Största gemensamma faktorn

Definition: Låt $a, b \in \mathbb{Z}$, där båda talen inte är $= 0$. Största heltalet som delar både a och b kallas deras största gemensamma faktor (största gemensamma delare)

Beteckning: $sgf(a,b)$

- Fråga: Varför måste vi anta, att båda talen inte är noll?

Ex. För talen 24 och 30 är $sgf(24,30) = 6$

Motiveringen: Primtalsfaktorisering:

$$\left.\begin{array}{l} 24 = 2 \cdot 2 \cdot 2 \cdot 3 \\ 30 = 5 \cdot 2 \cdot 3 \end{array}\right\} \Rightarrow sgf(24,30) = 2 \cdot 3 = \underline{\underline{6}}$$

Annat sätt att hitta $sgf(24,30)$ är genom

Euklides algoritm:

$$30 = 1 \cdot 24 + 6$$
$$24 = 4 \cdot \underset{\substack{\uparrow \\ sgf(24,30)}}{6} + 0$$

Ex. Vi bestämmer sgf(110, 273) med Euklides algoritm:

$$273 = 2\cdot 110 + 53$$
$$110 = 2\cdot 53 + 4$$
$$53 = 13\cdot 4 + 1$$
$$4 = 4\cdot 1 + 0$$

$\text{sgf}(110, 273) = 1.$

Alternativt med primtalsfaktorering: $273 = 3\cdot 91 = 3\cdot 7\cdot 13$

$110 = 2\cdot 55 = 2\cdot 5\cdot 11$

inga gemensamma primtal $\Rightarrow$ $\text{sgf}(110, 273) = 1$

Sats: (Bezout) Låt $a, b \in \mathbb{Z}$ där båda talen inte är 0. Då $\exists\, x, y \in \mathbb{Z}$ för vilka

$$\boxed{\text{sgf}(a,b) = xa + yb}$$

$\square$

x och y hittas genom Euklides algoritm "baklänges".

Ex. Vi bestämmer $x, y \in \mathbb{Z}$ för vilka

$$\text{sgf}(110, 714) = 110x + 714y.$$

Vi bestämmer sgf med Euklides algoritm:

$$714 = 6 \cdot 110 + 54$$
$$110 = 2 \cdot 54 + 2$$
$$54 = 27 \cdot 2 + 0$$

$2 \leftarrow$ sgf(110,714)

Algoritmen "baklänges":

$$\text{sgf}(110,714) = 2 = 110 - 2 \cdot 54$$
$$= 110 - 2 \cdot (714 - 6 \cdot 110)$$
$$= \underline{13} \cdot 110 \underline{-2} \cdot 714$$

(Kontroll: $13 \cdot 110 - 2 \cdot 714 = 1430 - 1428 = \underline{\underline{2}}$)

Ex. Lös kongruensen $110x \equiv 42 \pmod{273}$.

(D.v.s. hitta talet $0 \leq a < 273$ för vilket

$110x \equiv 42 \pmod{273} \iff x \equiv a \pmod{273}$)

Anta, att $110x \equiv 42 \pmod{273}$. Genom Euklides algoritm fram och baklänges får man $\text{sgf}(110, 273) = 1$ och

$$1 = 27 \cdot 273 - 67 \cdot 110.$$

Eftersom $27\cdot 273 \equiv 0 \pmod{273}$

så gäller $\underbrace{27\cdot 273 - 67\cdot 110}_{=1} \equiv 0 - 67\cdot 110 \pmod{273}$

d.v.s. $1 \overset{(*)}{\equiv} -67\cdot 110 \pmod{273}$

Antagandet $\Rightarrow -67\cdot 110x \equiv -67\cdot 42 \pmod{273}$

Alltså $x \overset{(*)}{\equiv} \underbrace{-67\cdot 42}_{-2814} \pmod{273}$

$-2814 \equiv 189 \pmod{273}$: $-2814 = -11\cdot 273 + 189$
$189 = 0\cdot 273 + 189$ Samma rest

Alltså $x \equiv 189 \pmod{273}$.

$\therefore\ 110x \equiv 42 \pmod{273} \Rightarrow x \equiv 189 \pmod{273}$

"$\Leftarrow$" Anta, $x \equiv 189 \pmod{273}$.

Då gäller $110x \equiv \underbrace{110\cdot 189}_{20790} \pmod{273}$

$20790 \equiv 42 \pmod{273}$: $20790 = 76\cdot 273 + 42$
$42 = 0\cdot 273 + 42$ Samma rest

$\therefore\ 110x \equiv 42 \pmod{273}$

$\therefore\ 110x \equiv 42 \pmod{273} \Leftrightarrow x \equiv 189 \pmod{273}$.

Grafer

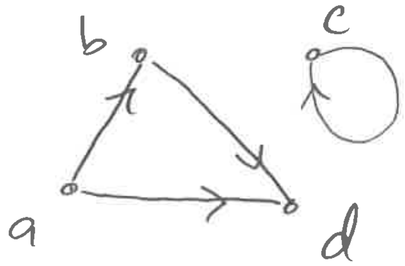
Definition: En graf $\mathcal{G}$ är paret (G, E) där

$G \neq \emptyset$ är en mängd vars element kallas för grafens **noder**. och $E \subset G \times G$ (dvs. E är en relation på G)

Om $(a,b) \in E$ så säger vi att det finns en båge från noden a till noden b.

Ex. En riktad graf:

$\mathcal{G}$:



Här är $G = \{a, b, c, d\}$ och $E = \{(a,b), (a,d), (b,d), (c,c)\}$

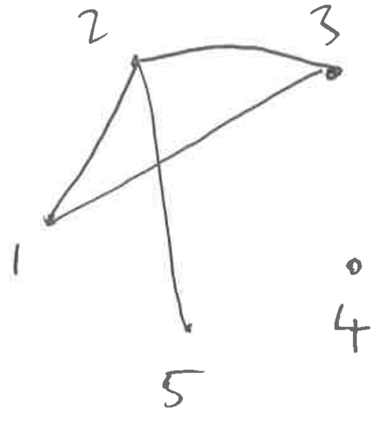
$(a,b) \in E$: b är granne till a (annan beteckning: $a \to b$)

$(c,c) \in E$: det finns en ögla (eller loop) i noden c.

$(b,a) \notin E$: a är inte granne till b.

<u>Ex</u>. En <u>oriktad</u> graf

$\mathcal{G}$:



$G=\{1,2,3,4,5\}$

$E=\{(1,2),(2,1),(2,3),(3,2),(1,3),(3,1),(2,5),(5,2)\}$

($\mathcal{G}$ oriktad = E symmetrisk relation)

Graden av en nod = antalet bågar till noden

$\deg(1)=2=\deg(3)$

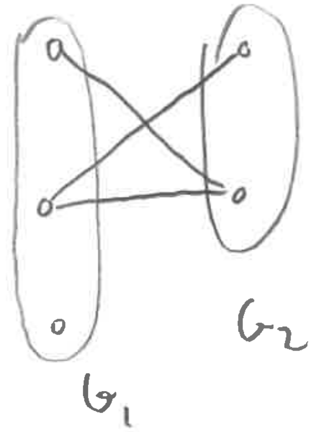
$\deg(2)=3$, $\deg(4)=0$, $\deg(5)=1$

Anta, att $\mathcal{G}=(G,E)$ är en oriktad graf utan öglor.

$\mathcal{G}$ är <u>tudelad</u> om $\exists G_1, G_2$ så att $G=G_1\cup G_2$ och $G_1\cap G_2=\emptyset$

och varje båge går från G_1 till G_2.

$\mathcal{G}$

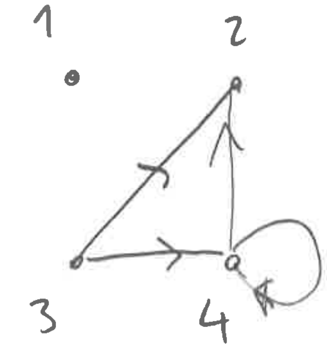


tudelad.

Sats. En oriktad graf utan öglor är tudelad $\iff$ noderna kan färgläggas med **två** färger så att grannar alltid har olika färger.

Låt G vara en graf. Grafens **grannmatris** A är matrisen där
$$A(i,j) = \begin{cases} 1, & \text{om } (i,j) \in E \\ 0, & \text{annars.} \end{cases}$$

Ex. G:

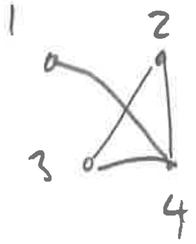


$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

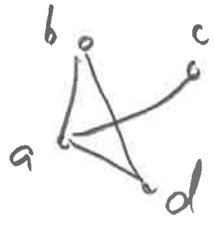
Anta, att $G_1 = (G_1, E_1)$ och $G_2 = (G_2, E_2)$ är oriktade grafer utan öglor. G_1 och G_2 är **isomorfa** om det finns en bijektion $f: G_1 \to G_2$ för vilken följande gäller:

$$(a,b) \in E_1 \iff (f(a), f(b)) \in E_2.$$

Ex. G_1:



G_2:



$$\boxed{G_1 \cong G_2}$$

Låt $\mathcal{G}=(G,E)$ vara en graf, och $v_1,v_2,\dots,v_n\in G$

(Den ändliga) Följden $v_1,v_2,\dots,v_n$ är en <u>stig</u> om

$$(v_1,v_2)\in E,\ (v_2,v_3)\in E,\ \dots,\ (v_{n-1},v_n)\in E.$$

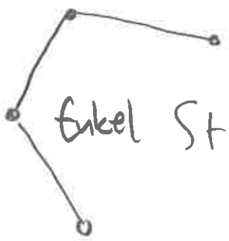
Stigens längd = antalet bågar $n-1$

Stigen $v_1,\dots,v_n$ är <u>enkel</u> om $v_i\neq v_j$ för varje

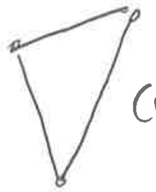
$1<i,j<n$, $i\neq j$.

Om $v_1=v_n$ för en enkel stig $v_1,\dots,v_n$ så är stigen <u>cyklisk</u>. En oriktad graf är <u>sammanhängande</u> om det finns en stig mellan varje nod.

<u>Ex.</u>

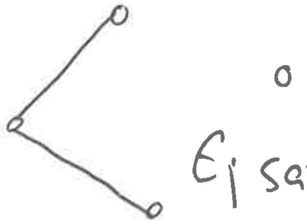


Enkel Stig



Cyklisk stig

Sammanhängande graf



Ej sammanhängande