

Ugeseddel 1.

Velkommen til Matematik 2AL. Kurset har en hjemmeside:

<http://www.math.ku.dk/kurser/mat2al>

Her kan du finde oplysninger om kurset, om øvelser, lærebøger, pensum, og eksamen. Der er også en *undervisningsplan*, med beskrivelser af undervisning og øvelser for de enkelte uger i semestret. Jeg vil gøre, hvad jeg kan, for at overholde planen, men det er altså kun en plan, og den kan blive ændret i løbet af semestret. I øvrigt hedder jeg Anders Thorup, og jeg kan træffes på H. C. Ørsted Institut (lokale E209), tlf 3532 0749, e-mail: <thorup@math.ku.dk> — eller privat, tlf 44653153.

Inden hver uges undervisning lægges en *ugeseddel* ud på nettet. Den fortæller bl.a. lidt om hvad der foregik i den forgangne uge og om hvad der planlægges for den kommende. Videre fremhæves på ugesedlen – lidt uformelt – nogle aktuelle hovedresultater fra noterne. Endelig vil der være diverse kommentarer og oplysninger.

Program. Den første uge i semestret, 3/2-7/2, har overskriften „Tallene“, på baggrund af TAL1-6, med hovedvægt på naturlige tal, hele tal, og (delvis) restklasser. Der er ingen øvelser i den første uge.

Nøgleord: Ugesedlen vil i reglen indeholde en liste over *nøgleord*. Det er ord, der dækker de begreber, der har været omtalt. Det er en god og vigtig øvelse, at du ord for ord gennemgår listen: har du en klar fornemmelse af hvad ordet dækker, – eller kan du i det mindste genkende ordet? På denne ugeseddel er der kun tre nøgleord: undervisningsplan, ugeseddel, nøgleord.

Kuglerne.

- *Induktion* er en særlig bevisteknik, som af og til kan bruges for at bevise udsagn af formen „For ethvert naturlige tal n gælder $\varphi(n)$ “. Bemærk, at induktion bestemt ikke altid er nødvendigt. Den oplagte måde at angribe et sådant udsagn er følgende: Betragt et tilfældigt n , og gå så i gang med at bevise $\varphi(n)$. Til rådighed i dette bevis kan man forudsætte hele sin matematiske viden, specielt egenskaber, man har bevist ved naturlige tal, og alle antagelser, der ligger som forudsætninger i udsagnet $\varphi(n)$. Pointen, når man bruger induktion, er så, at når $n > 1$, må man yderligere antage, at $\varphi(n-1)$ er sandt; når det er fuldstændig induktion, må man endda antage, at $\varphi(k)$ er sandt for alle $k < n$.

- *Divisionssætning*, division med rest: Når $n \geq 1$ er givet, kan hvert helt tal a skrives $a = qn + r$, hvor $0 \leq r < n$. Det er grundlaget for Euklid's algoritme, og grundlaget for et vigtigt resultat om største fælles divisorer: *Den største fælles divisor d for a, n har formen $d = xa + yn$ med hele tal x, y , og enhver fælles divisor for a, n er divisor i d .*

- *Euklid beviste*, at der er uendelig mange primtal.

- *Man går op i et produkt*, hvis man går op i en af faktorerne: $p|ab \iff p|a$ eller $p|b$; det er klart nok! Det er helt fundamentalt, at for et *primtal* p gælder der også det omvendte: $p|ab \implies p|a$ eller $p|b$.

31. januar 2003

• Hvis et produkt går op, så går hver af faktorerne op: $n_1 n_2 | a \implies n_1 | a$ og $n_2 | a$; det er klart nok! Det er fundamentalt, at hvis de to faktorer n_1 og n_2 er primiske, så gælder det omvendte: $n_1 | a$ og $n_2 | a \implies n_1 n_2 | a$.

• *Aritmetikens Fundamentalsætning.* Hvert naturligt tal n kan skrives som produkt af primtal, $n = p_1 \cdots p_r$, og fremstillingen er entydig bortset fra ombytning af faktorerne p_i . Når primopløsninger af a, n kendes, er det umiddelbart at angive den største fælles divisor d for a, n . Det er en vigtig pointe, at Euklid's algoritme tillader at bestemme den største fælles divisor for a, n uden kendskab til primopløsningerne.

• Restklassen af a modulo n betegnes $[a]$ (eller udførligt $[a]_n$). Den består af *alle* de tal r , der passer i en ligning af formen $a = qn + r$; alternativt kan $[a]_n$ beskrives som mængden af de tal r , som er kongruente med a modulo n , dvs opfylder, at $r \equiv a \pmod{n}$. Restklassen $[a]_n$ er altså ifølge definitionen en (uendelig) delmængde af \mathbb{Z} . I praksis kan det betale sig snarere at tænke på $[a]_n$ som et symbol, knyttet til det hele tal a , med følgende egenskab: $[a]_n = [a']_n \iff a \equiv a' \pmod{n}$.

Mængden af restklasser modulo n betegnes \mathbb{Z}/n .

• Man regner med restklasser sådan:

$$[a]_n + [b]_n := [a + b]_n, \quad [a]_n \cdot [b]_n := [ab]_n.$$

Faktisk er det lidt mere sofistikeret end det ser ud: Det første lighedstegn definerer summen af de to restklasser på venstresiden som den restklasse, der står på højresiden. En oplagt indvending er så: Tallet a er jo blot et af de mange mulige tal i restklassen $[a]_n$, og med et andet valg, fx a' , ville vi få en anden sum, nemlig $a' + b$, som det tal, der bestemmer højresiden. Det ser altså ud som om højresiden afhænger af et valg. (Men det gør den selvfølgelig ikke.) Tilsvarende med definition af produktet.

Et lignende problem gør sig gældende i følgende definition: Når d er divisor i n , defineres en afbildning $\mathbb{Z}/n \rightarrow \mathbb{Z}/d$ ved

$$[a]_n \mapsto [a]_d;$$

venstresiden er en restklasse modulo n , og højresiden skulle gerne beskrive den restklasse modulo d , der bliver resultatet ved afbildningen. Men det ser jo ud som om resultatet afhænger af det tal a , der er valgt i restklassen på venstresiden. (Mon det gør?)

Hvornår var det nu det var? Eratosthenes 276–197, Euklid (ca) 365–300 (det fremgår, at det var før vor tidsregning).

På sigt: I den anden uge, 10/2-14/2, er overskriften „Grupper“, med materiale fra TAL6 og GRP1. Ugens øvelser er TAL2: 5, 9, 10, 12, 13, 14; TAL3: 2, 4, 6, 7, 10, 12. De markerede opgaver er til skriftlig aflevering til instruktorerne.

Anders Thorup