (b - d)$, så $n \mid (a + b) - (c + d)$.
2. Görs på liknande sätt
3. Görs på liknande sätt

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

Def: Vi definierar addition, subtraktion och multiplikation på $\mathbb{Z}_{\ltimes}$ genom
$[a]_n + [b]_n = [a + b]_n$
$[a]_n - [b]_n = [a - b]_n$
$[a]_n \cdot [b]_n = [a \cdot b]_n$
Varför är denna definitionen okej? Säg att $[a]_n = [c]_n$ och $[b]_n = [d]_n$. Är då

1. $[a + b]_n = [c + d]_n$?
2. $[a - b]_n = [c - d]_n$?
3. $[a \cdot b]_n = [c \cdot d]_n$?

$[a]_n = [c]_n \Leftrightarrow a \equiv c\ (n)$ och $[b]_n = [d]_n \Leftrightarrow b \equiv d\ (n)$

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

Så definitionen är ok.

Ex: I $\mathbb{Z}_{\not 4}$
$[3]_4 + [2]_4 = [3+2]_4 = [5]_4 = [1]_4$
$[1]_4 - [3]_4 = [1-3]_4 = [-2]_4 = [2]_4$
$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$

10.3 Division i $\mathbb{Z}_{\ltimes}$

Division i $\mathbb{Z}$ - normalt är $\frac{a}{b}$ inte ett heltal även om a och b är heltal.
Så det kommer inte funka att göra på samma sätt.
$\frac{[1]_3}{[2]_3} = [\frac{1}{2}]_3$??? vad är $[\frac{1}{2}]_3$? (Finns inte)

10.3.1 Vad är division?

$a, b \in \mathbb{C}$ eller i $\mathbb{R}$.
$\frac{b}{a} = \frac{1}{a} \cdot b$ Divison a = multiplikation med $\frac{1}{a}$ Vad är $\frac{1}{a}$? $\frac{1}{a}$ är ett tal x så $x \cdot a = 1$
Med andra ord $\frac{1}{a}$ är lösningen (om den finns!) på $a \cdot x = 1$.
Om a=0 har $a \cdot x = 1$ ingen lösninge - går inte att dela med 0.

I $\mathbb{Z}_{\ltimes}$ Givet $[a]_n \in \mathbb{Z}_{\ltimes}$, när kan vi lösa $[a]_n[x]_n = [1]_n$?
Ex: Kan jag lösa $[2]_3[x]_3 = [1]_3$?
Ja, $[x]_3 = [2]_3$ är en lösning
$[2]_3[2]_3 = [4]_3 = [1]_3$

10.3.2 Att lösa $[a]_n[x]_n = [1]_n$

Samma som $[ax-1]_n = [0]_n$, dvs $n \mid ax - 1$, dvs $\exists y \in \mathbb{Z}$
$ax - 1 = ny \Leftrightarrow ax - ny = 1$ (vilket är en linjjär diofantiskekvation!)
$ax - ny = 1$ är lösbar $\Leftrightarrow sgd(a,n) \mid 1 \Leftrightarrow sgd(a,n) = 1$ och vi kan lösa den genom Euklides algoritm. Vår formel för den allmänna lösningen till $ax - ny = 1$ ger att x är unik modulo n.

Modulo 3: Om

- $a = 0$ finns inget x
- $a = 1$, $x \equiv 1 \ (3)$
- $a = 2$, $x \equiv 2 \ (3)$

Modulo 5: Om

- $a = 0$ finns inget x
- $a = 1$, $x \equiv 1\ (5)$
- $a = 2$, $x \equiv 3\ (5)$ $2 \cdot 3 = 6 \equiv 1\ (5)$
- $a = 3$ $x \equiv 2\ (5)$
- $a = 4$ $x \equiv 4\ (5)$
  $4 \equiv -1$ $x \equiv -1$

Def: Låt $[a]_n \in \mathbb{Z}_\ltimes$. Om $sgd(a, n) = 1$ så finns ett unikt $[x]_n \in \mathbb{Z}_\ltimes$ så att $[a]_n[x]_n = [1]_n$
$[x]_n$ kallas för inversen till $[a]_n$
Ett heltal x med egenskapen $ax \equiv 1\ (n)$ kallas för en invers till a modulo n. Om a har en invers modulo n säger vi att a är inverterbar modulo n.

Ex: 4 är inverterbar mod 9, eftersom $sgd(4, 9) = 1$. Hur hittar vi inversen till 4 mod 9?
Euklides algoritm:
$9 = 4 \cdot 2 + 1$
$4 = 1 \cdot 4$
Balänges
$1 = 9 - 4 \cdot 2$, ta det här mod 9
$1 \equiv 0 - 4 \cdot 2 \equiv (-2) \cdot 4\ (9)$
Så $x = -2$ löser $4x \equiv 1\ (9)$, dvs -2 är en invers till 4 mod 9

11 Linjära kongruens ekvationer

Ex: Lös $4x \equiv 3$ mod 11. En lösning: Prova allt!
Där $x \equiv 9$ mod 9 är lösningen.

Mer systematiskt $4x \equiv 3$ mod 11 Vill multiplicera ekvationen med inversen till 4 (om den finns) modulo 11, för att "få bort" 4:an.
Hitta inversne till 4 mod 11:
$11 = 4 \cdot 2 + 3$
$4 = 3 \cdot 1 + 1$
$1 = 4 - 3 = 4 - (11 - 4 \cdot 2) = 3 \cdot 4 - 11$
$1 = 3 \cdot 4 - 11$ ger att $1 \equiv 3 \cdot 4$ mod 11.

För en vanlig ekvation $4x = 3$ hade vi delat med 4, dvs multiplicerat med $\frac{1}{4}$, dvs multiplicerat med inversen till 4.

12 Eulers Φ-funktion

$n \in \mathbb{Z}_+$. $u(n)\{[x]_n \in \mathbb{Z}_\ltimes \mid [x]_n$ är inverterbar $\} = \{[x_n \in \mathbb{Z}_\ltimes] \mid sgd(x, b) = 1\} \subseteq \mathbb{Z}_\ltimes$
Def: $\Phi(n) = \mid u(n) \mid$, dvs

$\Phi(n)$ = antalet tal i $\{1,\ldots,n\}$ som är relativt prima med n.

Ex:
$\Phi(1) = 1$ $u(1) = \{1\}$
$\Phi(2) = 1$ $\mathbb{Z}_{\not 2} = \{[0]_2, [1]_2\}$ och $u(2) = \{[1]_2\}$ har ett element
n=6 $\mathbb{Z}_{\not 6} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$
$u(6) = \{[1]_6, [5]_6\}$, så $\Phi(6) = 2$.

12.1 Eulers sats

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

p primtal $\Phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. $(k \in \mathbb{Z}_+)$
Varför? Vill beräkna antalet a mellan 1 och p^k som är relativt prima med p^k, dvs $sgd(a, p^k) = 1 \Leftrightarrow p \nmid a$

De a mellan 1 och p^k med $p \mid a$ är $p, 2p, 3p, \ldots, p^k = p^{k-1}p^k$, så de är p^{k-1} st
Så antalet a med $p \nmid a$ är $p^k - p^{k-1}$, så $\Phi(p^k) = p^k - p^{k-1}$.

Sats (5.54) Om sgd(m,n)=1, så är $\Phi(m,n) = \Phi(m) \cdot \Phi(n)$.
Varför?
$\Phi(mn)$ = antalet a mellan 0 och $mn-1$ som är relativt prima med mn.
Definiera en funktion $\{0,1,\ldots,mn-1\} \to \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\}$ på följande sätt.
Om $a \in \{0,1,\ldots,mn-1\}$ så är $\quad a = mq_1 + r_1 \quad r_1 \in \{0,1,\ldots,m-1\}$
$\qquad\qquad\qquad\qquad\qquad\quad a = nq2 + r_2 \quad r_2 \in \{0,1,\ldots,n-1\}$
Vi sätter $f(a) = (r_1, r_2)$.

1. f är ingektiv: Om $f(a) = f(b)$, så är $a \equiv b\ (m)$ och $a \equiv b\ (n) \Rightarrow a \equiv b\ (mn)$ enligt kinesiska restsatsen, så $a = b$ eftersom $a, b \in \{0,1,\ldots,mn-1\}$.

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

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

Alltså f ger en bijektion mellan $\{a \mid a \in \{0,1,\ldots,mn-1\}, sgd(a,mn) = 1\}$ (har $\Phi(mn)$ element) och $\{x \mid x \in \{0,1,\ldots,mn-1\}, sgd(x,m) = 1\} \times \{y \mid y \in \{0,1,\ldots,n-1\}, sgd(y,n) = 1\}$. Så $\Phi(mn) = \Phi(m)\Phi(n)$ v.s.b

Om $n = p_1^{e_1} \ldots p_r^{e_r}$, med p_i olika primtal och $e_i \geq 1$, så är $\Phi(n) = \Phi(p_1^{e_1} \ldots p_r^{e_r}) = \Phi(p_1^{e_1}) \ldots \Phi(p_r^{e_r}) = (p_1^{e_r} - p_1^{e_1 - 1}) \ldots (p_r^{e_r} - p_r^{e_1 - 1})$
Ex: $\Phi(6) = \Phi(2 \cdot 3) = \Phi(2) \cdot \Phi(3) = (2^1 - 2^0)(3^1 3^0) = (2-1)(3-1) = 1 \cdot 2 = 2$
$\Phi(48) = \Phi(2^4 \cdot 3) = \Phi(2^4)\Phi(3) = (2^4 - 2^3)(3^1 - 3^0) = (16-8)(3-1) = 8 \cdot 2 = 16$

Specialfall av Eulers sats p primtal.

1. Om $p \nmid a$, så är $a^{p-1} \equiv 1\ (p)$.
2. $a^p \equiv a\ (p)$ för alla $a \in \mathbb{Z}$

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

Entalssiffra = rest vid division med 10 $77 \equiv 7\ (10)$, $121 \equiv 1\ (10)$.
3^8 $\Phi(10) = \Phi(2)\Phi(5) = 1 \cdot 4 = 4$, så $3^8 = (3^4)^2 \equiv 1^2 \equiv 1\ (10)$
2^{10} kan inte använda Eulers sats då $sgd(2, 10) = 2 \neq 1$.
$2^8 \equiv -2\ (10)$ så $2^{10} = 2^{3\cdot 3+1} = (2^3)^3 \cdot 2 = -(-2)2 \equiv 4\ (10)$.
$3^8 \cdot 77 + 2^{10} \cdot 121 \equiv 1 \cdot 7 + 4 \cdot 1 \equiv 11 \equiv 1\ (10)$
Så entalssiffran är 1.