Sammanfattning av modul 1

Division med rest:

Om p, d är heltal, $d \neq 0$ så finns entydiga heltal q, r så att
$p = qd + r, \; 0 \leq r < |d|$.

q kallas kvoten av p och d.
r kallas (den principala) resten.

Ett (naturligt) tal kan skrivs i bas t ($t \geq 2$):

$$
\begin{aligned}
x &= q_0 t + r_0 \\
q_0 &= q_1 t + r_1 \\
&\vdots \\
q_{n-2} &= q_{n-1} t + r_{n-1} \\
q_{n-1} &= q_n t + r_n
\end{aligned}
$$

$x = (r_1 r_2 \ldots r_{n-1} r_n)_t$ $\quad r_i$ är siffror.

t = 2 ger binär form	siffror:	01
t = 8 ger oktal form	siffror:	01234567
t = 10 ger decimal form	siffror:	0123456789
t = 16 ger hexadecimal form	siffror:	0123456789ABCDEF
	eller	0123456789abcdef

Andra, kanske bättre, siffror för A, B, C, D, E, F har funnits förr.

I andra baser än 10 ska siffrorna uttalas
separat (10 = ett noll, inte tio).

Om a, b är heltal betyder $a \mid b$ (”a delar b”) att $b = qa$, q heltal.

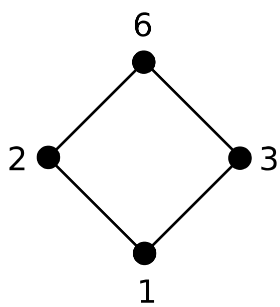
Ett primtal är ett heltal $p > 1$ som bara har delarna ± 1, $\pm p$.

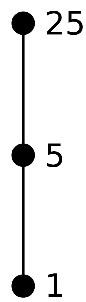
Största gemensam delare (sgd, gcd på engelska):

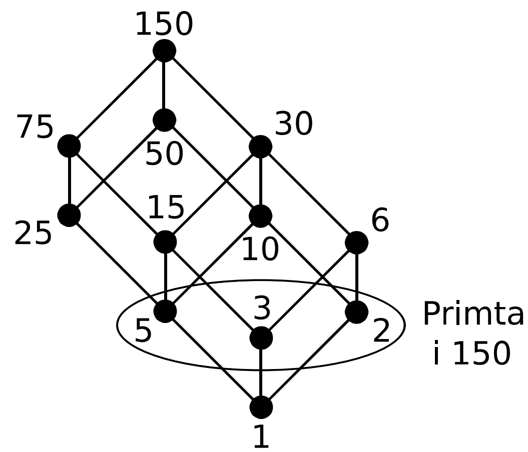
Största d så att $d|m$ och $d|n$.
Ger att $d = am + bn$ a, b heltal.
$\text{sgd}(m; n) = \text{sgd}(n; m) = \text{sgd}(\pm_n n, \pm_m m)$

Delargrafen för ett heltal $g > 0$:

Punkter svarar mot all talets delare,
uppåtriktade strck från “direkta delare”



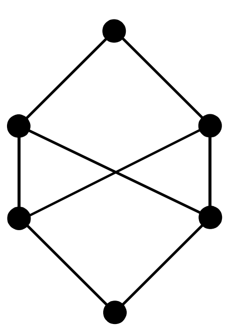




En gemensam delare till m, n i en delargraf:

Ett tal ligger under båda

Att del finns en entydig största gemensamma delare ger ett villkor på hur delargrafen kan se ut.



Finns ingen sådan delargraf.
Ty 0 saknar sgd.

Euklides' algoritm:

$\text{sgd}(m; n) = \text{sgd}(n; m - qn) \qquad$ heltal q

Detta medför:

$$
\begin{array}{ll}
m = q_1 n + r_1 & 0 \le r_1 < n \\
n = q_2 r_1 + r_2 & 0 \le r_2 < n \\
r_1 = q_3 r_2 + r_3 & 0 \le r_3 < n \\
\quad\vdots & \quad\vdots \\
r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & \\
r_{k-2} = q_k r_{k-1} + 0 &
\end{array}
$$

$\text{sgd}(m; n) = r_{k-1}$

Två heltal, m och n, är relativt prima om $\text{sgd}(m; n) = 1$. Alltså om $m \nmid n$ och $n \nmid m$.

Minsta gemensam multipel (mgm, lcm på engelska):

$\text{mgm}(a; b) = m$ så att $a | m$ och $b | m$, minsta m.

$\text{mgm}(a; b) \cdot \text{sgd}(a; b) = ab$

En diofantisk ekvation är en ekvation där endast heltalslösningar sökes.

Den linjära diofantiska ekvationen

$ax + by = c \qquad$ a, b, c heltal

är lösbar omm (om och endast om; precis om; exakt om) $\text{sgd}(a; b) \mid c$.

Om lösbar, men inte $a = b = 0$, och $\text{sgd}(a; b) = d = ma + nb$, m, n heltal

så ges alla lösningar av $\begin{cases} x = \frac{c}{d} m + \frac{b}{d} q \\ y = \frac{c}{d} n - \frac{a}{d} q \end{cases}$, $\quad q$ hetal.

Aritmetikens fundamentalsats:

Alla positiva heltal (större än 1) kan faktoriseras
till en unik mängd av (icke-unika) primtal.
(1 är “den tomma produkten”.)

Om $a = p_1^{s_1} \dots p_k^{s_k}$, $b = p_1^{t_1} \dots p_k^{t_k}$ så är

$sgd(a; b) = p_1^{\min(s_1; t_1)} \dots p_1^{\min(s_1; t_k)}$ och $mgm(a; b) = p_1^{\max(s_1; t_1)} \dots p_1^{\max(s_1; t_k)}$

Modulär aritmetik:

$x \equiv y \pmod{m}$ eller $x \equiv_m y$ eller $x = y$ i $\mathbb{Z}_m$

(Sista bara för heltal, för andra mängder måste man byta ut $\mathbb{Z}$.)

betyder $m|(x - y)$, och läses “x är kongruent med y modulo m”.

$x_1 \equiv_m x_2,\ y_1 \equiv_m y_2 \Rightarrow x_1 + y_1 \equiv_m x_2 + y_2,\ x_1 y_1 \equiv_m x_2 y_2$

r i $\mathbb{Z}_m$ är inverterbart om $x \in \mathbb{Z}_m$ så att $rx = 1$ i $\mathbb{Z}_m$.
$x = r^{-1}$ r:s invers.
r är inverterbart omm $sgd(r; m) = 1$ (i $\mathbb{Z}_m$).

Om m är ett primtal så är alla tal utom 0 inverterbart.

En mängd kan ses som en ”pås” med ”saker” (eller pekare till saker), dessa ”saker” kallas element.

Två mängder är lika omm de innehåller samma element.
Elementen i en mängd är oordnade.

$\{1, 2\}$ är mängden med talen 1 och 2.
$\{x \mid Px\}$ är mängden av alla tal med egenskapen P, till exempel:
$\{x \mid x > 4\}$ är mängden med alla tal som är strikt större än 4.

Den tomman mängden är mängden utan element, och betecknas $\emptyset$
$\emptyset = \{x \mid x \neq x\} = \{\}$.

$\{\emptyset\} \neq \emptyset$, $\emptyset$ är tom, $\{\emptyset\}$ är mängden som innehåller den tomma mängden.

Universum, $\mathcal{U}$, är grundmängden med alla element vi sysslar med.

Standardbeteckningar för olika talmängder: $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Z}_+$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

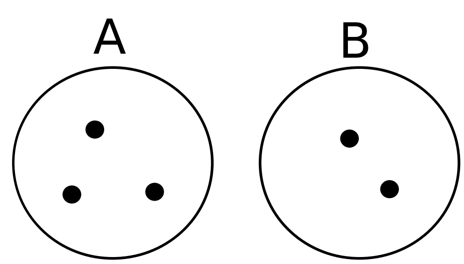
$a \in A$	a är ett element i A.	
$a \notin A$	a är ett inte element i A.	
$B \subseteq A$	B är en delmängd av A.	Alla element i B finns i A.
$B \subset A$	B är en äkta delmängd av A.	$B \subseteq A$, men $B \neq A$.
$\lvert A \rvert$	A:s kardinalitet.	Antalet element i A.
$A \cup B$	Unionen av A och B; mängden med alla element i A eller B.	
$A \cap B$	Snittet (skärningen) av A och B; mängden med de element som finns i både A eller B.	
$A \setminus B$	Differensen mellan A och B; mängden med alla element som finns i A förutsatt att elementet inte finns i B.	
A^C	Komplementet till A; mängden med alla element som inte finns i A, (men finns i grundmängden (universum)).	
$\mathcal{P}(A)$	A:s potensmängd; mängden av alla A:s delmängder.	
$A \times B$	Produktmängden av A och B; mängden med alla elementpar mellan A och B, det vill säga $\{(a; b) \mid a \in A, b \in B\}$.	

$C \subseteq A,\ A \subseteq B \Rightarrow C \subseteq B$

Associativa lagen:	$(A \cup B) \cup C = A \cup (B \cup D)$ $(A \cap B) \cap C = A \cap (B \cap D)$
Kommutativa lagen:	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Distributiva lagen:	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgans lag:	$(A \cup B)^C = A^C \cap B^C$ $(A \cap B)^C = A^C \cup B^C$
Identitetslagar:	$A \cup A = A$ $A \cap A = A$ $A \cap \mathcal{U} = A$ $A \cup \emptyset = A$
Absorptionslagen:	$A \cup (A \cap B) = A \cap (A \cup B) = A$
Dubbelt komplement:	$(A^C)^C = A$
Inverslagar:	$A \cup A^C = \mathcal{U}$ $A \cap A^C = \emptyset$
Dominanslagar:	$A \cap \emptyset = \emptyset$ ($A \cap B = B$ omm $B \subseteq A$) $A \cup \mathcal{U} = \mathcal{U}$ ($A \cup B = B$ omm $B \supseteq A$)

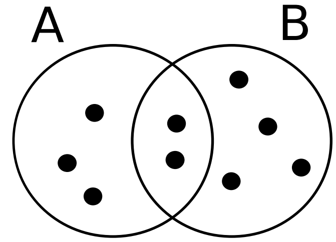
Om A, B disjunkta ($A \cap B = \emptyset$):

$$|A \cup B| = |A| + |B|$$



I allmänhet: (ej disjunkta eller disjunkta)

$$\underset{9}{|A \cup B|} = \underset{5}{|A|} + \underset{6}{|B|} - \underset{2}{|A \cap B|}$$



Induktionsbevis:

Om $P(a)$ är sant och om $P(n) \Rightarrow P(n + 1)$
så är $P(x)$ sant för alla heltal $x \geq a$.

Rekursion:

En följd har en eller fler fördefinierade värden,
startvärden. Till exempel: $F_0 = 0$, $F_1 = 1$

Nästa tal i möljden bestäms av föregående.
Till exempel:

$$F_n = F_{n-1} + F_{n-2}$$

(Detta är Fibonaccitalen.)

Funktioner, avbildningar

$f : X \to Y, \quad y = f(x)$

Sammansättning av funktion

$f : X \to Y, \quad g : Y \to Z$ ger $gf : X \to Z, \ (gf)(x) = g(f(x))$

gf brukar, mer tydligt, skrivas $g \circ f$

Den funktion $f : X \to Y$ kan definieras som en delmängd $f \subseteq X \times Y$ med

$(x; y_1), (x; y_2) \in f \Rightarrow y_1 = y_2$
För alla $x \in X$ finns $y \in Y$ så att $(x, y) \in f$

$f : X \to Y$ är en

injektion	om har högst en $x \in X$ för alla $y \in Y$
surjektion	om har minst en $x \in X$ för alla $y \in Y$
bijektion	om har exakt en $x \in X$ för alla $y \in Y$ (injektion och surjektion).

Sammansättning av två -jektioner ger en -jektion (in-, sur-, bijektion)

$g : Y \to X$ är en inversfunktion, f^{-1}, till $f : X \to Y$ omm ($fg = f \circ g$) $fg = id_Y$, $gf = id_X$,
där $id_\Lambda(\lambda) = \lambda$ för alla $\lambda \in \Lambda$. (Λ är X eller Y)

f har en inversfunktion (är inverterbar) omm f är en bijektion,
f^{-1} är också en bijektion.

Två mängder, X och Y, har samma kardinalitet
omm det finns en bijektion $f : X \to Y$.

En mängds kardinalitet är entydig.

$|X| = n$ (kardinaliteten, antalet element = n)
betyder att det finns en bijektion
$f : \{1, 2, \ldots, n\} \to X$.

Att X är uppräknelig (uppräkneligt oändligt) betyder att det finns
en bijektion $f : \mathbb{N} \to X$.

$\mathbb{Q}$ (de rationella talen)	är uppräknelig
$\mathbb{R}$ (de reella talen)	är oändlig, men inte uppräknelig (den är överuppräknelig)

$|\mathbb{Q}| = |\mathbb{N}| < |\mathbb{R}|$

För alla mängder, ändliga som oändliga, X, gäller att:

$|X| < |\mathcal{P}(X)|$

Om $\mathcal{R}$ är en binär relation på mängden X är $a\mathcal{R}b$ antingen sann eller falsk, för alla $a, b \in X$.

Relationen $\mathcal{R}$ kan beskrivas med

en delmängd till X^2, $\{(a; b) \in X^2 \mid a\mathcal{R}b\}$.

en graf med punkter svarande mot elementen i X och en pil från a till b omm $a\mathcal{R}b$.

en matris med rader och kolonner svaradne mot X:s element, 1 i position ab omm $a\mathcal{R}b$, annars 0.

Viktiga egenskaper för binära relationer:

$\mathcal{R}$ reflexiv:	$x \mathcal{R} x$,	$\forall x \in X$
$\mathcal{R}$ symmetrisk:	$x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$,	$\forall x, y \in X$
$\mathcal{R}$ antisymmetrisk:	$x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y$,	$\forall x, y \in X$
$\mathcal{R}$ transitiv:	$x \mathcal{R} y, y \mathcal{R} z \Rightarrow x \mathcal{R} z$,	$\forall x, y, z \in X$

En ekvivalensrelation på en mängd X är en relation $\mathcal{R}$ som är reflexiv, symmetrisk och transitiv.

En ekvivalensrelation delar in X i ekvivalensklasser av element som står i relationen till varandra:

$\mathcal{C}_x = [x] = \{y \in X \mid y\mathcal{R}x\}$

En partialordning är en relation på mängden X som är
reflexiv, antisymmetrisk och transitiv.

Om $\preccurlyeq$ ($\preceq$) är en partialordning på mängden X och $a \in X$ så är a

ett minimalt element i X omm det inte finns $x \in X$ med $x \preccurlyeq a$, $x \neq a$.

ett minsta element omm $a \preccurlyeq x$ är alla $x \in X$.

Motsvarande för maximala och största element.

Det finns antingen 0 eller 1 minsta element i X,
samma sak ger största element.