2011-(01)jan-14: dag 1

SF1610 – Diskret matematik

Diskret = inkontinuerlig (inga derivator, integraler &c)

Kursintroduktion

Aritmetik och mängder	(Heltalsräkning, primtal, med mera)
Kombinatorik	(Räkna saker och möjligheter)
Algebra	(Grupper, permutationer)
Tillämpad algebra	

Kursens huvuddelar: (Motsvarar KS:arna)

Aritmetik och mängder

Exempel: Finn alla heltal, m och n, så att
$31m + 15n = 102$

Exempel: Låt $a_0 = 0$, $a_1 = 1$, $a_2 = 1$, $a_3 = 2$,
$a_4 = 3$, $a_5 = 5$, ... vad är $a_{1000000}$?

Kominatorik

Exempel: n styckna brev stoppas i varsit slumpmässigt kuvert. Hur stor sannolikhet är det att inget brev hamnar i rätt kuvert?

Exempel: På hur många sätt kan 13 identiska vita kulor och 3 färgade olika kulor ordnas så att inga färgade kulor ligger intill varandra?

Algebra, gruppteori

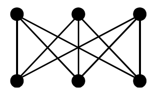
Exempel: Om p är ett primtal så är talet $(p - 1)! + 1$ delbart med p.

Exempel: Riffeblandning av en kortlek; hur många gånger behövs den blandas för att återgå till ursprungliga tillståndet?

Tillämpad algebra

Koder, logiska kretsar.

Grafer och nätverk.

Exempel: Visa att  inte kan ritas utan minst två korsande linjer.

Idag om heltal, 3 kap. i först boken.

Division av heltal

$\frac{37}{5}$? Inget heltal!
- Rationella tal
- Division med rest

37 delat med 5 get kvoten 7 med resten 2. Det vill säga $37 = 5 \cdot 7 + 2$.

↑

Principala resten, $0 \leq r < 5$

Sats: Division med rest

Om heltalen p och $d \neq 0$ finns entydiga heltal q och r sådana att

$$p = \underbrace{q}_{\text{kvot}} \cdot d + \underbrace{r}_{\text{rest}}, \quad 0 \leq r < |d|$$

Bevis:

Låt $d > 0$ ($d < 0$ byter tecken på q)

Betrakta alla heltal > 0, av formen $p - ad$, $a \in \mathbb{Z}$

Finns minst ett sådant tal ($a = -|p| \Rightarrow p - ad = p + d|p| \geq 0$)

Låt r vara det minsta sådana talet.

($r = p - qd \geq 0$, q = lägsta)

Vi har då q och r så att $p = qd + r$, $0 \leq r < d$.

Kvar att visa: entydighet

Om $p = qd + r = q'd + r$, $0 \leq r, r' < d$ då $(q - q')d = r' - r$

$q - q'$: heltal

$r' - r$: $-d < r' - r < d$

Detta ger $q - q' = 0$, det vill säga $q = q'$, $r = r'$

Talbaser

Att skriva tal i basen t:

Låt x och t vara heltal $(x \geq 0,\ t \geq 2)$
(Det går att ha godtyckliga komplexa tal x, eller generellare, och reela, komplexa, eller generellare t med heltals komponent, och $|t| > 1$)

Dividera x med t:

$$
\begin{array}{ll}
x = q_0 t + r_0, & 0 \leq r_0 < t \\
q_0 = q_1 t + r_1, & 0 \leq r_1 < t \\
q_1 = q_2 t + r_2, & 0 \leq r_2 < t \\
q_3 = q_3 t + r_3, & 0 \leq r_3 < t \\
\quad\vdots & \\
q_{n+1} = q_n t + r_n, & q_n = 0,\ 0 \leq r_n < t \Rightarrow q_{n-1} = r_n
\end{array}
$$

Detta ger:

$$
x = \underbrace{(((\ldots(\overbrace{(r_n \cdot t + r_{n-1})}^{q_{n-2}} t + r_{n-2})t + \ldots)t + r_2)t + r_1)}_{q_0} t + r_0 =
$$

$$
= r_n t^n + r_{n-1} t^{n-1} + \ldots + r_1 t^1 + r_0 = \underbrace{(r_n r_{n-1} r_{n-2} \ldots r_1 r_0)_t}_{\text{x i basen t}}
$$

Exempel

2011 i basen $\underline{11}$

$$
\left.
\begin{array}{rcll}
2011 & = & 182 & \cdot \underline{11} + \underset{1}{4} \\
182 & = & 16 & \cdot \underline{11} + \underset{2}{6} \\
16 & = & 1 & \cdot \underline{11} + \underset{3}{5} \\
1 & = & \mathbf{0} & \cdot \underline{11} + \underset{4}{1}
\end{array}
\right\} \Rightarrow 2011_{10} = \underset{4}{1}\,\underset{3}{5}\,\underset{2}{6}\,\underset{1}{4}{}_{11}
$$

Exempel

$$\underset{1}{2}\,\underset{2}{5}\,\underset{3}{1}_6=\underset{1}{2}\cdot 6^2+\underset{2}{5}\cdot 6^1+\underset{3}{1}\cdot 6^0=2\cdot 36+5\cdot 6+1=72+30+1=103_{10}$$

Särskillt viktigt: Binära tal (2-bas)

$$\left.\begin{array}{ccccc}
2011 & = & 1005 & \cdot 2+1 \\
1005 & = & 502 & \cdot 2+1 \\
502 & = & 251 & \cdot 2+0 \\
251 & = & 125 & \cdot 2+1 \\
125 & = & 62 & \cdot 2+1 \\
62 & = & 31 & \cdot 2+0 \\
31 & = & 15 & \cdot 2+1 \\
15 & = & 7 & \cdot 2+1 \\
7 & = & 3 & \cdot 2+1 \\
3 & = & 1 & \cdot 2+1 \\
1 & = & 0 & \cdot 2+1
\end{array}\right\} 2011_{10}=11111011011_2$$

Delbarhet, primtal &c

Om d och m är heltal:

d|m läses som “d derlar m”, “d är en delare till m”,
“m är en multipel av d”...

En heltalsrelation

d|m betyder att det finns ett heltal q sådant att m = qd,
det vill säga en kvot utan rest.

Exempel:

$2|6$, $-8|24$ $14\nmid 2$, $5|0$, $0\nmid 7$, $-3|-18$, $0|0$.

Definition på primtal

Ett primtal är ett heltal p > 1 ($p \in \mathbb{P}$) som bara har delarna ±1 och ±p.

$\mathbb{P}$ = {2, 3, 5, 11, ..., 113, ..., 85218761, ...}

Det finns oändligt många primtal.

Största gemensamma delare, sgd (gcd)

Definition:

Om m, n är heltal är en sgd för m, n ett heltal d sådant att:

1) $d|m$, $d|n$ (är gemensam delare)

2) om $c|m$, $c|n \Rightarrow c \mid d$ (är störst)

3) $d \geq 0$ (är entydig) ← nästa föreläsning!

Exempel:

$\text{sgd}(28; 49) = 7$

$\text{sgd}(11; 0) = 11$ $(11|0)$

$\text{sgd}(m; n) = \text{sgd}(n; m)$

$\text{sgd}(m; 1) = 1$

$\text{sgd}(0; 0) = 0$ $(c|0)$

$\text{sgd}(\pm m; \pm n) = \text{sgd}(m; n)$

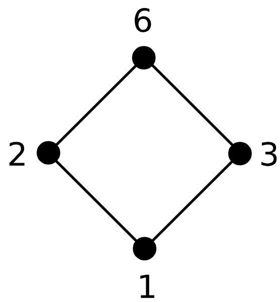
$\text{sgd}(m; n) = \text{sdg}(m + kn; n)$ ty $c|m, c|n \Leftrightarrow c|(m + kn), c|n$

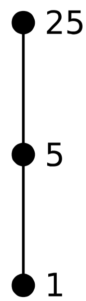
Speciellt:

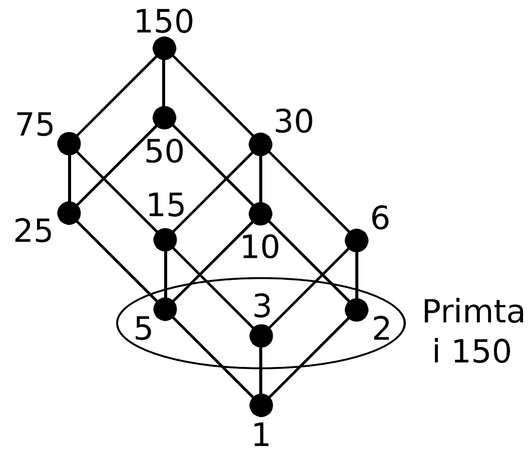
$\text{sgd}(m; n) = \text{sgd}(n; m - qn)$

Delargrafen för ett heltal g > 0:

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



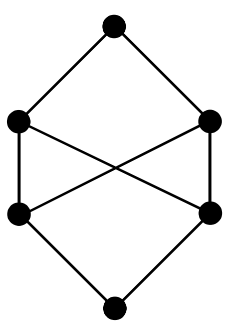




En gemensam delare till m, n i en delargraf:

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.