Diskret matematik 2018-03-19 #1

Olof Sisask sisask@kth.se

IDAG:
- Matte
- Divisionsalgoritmen
- gcd
- Euklides algoritm

INPUT: heltal $a, d > 0$
OUTPUT: tal (q, r)

```
q ← 0
r ← a
while r ≥ d {
  q ← q+1
  r ← r−d
}
return (q, r)
```

I ord: Subtrahera d från a tills vi får något mindre än d.

Ex. dela 1024 med 393

$$1024 = 393 + 631 = \underset{q}{2} \cdot 393 + \underset{r}{238}$$

för $0 \leq 238 < 393$

Def^{n} $4 = 1+1+1+1$

Sats $4 = 2+2$

Sats För alla heltal $n \geq 1$ gäller det att

$$1 + 2 + 3 + \ldots + (n-1) + n = \frac{n(n+1)}{2}$$

Def^{n} Med $\binom{n}{k}$ betecknas antalet sätt att välja k saker från en kollektion med n olika objekt.

Sats $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ $\quad n! = n(n-1)\ldots 3\cdot 2\cdot 1$

Bevis Förklaring!

Problem Om vi ska dela 9 pannkakor lika bland 4 personer, hur mycket får varje person?

$9/4 = 2\frac{1}{4} = 2{,}25$

Problem 2 Om vi har 9 konsertbiljetter som ska delas lika mellan 4 grupper, hur många får varje?

→ 2 biljetter per grupp, och 1 över.

$(9 = 2 \cdot 4 + 1)$

Sats (Division med rest)

Givna två heltal a & d, $d \neq 0$, så finns det två unika tal q & r så att

$$a = q \cdot d + r \quad \text{och} \quad 0 \leq r < |d|$$

Def^{n} q: "kvot" $\quad r$: "rest"/principala resten

<u>Bevis av sats</u> Att åtminstone ett par (q, r) finns följer från divisionsalgoritmen.

Varför unikt? Strategi: Anta att det finns två par och visa att de måste vara lika.

Så anta att $a = q_1 \cdot d + r_1 \quad 0 \leq r_1 < |d|$
$a = q_2 \cdot d + r_2 \quad 0 \leq r_2 < |d|$

Vi vill visa att $q_1 = q_2$ & $r_1 = r_2$

Vi vet att $q_1 d + r_1 = q_2 d + r_2$

Så $(q_1 - q_2)d = r_2 - r_1$

Men q_1 & q_2 är heltal, så vänsterledet är ett av talen

$0, \pm d, \pm 2d, \pm 3d, \ldots$

Men högerledet har $-|d| < r_2 - r_1 < |d|$

Men 0 är den enda multipeln av d i detta intervall.
Så $r_2 = r_1$, & $q_2 = q_1$ ■

<u>Delare</u>

<u>Def^n</u> Låt a & d vara heltal. Om det finns ett heltal q sådant att $a = q \cdot d$ säger vi att d är en delare eller faktor i a, och att a är en multipel av d.

Vi skriver också: $d \mid a$
"d delar a"

Ex. $6|24$, $5|10$, $3|3$, $-5|10$, $-5|10$, $-5|-10$, $10|100$,
$3|0$ $57|0$, men $5 \nmid 11$, $4 \nmid 1$

<u>Fråga</u> Vad är den största möjliga längden på en pinne som kan mäta ut både 57 cm och 12 cm?

<u>Def^n</u> Om ett tal d delar både talet a och talet b kallas d för en gemensam delare till a & b.

<u>Def^n</u> Den största gemensamma delaren till a & b betecknas $\gcd(a, b)$ $(sgd(a,b))$ greatest common divisor

$1|57$ & $1|12$ så 1 är en gemensam delare till 57 & 12, men är inte den största för $3|57$ & $3|12$.

Det visar sig att $\gcd(57, 12) = 3$

Euklides algoritm

via exempel: hitta $\gcd(133, 56)$

$$\begin{aligned}
133 &= 2\cdot 56 + 21\\
56 &= 2\cdot 21 + 14\\
21 &= 1\cdot 14 + \boxed{7}\\
14 &= 2\cdot 7 + 0
\end{aligned}$$

sista nollskilda resten är $\gcd(133, 56)$

Analys av algoritmen
- varför terminerar den?
- varför är sista nollskilda resten $= \gcd(a,b)$?
- hur snabb är algoritmen (tittar vi inte på)

① Varför når vi 0 till slut?
När vi tar talen (a,b) och byter ut mot (b, r), där $a = qb + r_1$ & $0 \le r_1 < b$ så är det andra talet i paret, dvs r_1, strikt mindre än det andra talet i (a,b)

Så algoritmen tar två tal	(a,b)	
och byter ut mot	(b, r_1),	$0 \le r_1 \le b-1$
-"-	$(r_1\ r_2)$	$0 \le r_2 \le r_1 - 1$
-"-	$(r_2\ r_3)$	$0 \le r_3 \le r_2 - 1$

Resterna längst till höger i algoritmen blir mindre vid varje rad/division, och är alltid åtminstone 0.
Alltså måste de till slut nå 0.

$$0 \le r_1 \le b-1$$

<u>Sats</u> Om d är en gemensam delare till a & b, dvs $d|a$ och $d|b$, så delar d alla linjärkombinationer

$$m\cdot a + n\cdot b \quad \text{där } m, n \text{ är heltal}$$

<u>Bevis</u> Enligt def^n av $d|a, d|b$ så finns det heltal p & q så att

$$a = p\cdot d \quad \& \quad b = q\cdot d.$$

Då är $ma + nb = mpd + nqd = (mp + nq)d$, som är en multipel av d.

Vid varje steg i Eulides algoritm tar vi två tal (a,b) och byter ut mot (b,r) där $a = q\cdot b + r$,

Om $d|a$ & $a|b$ så delar d också r enligt satsen.

Så om vi har en gemensam delare till (a,b) så är det en gemensam delare till (b,r)
OCH, om d är en gemensam delare till (b,r) så är det en gemensam delare till (a,b), för $a = qb + r$

<u>SÅ</u> (a,b) & (b,r) har <u>precis samma</u> gemensamma delare.

Därför har de samma <u>största gemensamma</u> delare.
Dvs $\boxed{\gcd(a,b) = \gcd(b,r) \text{ om } a = qb + r}$

EUKLIDES

INPUT: heltal $a \geq b \geq 1$
OUTPUT: gcd(a, b)

```
function gcd(a, b) {
    r ← resten i a delat på b   //a = q·b + r
    if(r=0) then return b;
    else return gcd(b,r). }
```