# MS-A0409 Grundkurs i diskret matematik
# Sammanfattning, del II

G. Gripenberg

Aalto-universitetet

15 maj 2014

## Delbarhet

*Ett tal $a$ delar ett tal $b$ eller $b$ är delbart med $a$ om det finns ett* **heltal** *$k$ så att $b = ak$, dvs. $b \in a\mathbb{Z}$. Detta skrivs också ofta som $a \mid b$ (men detta är inte "a eller b"). Då säger man också att $b$ är en (heltals)multipel av $a$.*

## Modulofunktionen mod

*Om $n > 0$ så är $\operatorname{mod}(m, n) = j$ ifall $0 \leq j < n$ och $m = j + kn$ där $k \in \mathbb{Z}$. (men $\operatorname{mod}(m, 0) = m$ och $\operatorname{mod}(m, n) = -\operatorname{mod}(m, -n)$ om $n < 0$). Om $m$ och $n$ är positiva tal så är $\operatorname{mod}(m, n)$ den rest som erhålls då man dividerar $m$ med $n$ men om $m < 0$ är denna rest inte positiv.*

## Kongruens modulo

*Två tal $a$ och $b$ är kongruenta modulo $n$ vilket skrivs $a \equiv_n b$ eller $a \equiv b \pmod{n}$ om $n$ delar $a - b$, dvs. $b - a$ är en multipel av $n$:*

$$a \equiv_n b \quad \leftrightarrow \quad a \equiv b \pmod{n} \quad \leftrightarrow \quad n \mid (a - b)$$
$$\leftrightarrow a = b + kn, \quad k \in \mathbb{Z} \quad \leftrightarrow \quad \operatorname{mod}(a, n) = \operatorname{mod}(b, n)$$



## $\mathbb{Z}/n\mathbb{Z}$, kongruensklasser

*Relationen $a \equiv_n b$ är en ekvivalensrelation i $\mathbb{Z}$ ($x \sim x$, $x \sim y \to y \sim x$, $x \sim y$ & $y \sim z \to x \sim z$) och delar upp $\mathbb{Z}$ i ekvivalensklasser, som kallas* **kongruensklasser** *(eller restklasser), dvs. delmängder $\{\ldots, -2n, -n, 0, n, 2n \ldots\}$, $\{\ldots, -2n+1, -n+1, 1, n+1, 2n+1 \ldots\}$, $\ldots$, $\{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}$ där alla element i samma ekvivalensklass är kongruenta modulo $n$ med varandra. Man kan använda följande beteckningar:*

$$[k]_n \stackrel{\text{def}}{=} \{\, m \in \mathbb{Z} : m \equiv_n k \,\} = \{\, m \in \mathbb{Z} : \operatorname{mod}(m, n) = \operatorname{mod}(k, n) \,\},$$
$$\mathbb{Z}/n\mathbb{Z} \stackrel{\text{def}}{=} \{\, [k]_n : k = 0, 1, 2, \ldots, n-1 \,\}, \quad \text{om } n > 0.$$

## Obs!

*Eftersom $\operatorname{mod}(m_1, n) = \operatorname{mod}(m_2, n) \Leftrightarrow [m_1]_n = [m_2]_n$ så väljer man ofta elementet $\operatorname{mod}(m, n)$ för att representera kongruensklassen $[m]_n$ så att man tex. kan tala om talen $0, 1, 2, \ldots, 5$ som elementen i $\mathbb{Z}/6\mathbb{Z}$ istället för mängderna $[0]_6, [1]_6, \ldots, [5]_6$. Ofta används $\overline{k}_n$ istället för $[k]_n$ och $\mathbb{Z}_n$ istället för $\mathbb{Z}/n\mathbb{Z}$.*

## Addition, subtraktion och multiplikation i $\mathbb{Z}/n\mathbb{Z}$

*Man kan visa att om*

$$a_1 \equiv_n a_2 \quad \textit{och} \quad b_1 \equiv_n b_2$$

*så är*

$$\begin{aligned}(a_1 + b_1) &\equiv_n (a_2 + b_2)\\ (a_1 - b_1) &\equiv_n (a_2 - b_2)\\ (a_1 b_1) &\equiv_n (a_2 b_2)\end{aligned}$$

*Därför kan man definiera räkneoperationer i $\mathbb{Z}/n\mathbb{Z}$ med*

$$\begin{aligned}[a]_n + [b]_n &= [a+b]_n,\\ [a]_n - [b]_n &= [a-b]_n,\\ [a]_n \cdot [b]_n &= [a \cdot b]_n,\end{aligned}$$

*och alla "normala" räkneregler gäller (bortsett från de som gäller olikheter).*



## Största gemensamma delare

*Om $m$ och $n$ är heltal som inte båda är noll så är deras största gemensamma delare*

$$\text{sgd}\,(m,n) = \max\{\, d \in Z : d|m \textit{ och } d|n \,\}.$$

*(sgd=största gemensamma delare, gcd= greatest common divisor, och vanligen definierar man* $\text{sgd}\,(0,0) = 0$*)*
*Om* $\text{sgd}\,(m,n) = 1$ *sägs talen $m$ och $n$ vara relativt prima.*
*Observera att av defintionen följer att* $\text{sgd}\,(m,n) = \text{sgd}\,(n,m)$.

## Inverser i $\mathbb{Z}/n\mathbb{Z}$

*Om $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ och det finns en kongruensklass $[j]_n \in \mathbb{Z}/n\mathbb{Z}$ så att $[m]_n \cdot [j]_n = [1]_n$, dvs $m \cdot j \equiv_n 1$ så säger man att $[m]_n$ (eller bara $m$) är inverterbar i $\mathbb{Z}/n\mathbb{Z}$ och inversen är $[j]_n = [m]_n^{-1}$. Detta innebär att man kan dividera med $[m]_n$ för det är det samma som att multiplicera med $[j]_n$. Eftersom $m \cdot j \equiv_n 1$ så finns det ett heltal $k$ så att $m \cdot j = 1 + k \cdot n$. Om nu $d|m$ och $d|n$ så gäller $d|(m \cdot j - k \cdot n)$ dvs. $d|1$ och då är $d = 1$. Därför måste $\text{sgd}\,(m, n) = 1$. Man kan också visa att det omvända gäller så man får att*

$$[m]_n \text{ är inverterbar i } \mathbb{Z}/n\mathbb{Z} \quad \Leftrightarrow \quad \text{sgd}\,(m, n) = 1.$$

## Obs

*Om $p$ är ett primtal så är alla element i $\mathbb{Z}/p\mathbb{Z}$ som inte är $[0]_p$ inverterbara.*

## Exempel

*Kongruensklasserna $[1]_6$ och $[5]_6$ är de enda som är inverterbara i $\mathbb{Z}_6$.*



## Euklides algoritm för att räkna $\text{sgd}\,(m, n)$

- *Antag att $m > n$ ($\text{sgd}\,(m, m) = m$).*
- *Låt $r_0 = m$ och $r_1 = n$.*
- *Räkna ut $q_i$ och $r_i$ så att $0 \le r_i < r_{i-1}$ och*

$$r_{i-2} = q_i r_{i-1} + r_i$$

  *då $i \ge 2$ så länge $r_{i-1} \neq 0$.*
- $\text{sgd}\,(m, n) = r_{k-1}$ *om* $r_k = 0$.

## Varför fungerar Euklides algoritm?

*Det följer av ett allmänt resultat att om $r_{i-2} = q_i r_{i-1} + r_i$ så är $\text{sgd}\,(r_{i-2}, r_{i-1}) = \text{sgd}\,(r_{i-1}, r_i)$ för alla $i \ge 2$ för vilka $r_{i-1} \neq 0$. Eftersom $d|0$ för alla $d$ gäller $\text{sgd}\,(r_{k-1}, 0) = r_{k-1}$ vilket innebär att $\text{sgd}\,(m, n) = \text{sgd}\,(r_0, r_1) = \ldots = \text{sgd}\,(r_{k-1}, r_k) = \text{sgd}\,(r_{k-1}, 0) = r_{k-1}$ om $r_k = 0$.*

## Euklides algoritm och inversa element i $\mathbb{Z}/n\mathbb{Z}$

*Om man i Euklides algoritm valt* $r_0 = m$, $r_1 = n$ *och sedan räknat* $q_i$ *och* $r_i$ *för* $i = 2, \ldots, k$ *med formeln* $r_{i-2} = q_i r_{i-1} + r_i$ *tills* $r_k = 0$, *så att* $r_{k-1} = \operatorname{sgd}(m, n)$ *så kan man räkna baklänges så att man startar med ekvationen* $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ *så får man*

$$\operatorname{sgd}(m, n) = r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}.$$

*Sedan sätter man in* $r_{k-2}$ *ur ekvationen* $r_{k-2} = r_{k-4} - q_{k-2} r_{k-3}$ *och uttrycker* $\operatorname{sgd}(m, n)$ *med hjälp av* $r_{k-4}$ *och* $r_{k-3}$ *och fortsätter tills man får*

$$\operatorname{sgd}(m, n) = am + bn.$$

*Om nu* $\operatorname{sgd}(m, n) = 1$ *betyder detta att*

$$[a]_n \cdot [m]_n = [1]_n \quad \textit{dvs.} \quad [a]_n = [m]_n^{-1},$$

*och*

$$[b]_m \cdot [n]_m = [1]_m \quad \textit{dvs.} \quad [b]_m = [n]_m^{-1}.$$



## Eulers $\varphi$-funktion

$$\begin{aligned}\varphi(n) &= \textit{antalet tal i mängden } \{\, m \in \mathbb{Z} : 0 \le m \le n-1, \operatorname{sgd}(m, n) = 1 \,\}, \\ &= \textit{antalet element i } \mathbb{Z}/n\mathbb{Z} \textit{ som har en en invers.}\end{aligned}$$

*Notera att* $[0]_1$ *är inverterbar i* $\mathbb{Z}/1\mathbb{Z}$ *så att* $\varphi(1) = 1$ *men* $[0]_n$ *är förstås (?) inte inverterbar i* $\mathbb{Z}/n\mathbb{Z}$ *då* $n > 0$.

## Eulers teorem

*Om* $\operatorname{sgd}(a, n) = 1$ *och* $n > 1$ *så är*

$$a^{\varphi(n)} \equiv_n 1.$$

## Fermats lilla teorem

*Om $p$ är ett primtal och* $\text{sgd}(a, p) = 1$ *så är*

$$a^{p-1} \equiv_p 1.$$

## Potenser i $\mathbb{Z}/p\mathbb{Z}$ då $p$ är ett primtal

*Om man skall räkna ut* $\text{mod}(a^m, p)$ *då $p$ är ett primtal får man naturligtvis* 0 *om* $\text{sgd}(a, p) \neq 1$ *(för då är* $\text{sgd}(a, p) = p$ *och $p|a$ eftersom $p$ är ett primtal) och annars kan man utnyttja det faktum att* $a^{p-1} \equiv_p 1$ *för det innebär att* $a^m \equiv_p a^{\text{mod}(m,p-1)}$ *vilket kan vara mycket enklare att räkna ut.*



## RSA-algoritmen

*I RSA-algoritmen används en publik nyckel $(n, k)$ för kryptering och en privat nyckel $(n, d)$ för dekryptering:*

- *Kryptering: "Meddelandet" $a$, som är ett tal mellan* 0 *och* $n - 1$ *krypteras till* $b = \text{mod}(a^k, n)$.
- *Det mottagna meddelandet $b$ dekrypteras till* $a = \text{mod}(b^d, n)$.

*Ideen är den att vem som helst kan skicka meddelanden krypterade med den publika nyckeln men bara den som känner till den privata nyckeln, som är "svår" at räkna ut bara med hjälp av $n$ och $k$, kan dekryptera meddelandet.*

## Hur skall nycklarna i RSA-algoritmen väljas?

- *$n = pq$ där $p$ och $q$ är två olika "mycket stora" primtal.*
- *$k$ är ett "inte alltför litet" tal så att $\text{sgd}(k, m) = 1$ där $m = (p-1)\cdot(q-1)$ (och det "svåra" med att räkna ut $d$ är att bestämma $p$ och $q$ och därmed $m$ om man bara känner till $n$).*
- *Med hjälp av Euklides algoritm kan $d$ bestämmas så att $[d]_m = [k]_m^{-1}$.*

## Varför fungerar RSA-algoritmen?

- *Antag för enkelhets skull att $\text{sgd}\,(a, n) = 1$.*
- *Man kan visa att $\varphi(n) = m$.*
- *Enligt Eulers teorem gäller $a^m \equiv_n 1$*
- *Eftersom $k \cdot d = 1 + r \cdot m$ är*

$$\left[b^d\right]_n = \left[a^{k\cdot d}\right]_n = \left[a^{1+r\cdot m}\right]_n = [a]_n \cdot [a^m]_n^r = [a]_n \cdot [1]_n^r = [a]_n,$$

*vilket betyder att $\text{mod}\,(b^d, n) = \text{mod}\,(a, n) = a$.*



## Underskrifter och RSA-algoritmen

*Antag att A vill skicka meddelandet $a$ till B och övertyga B om att meddelandet verkligen kommer från A. De kan göra detta på följande sätt:*

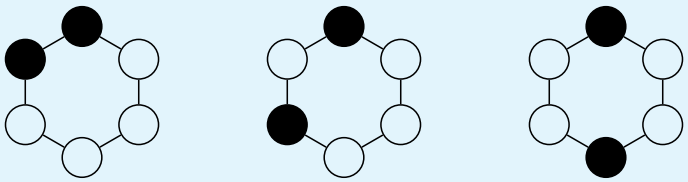
- *A räknar ut ett "sammandrag" $h(a)$ av $a$ (ur vilket $a$ inte kan bestämmas).*
- *A krypterar $a$ med B:s publika nyckel $(n_B, k_B)$ till $b = \text{mod}\,(a^{k_B}, n_B)$.*
- *A krypterar $h(a)$ med sin egna privata nyckel $(n_A, d_A)$ till $s = \text{mod}\,(h(a)^{d_A}, n_A)$.*
- *A skickar $b$ och $s$ till B.*
- *B dekrypterar $b$ med sin privata nyckel $(n_B, d_B)$ till $a$.*
- *B räknar ut $h(a)$ och dekrypterar $s$ med A:s publika nyckel $(n_A, k_A)$ och om resultatet är samma som $h(a)$ så är det troligt att meddelandet $a$ verkligen kom från A eftersom ingen annan borde kunna kryptera $h(a)$ med A:s privata nyckel $(n_A, d_a)$.*

*Det faktum att ett meddelande krypterat med $(n_A, d_A)$ kan dekrypteras med $(n_A, k_A)$ följer av att om $[d_A]_{m_A} = [k_A]_{m_A}^{-1}$ så är $[k_A]_{m_A} = [d_A]_{m_A}^{-1}$, dvs. de publika och privata nycklarna är utbytbara.*

## Ett färgningsproblem

*Antag att man har 6 bollar. På hur många sätt kan man färga 2 bollar svart och resten vita?*

- *Om bollarna är identiska finns det bara ett sätt, 2 blir svarta och 4 vita.*
- *Om bollarna är numrerade finns det* $\binom{6}{2} = 15$ *sätt att välja ut de som skall bli svarta och resten vita.*
- *Om bollarna ligger i hörnen på en reguljär 6-hörning och man kan vända och vrida på 6-hörningen finns det 3 alternativ som är:*



*Hur skall man lösa mera komplicerade problem av den tredje typen? Observera också att "färgning" inte skall tas för bokstavligt: Bilderna ovan kan också tex. representera tre isomerer av xylen* ($C_8H_{10}$) *där två väteatomer i bensen bytts ut mot metylgrupper.*



## Grupper

*En grupp är ett par* $[G, \bullet]$ *där* $G$ *är en mängd och* $\bullet$ *en funktion* $G \times G \to G$ *så att*

- *Slutenhet:* $x \bullet y \in G$ *ifall* $x$ *och* $y \in G$. *(En följd av att* $\bullet$ *är en funktion* $G \times G \to G$.*)*
- *Associativitet:* $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ *ifall* $x$, $y$ *och* $z \in G$.
- *Identitetselement: Det finns ett element* $e \in G$ *(som visar sig vara entydigt) så att* $e \bullet x = x \bullet e = x$ *ifall* $x \in G$.
- *Inverst element: Om* $x \in G$, *så finns det ett element* $x' \in G$ *så att* $x \bullet x' = x' \bullet x = e$.

## Obs!

- *Man säger ofta att "G är en grupp" om det är klart vad gruppoperationen är eller om det inte har så stor betydelse.*
- *Istället för att skriva* $x \bullet y$ *(eller ens* $\bullet(x, y)$*) kan man skriva* $xy$ *och eftersom man kan visa att det inversa elementet är entydigt så skrivs det ofta som* $x^{-1}$. *Identitetselementet kan också skrivas som* 1 *eller* $I$, *beroende på sammanhanget.*

## Kommutativa eller abelska grupper

*Om $[G, \bullet]$ är en grupp så att $a \bullet b = b \bullet a$ för alla $a$ och $b \in G$ så sägs gruppen vara* **kommutativ** *eller* **abelsk**. *I detta fall använder man ofta $+$ som beteckning för gruppeoperationen, $0$ som identiteselement och $-a$ för inversen av $a$.*

## Delgrupper

*Antag att $G$ (dvs. $[G, \bullet]$) är en grupp. En icke-tom delmängd $H$ av $G$ är en delgrupp av $G$ om följande villkor gäller och då är $H$ (egentligen $[H, \bullet]$) också en grupp:*

- *Om $x$ och $y \in H$ så gäller $x \bullet y \in H$.*
- *Om $x \in H$ så gäller $x^{-1} \in H$.*

*Om $H$ är ändlig så följer det senare villkoret av det första eftersom $x^m \in H$ för alla $m \geq 1$ och eftersom $|H| < \infty$ så finns det ett tal $m > k \geq 1$ så att $x^m = x^k$ men då är $x^{m-k} = e$ och då är antingen $x = e$ om $m = k + 1$ eller så är $m > k + 1$ och då är $x^{-1} = x^{m+k-1} \in H$.*



## Homomorfismer och isomorfismer

*Antag att $[G_1, \bullet_1]$ och $[G_2, \bullet_2]$ är två grupper och $\psi$ är en funktion: $G_1 \to G_2$.*

- *$\psi$ är en* **homomorfism** *ifall $\psi(x \bullet_1 y) = \psi(x) \bullet_2 \psi(y)$ för alla $x$ och $y \in G_1$.*
- *$\psi$ är en* **isomorfism** *ifall den är en homomorfism och en bijektion (och då är också $\psi^{-1}$ en homomorfism).*

*Det är inget speciellt med grupper här, det är frågan om att en homoformism "bevarar strukturen"!*

## Cykliska grupper

*En grupp $G$ är cyklisk om det finns ett element $x \in G$ så att varje element i $G$ är någon potens $x^j$ av $x$ där $j \in \mathbb{Z}$. I detta fall säger man att $G$ genereras av $x$ och man skriver $G = \langle x \rangle$.*
*Om $G$ är en grupp och $x \in G$ så är gruppen $\langle x \rangle = \{ x^j : j \in Z \}$ genererad av $x$ en delgrupp av $G$.*
*Eftersom alla cykliska grupper med $m$ element är isomorfa så betecknar man en sådan grupp med $C_m$.*

## En grupps och ett elements ordning

*Antag att $G$ är en grupp.*

- *Gruppen $G$:s ordning är antalet element $|G|$ i gruppen.*
- *Ett elements $g \in G$ ordning är $\inf\{ j \geq 1 : g^j = e \}$ och detta är ordningen av den cykliska gruppen genererad av $g$.*

## Permutationer

*En* **permutation** *av en (ändlig) mängd $A$ är en bijektion $A \to A$.*

- *Mängden av alla permutationer av en mängd $A$ är en grupp då gruppoperationen är sammansättning av funktioner. Eftersom alla grupper av permutationer av någon mängd med $m$ element är isomorfa så betecknar man en sådan grupp med $S_m$.*
- *Varje grupp $[G, \bullet]$ är isomorf med en delgrupp av gruppen av permutationer av en mängd, eftersom mängden kan tas som $G$ och isomorfin som $\psi(a)(b) = a \bullet b$ men detta betyder inte att det alltid är nyttigt eller nödvändigt att tänka på gruppen på dethär sättet.*



## Permutationer, banor, cykelnotation

*Antag att $A$ är en ändlig (icke-tom) mängd.*

- *Om $\alpha$ är en permutation av $A$ så är $\alpha$:s* **banor** *minsta möjliga delmängder $A_j \subset A$, $j = 1, 2, \ldots m$ så att $A_j \cap A_k = \emptyset$ då $j \neq k$, $\cup_{j=1}^m A_j = A$ och $\alpha(A_j) = \{ \alpha(x) : x \in A_j \} = A_j$.*
- *En* **cykel** *är en permutation $\alpha$ så att $\alpha(x_j) = x_{j+1}$, $j = 1, 2, \ldots, k-1$ och $\alpha(x_k) = x_1$ där $x_1, x_2, \ldots, x_k \in A$ och $\alpha(x) = x$ för alla $x \in A \setminus \{x_1, \ldots, x_k\}$. Cykeln $\alpha$ skrivs med* **cykelnotation** *som $\alpha = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}$.* **Längden** *av en sådan cykel $\alpha$ är $k$ och $\alpha$ sägs vara en $k$-cykel. Cykeln $\alpha$:s banor är $\{x_1, x_2, \ldots, x_k\}$ och mängderna $\{x\}$ för alla $x \in A \setminus \{x_1, \ldots, x_k\}$.*
- *Varje permutation kan skrivas som en produkt av cyklar som motsvarar banorna med minst 2 element (och identitetselementet).*

## Obs!

*Permutationen $\alpha$:s banor kan också definieras som ekvivalensklasserna för en relation där $x \sim y$ ifall $\alpha^j(x) = y$ för något $j \in \mathbb{Z}$.*

## Jämna och udda permutationer

- *Varje cykel med längden $k \geq 2$ kan skrivas som produkten av $k-1$ cykler med med längden 2 eftersom* $(x_1 \quad x_2 \quad \dots \quad x_k) = (x_1 \quad x_k)(x_1 \quad x_{k-1}) \dots (x_1 \quad x_3)(x_1 \quad x_2)$.
- *Varje permutation kan skrivas som en produkt av cykler med längden 2 (och 1).*
- *En permutation kan i allmänhet skrivas på flera sätt som en produkt av cykler med längden 2 men om permutationen $\alpha$ kan skrivas som en produkt av $r$, och som en produkt av $r'$, cykler med längden 2 så är $(-1)^r = (-1)^{r'}$ och därför kan man definiera cykelns* **tecken** *med* $\operatorname{sign}(\alpha) = (-1)^r$.
- *Om $\alpha$ är en cykel med längden $k$ så är* $\operatorname{sign}(\alpha) = (-1)^{k+1}$.
- *Om $\alpha$ är en permutation av en mängd med $n$ element och $\alpha$ har $m$ banor så är* $\operatorname{sign}(\alpha) = (-1)^{n-m}$.
- *En permutation $\alpha$ sägs vara* **jämn** *om* $\operatorname{sign}(\alpha) = 1$ *och* **udda** *annars.*
- *Om $\alpha$ och $\beta$ är permutationer av samma mängd så är* $\operatorname{sign}(\alpha\beta) = \operatorname{sign}(\alpha)\operatorname{sign}(\beta)$.



## Sidoklasser

*Antag att $G$ är en grupp, $H$ är en delgrupp i $G$ och $a \in G$.*

- *Mängden $aH = \{ ax : x \in H \}$ är den* **vänstra sidoklassen** *av $H$ som innehåller $a$.*
- *Mängden $Ha = \{ xa : x \in H \}$ är den* **högra sidoklassen** *av $H$ som innehåller $a$.*

*Sidoklasserna har följande egenskaper (som här endast formulerats för de vänstra sidoklasserna):*

- $|aH| = |H|$ *för alla $a \in G$.*
- *Om $a$ och $b \in G$ så är antingen $aH = bH$ eller $aH \cap bH = \emptyset$.*
- $\cup_{a \in G} aH = G$.
- *Om $a$ och $b \in G$ och $aH = bH$ så gäller $b^{-1}a \in H$.*
- $|G| = |H| \cdot |\{ aH : a \in G \}|$ *och därför delar talet $|H|$ talet $|G|$.*

## Homomorfismer, normala delgrupper och kvotgrupper

*Antag att $G$ är en grupp.*

- *Om $G'$ är en grupp med identitetselement $e'$ och $\psi : G \to G'$ är en homomorfism så är $H = \{ x \in G : \psi(x) = e' \}$ (kärnan av $\psi$) en delgrupp i $G$.*
- *En delgrupp $H$ i $G$ har formen $\{ x \in G : \psi(x) = e' \}$ för någon homomorfism $G \to G'$ om och endast om $aH = Ha$ för alla $a \in G$ (eller ekvivalent, $axa^{-1} \in H$ för alla $a \in G$ och $x \in H$). I detta fall säger man att $H$ är en* **normal** *delgrupp.*
- *Om $H$ är en normal delgrupp i $G$ så bildar sidoklasserna (med de vänstra och högra indentiska) en* **kvotgrupp**, *som betecknas med $G/H$, och som har gruppeoperationen operation $(aH)(bH) = (ab)H$, identitetselement $H$ och invers $(aH)^{-1} = a^{-1}H$. Funktionen $\psi : G \to G/H$ definierad med $\psi(a) = aH$ är en homomorfism med kärna $H$.*



## Gruppverkan

*Om $G$ dvs. $[G, \bullet]$ är en grupp och $X$ är en mängd så är* **gruppverkan** *av $G$ på mängden $X$ en homomorfism från $G$ till gruppen av permuationer: $X \to X$. Om man definerar sammansatta funktioner med $(f \circ g)(x) = f(g(x))$ så får man en* **vänstergruppverkan** *och om man definierar den med $x.(f \circ g) = (x.f).g$ så får man en* **högergruppverkan** *. Istället för att skriva $\psi(a)(x)$ där $\psi$ är homomorfismen, $a \in G$ och $x \in X$ skriver man ofta $ax$ och säger att $G$* **verkar** *på $X$. För en vänstergruppverkan blir homomorfismegenskapen då $(ab)x = a(bx)$, $a, b \in G$, $x \in X$.*

## Obs!

*Om $G$ är en grupp permutationer av $X$ så är identititetsavbildningen homomorfismen och hela begreppet gruppverkan behövs inte.*
*Om $G$ är en grupp kan man definiera dess gruppverkan på sig själv tex. med $\psi(a)(x) = ax$ (en vänstergruppverkan), med $\psi(a)(x) = axa^{-1}$ (en vänstergruppverkan), med $\psi(a)(x) = xa$ (en högergruppverkan) eller med $\psi(a)(x) = a^{-1}xa$ (en högergruppverkan).*

## Banor och stabilisatorer

*Antag att $G$ är en grupp som verkar på en mängd $X$ (från vänster).*

- *Om $x \in X$ så är dess* **bana** *under verkan av $G$ mängden $Gx = \{ gx : g \in G \} \subset X$.*
- *Om $x \in X$ så är dess* **bana** *under verkan av ett element $g \in G$ mängden $\langle g \rangle x = \{ g^j x : j \in \mathbb{Z} \} \subset X$. ($\langle g \rangle$ är den cykliska gruppen genererad av $g$.)*
- *Om $x \in X$ så är dess* **stabilisator** *under verkan av $G$ mängden $G_x = \{ g \in G : gx = x \}$ som är en delgrupp i $G$.*

*För varje $x \in X$ gäller $|Gx| \cdot |G_x| = |G|$.*

## Obs!

*Om $G$ verkar på $X$ så kan man definiera en ekvivalensrelation $\sim$ i $X$ med $x \sim y$ om och endast om $x = gy$ för något $g \in G$. Banorna är då ekvivalensklasserna och ofta kan det vara nyttigt att tänka på element i samma ekvivalensklass som om de vore desamma.*



## Cykelindex

**Cykelindexet** *för en permutation $g$ av $X$ eller ett element $g$ i en grupp som verkar på $X$ är monomet*

$$\zeta_{g,X}(t_1, \ldots, t_n) = t_1^{j_1} \cdot t_2^{j_2} \cdot \ldots \cdot t_n^{j_n}$$

*där $j_k$ är antalet banor med längden $k$ under verkan av $g$.*
**Cykelindexet** *för en grupp $G$ av permutationer av $X$ eller en grupp $G$ som verkar på $X$ är*

$$\zeta_{G,X}(t_1, \ldots, t_n) = \frac{1}{|G|} \sum_{g \in G} \zeta_{g,X}(t_1, \ldots, t_n).$$

## Antalet banor under verkan av en grupp (Burnsides lemma)

*Antag att (den ändliga) gruppen $G$ verkar på mängden $X$. Definiera för varje $g \in G$ mängden $X_g$ av* **fixpunkter** *till $g$ med*

$$X_g = \{ x \in X : gx = x \}.$$

*(Denhär mängden betecknas ibland också med $X^g$ eller $F(g)$.) Då är antalet banor i $X$ under verkan av $G$*

$$\frac{1}{|G|} \sum_{g \in G} |X_g|.$$



## Gruppverkan och "färgningar"

*Antag att gruppen $G$ verkar på en mängd $X$. En "färgning" av $X$ är en funktion $\omega : X \to K$ där $K$ är en mängd "färger". Gruppen $G$ verkar på mängden $K^X$ av alla färgningar med $(g\omega)(x) = \omega(g^{-1}x)$.*
*Detta är en vänstergruppverkan eftersom*

$$(g(h\omega))(x) = (h\omega)(g^{-1}x) = \omega(h^{-1}g^{-1}x) = \omega((gh)^{-1}x) = ((gh)\omega)(x).$$

*Om $\Omega \subset K^X$ är en delmängd av mängden färgningar av $X$ så verkar $G$ på $\Omega$ förutsatt att $G\Omega = \Omega$.*
*Gruppverkan av $G$ på en mängd färgningar bestämmer en ekvivalensrelation så att färgningar som hör till samma bana i $G$:s verkan på $\Omega$ är ekvivalenta, dvs. $\omega \sim \eta$ om och endast om $\omega = g\eta$ för något $g \in G$ och då kan man anse att dessa färgningar är desamma.*
*Således är antalet färgningar i $\Omega$ som inte är ekvivalenta under verkan av $G$ enligt resultatet om antalet banor*

$$\frac{1}{|G|} \sum_{g \in G} |\Omega_g|$$

*där $\Omega_g = \{ \omega \in \Omega : g\omega = \omega \}$ är mängden av färgningar fixpunkter till $g$.*

## Vilka färgningar är invarianta under verkan av ett gruppelelement $g$?

*Antag att gruppen $G$ verkar på mängden $X$. Antag att $g \in G$ och att $A_{g,1}, A_{g,2}, \ldots A_{g,m_g}$ är banorna i $X$ under verkan av $g$, dvs. banorna i gruppverkan av den cykliska gruppen $\{ g^j : j \in \mathbb{Z} \}$ på $X$.*
*Om $\omega$ är en färgning av $X$ (dvs. en funktion: $X \to K$ där $K$ är en mängd färger) då är $g\omega = \omega$ om och endast om $\omega$ är konstant på varje bana $A_{g,j}$, $j = 1, \ldots, m_g$.*

## Varför?

*Eftersom $g\omega = \omega$ så gäller $g^j\omega = \omega$ för alla $j \in \mathbb{Z}$. Om nu $x$ och $y$ hör till samma bana under verkan av $g$ så finns det ett tal $j$ så att $g^j x = y$ eller $g^{-j} y = x$. Enligt definitionen av gruppverkan på färgningar $((g\omega)(x) = \omega(g^{-1}x))$ och det faktum att $g^j\omega = \omega$ så får vi*

$$\omega(y) = (g^j\omega)(y) = \omega(g^{-j}y) = \omega(x).$$

*Om igen $\omega$ är konstant på alla banor så är $\omega(x) = \omega(g^{-1}x)$ för alla $x \in X$. Detta betyder att $\omega(x) = (g\omega)(x)$ för alla $x$, dvs. $\omega = g\omega$.*



## Pólyas teorem om antalet "färgningar"

*Antag att gruppen $G$ verkar på mängden $X$ och låt $K^X$ vara mängden av färgningar av $X$ med "färgerna" $K = \{a_1, a_2, \ldots, a_r\}$. Då är koefficienten av monomet*

$$a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_r^{i_r}$$

*i polynomet*

$$\zeta_{G,X}(a_1^1 + \ldots + a_r^1, a_1^2 + \ldots + a_r^2, \ldots, a_1^n + \ldots + a_r^n)$$

*antalet färgningar av $X$ som använder färgen $a_j$ exakt $i_j$ gånger (dvs. $|\{ x : \omega(x) = a_j \}| = i_j$) och som inte är ekvivalenta under verkan av $G$.*

*Om man använder $r$ färger men inte har andra begränsingar så är $\zeta_{G,X}(r, r, \ldots, r)$ antalet färgningar av $X$ som inte är ekvivalenta under verkan av $G$.*

## Grafer

- *En riktad graf $G = [V, E]$ består av en mängd $V$ vars element är noder (eller hörn) och en mängd $E$ av bågar (eller kanter) som (i det riktade fallet) är en delmängd av $V \times V$ (dvs. en relation i $V$).*
- *En (icke-riktad) graf $G = [V, E]$ består av en mängd $V$ vars element är noder (eller hörn) och en mängd $E$ av bågar (eller kanter) som vars element är delmängder av $V$ med 1 eller 2 element.*
- *En enkel graf $G = [V, E]$ är en icke-riktad graf i vilken bågarna i $E$ är delmängder av $V$ med exakt två element.*

*Antalet element i $V$ antas vanligen vara positivt men ändligt.*

## Obs!

*Om $V = \{v_1, v_2, \ldots v_m\}$ och $[V, E]$ är en enkel graf så kan mängden $\{v_j, v_j\} = \{v_j\}$ inte höra till $E$ eftersom den innehåller bara ett element och detta innebär att i en enkel graf finns det ingen båge mellan en nod och den själv, en sk. ögla eller loop. I alla graferna som här behandlas kan det finns högst en båge mellan två noder.*



## Definitioner

*Antag att $G = [V, E]$ är en graf.*

- *En **väg** i $G$ är en följd $[v_0, v_1, \ldots, v_n]$ där $v_j$, $j = 0, 1, \ldots, n$ är noder i $G$ (dvs. $v_j \in V$) och för varje $j = 1, \ldots, n$ finns det en båge i $G$ mellan $v_{j-1}$ och $v_j$, (dvs. $\{v_{j-1}, v_j\} \in E$ eller $[v_{j-1}, v_j]$ i det riktade fallet).*
- ***Längden** av vägen $[v_0, v_1, \ldots, v_n]$ i $G$ är $n$.*
- *En **cykel** (eller krets) i $G$ är en väg $[v_0, v_1, \ldots, v_n]$ i $G$ så att $v_n = v_0$.*
- *En väg $[v_0, v_1, \ldots, v_n]$ i $G$ är **enkel** om ingen nod i vägen upprepas (dvs. $v_j \neq v_k$ då $0 \leq j < k \leq n$).*
- *En cykel $[v_0, v_1, \ldots, v_0]$ i $G$ är **enkel** om vägen $[v_0, v_1, \ldots, v_{n-1}]$ är enkel.*
- *En **Euler**-väg (eller -cykel) i $G$ är en väg (eller cykel) i $G$ så att vägen eller cykeln går genom varje båge precis en gång (dvs. $\cup_{j=1}^{n} \{v_{j-1}, v_j\} = E$ och $\{v_{j-1}, v_j\} \neq \{v_{k-1}, v_k\}$ då $1 \leq j < k \leq n$).*
- *En **Hamilton**-väg (eller -cykel) i $G$ är en enkel väg (eller cykel) i $G$ så att vägen eller cykeln går genom varje nod, frånsett startnoden i*

## Definitioner, forts.

- *En graf är* **sammanhängande** *om det finns en väg från varje nod till varje annan nod.*
- *En graf är ett* **träd** *om det finns exakt en enkel väg från varje nod till varje annan nod.*
- *En graf är en* **skog** *om det finns högst en enkel väg från varje nod till varje annan nod.*
- *En graf är* **bipartit** *med delarna $X$ och $Y$ om $V = X \cup Y$, $X \cap Y = \emptyset$ och $E \subset \{\, \{x, y\} : x \in X, y \in Y \,\}$.*
- *En* **matchning** *i en graf är en mängd bågar $M \subset E$ så att två olika bågar i $M$ inte har någon gemensam ändnod, dvs. om $e_1 = \{v_1, v_1'\}$ och $e_2 = \{v_2, v_2'\}$ och $e_1 \neq e_2$ så är $e_1 \cap e_2 = \emptyset$.*
- *I en* **nodfärgning** *av en graf får noder som är grannar olika färg, dvs. färgningen är en funktion $\omega : V \to K$ så att $\omega(v_j) \neq \omega(v_k)$ om $\{v_j, v_k\} \in E$. Det* **kromatiska** *talet för en graf är minimiantalet färger som behövs för en nodfärgning.*



## Girig nodfärgning

*Ett enkelt men inte nödvändigtvis optimalt sätt att bestämma en nodfärgning är följande giriga algoritm:*

- *Sätt noderna i någon ordning: $[v_1, v_2, \ldots, v_n]$.*
- *Sätt färgerna i någon ordning: $[a_1, a_2, \ldots, a_r]$.*
- *Färga den första noden med den första färgen, dvs. $\omega(v_1) = a_1$.*
- *Om noderna $v_1, \ldots, v_k$ är färgade så färga $v_{k+1}$ med den första färg som kan användas så att villkoret att grannar inte får samma färg uppfylls, dvs. $\omega(v_{k+1}) = a_j$ där $j = \min\{\, i \geq 1 : \{v_p, v_{k+1}\} \in E \;\&\; p \leq k \to \omega(v_p) \neq a_i \,\}$.*

## Grannmatris

*Om $G = [V, E]$ är en graf med $m$ noder $V = \{v_1, \ldots v_m\}$ så är dess grannmatris den $m \times m$-matris för vilken gäller*

$$A(j,k) = \begin{cases} 1, & \{v_j, v_k\} \in E, \\ 0, & \{v_j, v_k\} \notin E. \end{cases}$$

*Om $n \geq 1$ och $B = A^n$ så är $B(j,k)$ antalet vägar från nod $v_j$ till nod $v_k$ med längden $n$.*

## Bipartita grafer och matchningar

*Om $G = [X \cup Y, E]$ är en bipartit graf (med delarna $X$ och $Y$) så finns det en matchning $M$ i $G$ så att varje $x \in X$ är ändnod för någon båge i $M$, dvs. en sk. fullständig matchning*
*om och endast om det är sant att*
*för varje $A \subset X$ är antalet noder i $A$ mindre eller lika med antalet noder i $Y$ som är granne med någon nod i $A$.*



## Minimalt uppspännande träd, girig algoritm

*Om $G = [V, E]$ är en sammanhängande graf så att varje båge $\{v_j, v_k\}$ har getts en vikt $w(\{v_j, v_k\})$ (och $w(\{v_j, v_k\}) = \infty$ ifall $\{v_j, v_k\} \notin E$) så är det minimalt uppsännande trädet en delgraf $T = (V, E_T)$ (dvs. $E_T \subset E$) som är ett träd och sådan att $\sum_{\{v_j, v_k\} \in E_T} w(v_j, v_k)$ är så litet som möjligt. Ett sätt att konstruera ett minimalt uppspännande träd är att använda följande giriga algoritm (Prims algoritm):*

- *Låt $T_1 = [\{v_1\}, \emptyset]$ där $v_1$ är en godtyckligt vald nod (dvs. $T_1$ är en graf som bara innehåller en nod och ingen båge).*
- *Om man redan bestämt $T_m = [V_m, E_m]$ så väljer man $v_j \in V_m$ och $v_k \in V \setminus V_m$ så att $w(\{v_j, v_k\})$ är så litet som möjligt och sedan $T_{m+1} = [V_m \cup \{v_k\}, E_m \cup \{\{v_j, v_k\}\}]$, dvs. man lägger till noden $v_k$ och bågen mellan $v_j$ och $v_k$ till $T_m$ för att få $T_{m+1}$.*

## Dynamisk optimering och grafer

*Antag att* $G = [V, E]$ *är en enkel sammanhängande graf så att varje båge* $e \in E$ *har getts en vikt* $w(e) \geq 0$ *(och* $w(\{v_j, v_k\}) = \infty$ *ifall* $\{v_j, v_k\} \notin E$*). En fråga som ofta dyker upp hur man kan bestämma en väg* $[v_0, v_1, \ldots, v_n]$ *från en given nod* $v_0$ *till en annan given nod* $v_n$ *så att* $\sum_{j=1}^{n} w(\{v_{j-1}, v_j\})$ *är så liten som möjligt.*

- *Definiera* $s(v) = \min\{\sum_{j=1}^{k} w(\{v_{j-1}, v_j\} : [v_0, v_1, \ldots, v_k]$ *är en väg från* $v_0$ *till* $v_k = v\}$.
- *Observera att för funktionen* $s$ *gäller principen för* **dynamisk optimering**:
$$s(v) = \min_{v'}(s(v') + w(\{v', v\}).$$
- *Bestäm de optimala värdena* $s(v)$ *på följande sätt:*
  - *Låt* $V_0 = \{v_0\}$ *och* $s(v_0) = 0$.
  - *Om de optimala värden* $s(v)$ *är bestämda för* $v \in V_j$ *så beräknas testvärden för grannarna till* $V_j$ *i* $V \setminus V_j$ *med* $t(v) = \min_{v' \in V_j}(s(v') + w(\{v', v\})$.
  - *Låt* $V_{j+1} = V_j \cup \{v\}$ *och* $s(v) = t(v)$ *där* $t(v) = \min_{v' \in V \setminus V_j} t(v')$.