DM547 øvelsestimer
04-11-19

Jonas Eriksen

4. november 2019

Antal fremmødte:

Opgave 4.1.6

Vis at hvis $a, b, c, d \in \mathbb{Z}$, hvor $a \neq 0$, sådan at $a|c$ og $b|d$, da gælder det at $ab|cd$.

Hvis $a|c$ og $b|d$ så $\exists s, r \in \mathbb{Z}$ sådan at $c = as$ og $d = br$. Da vil $cd = asbr = ab(sr)$, hvorfor $ab|cd$ iflg. Def 4.1.1.

$\square$

Opgave 4.1.8

Bevis eller modbevis at hvis $a|bc$, hvor $a, b, c \in \mathbb{Z}^+$, og $a \neq 0$ så gælder $a|b$ eller $a|c$.

Modeksempel: $a = 6$, $b = 4$ og $c = 3$. Vi ser at $6|(4 \cdot 3)$ men $6 \nmid 4$ og $6 \nmid 3$. Dette modbeviser sætningen.

$\square$

Opgave 4.1.13

Hvad er kvotienten og resten når

a) 19 divideres med 7?

Kvotient $= 2$. Rest $= 5$. Fordi $19 = 7 \cdot 2 + 5$

e) 0 divideres med 19?

Kvotient $= 0$. Rest $= 0$. Fordi $0 = 19 \cdot 0 + 0$.

f) 3 divideres med 5?

Kvotient $= 0$. Rest $= 3$. Fordi $3 = 5 \cdot 0 + 3$.

g) -1 divideres med 3?

Kvotient $= -1$. Rest $= 2$. Fordi $-1 = 3 \cdot (-1) + 2$.

Opgave 4.1.21

Lad $m \in \mathbb{Z}^+$. Vis at $a \equiv b \pmod{m}$ hvis $a \mod m = b \mod m$. (d.v.s. vi skal vise at $a \mod m = b \mod m \Rightarrow a \equiv b \pmod{m}$).

Antag at $a \mod m = b \mod m = r$. Så kan vi ifølge Sætning 4.1.2 kan vi skrive $a = q_1 m + r$ og $b = q_2 m + r$, hvor $q_1, q_2 \in \mathbb{Z}$. Det følger at

$$\begin{aligned} a - b &= (q_1 m + r) - (q_2 m + r) && \text{(Bruger udtrykkene for } a \text{ og } b) \\ &= q_1 m - q_2 m && \text{(Forkorter)} \\ &= m \underbrace{(q_1 - q_2)}_{\in \mathbb{Z}} && (m \text{ uden for parentes)} \end{aligned}$$

så $m|(a - b)$, iflg. Def. 4.1.1. Derfor kan vi slutte at $a \equiv b \pmod{m}$, iflg. Def. 4.1.3.

$\square$

Opgave 4.1.22

Lad $m \in \mathbb{Z}^+$. Vis at $a \mod m = b \mod m$ hvis $a \equiv b \pmod{m}$. (d.v.s. vi skal vise at $a \equiv b \pmod{m} \Rightarrow a \mod m = b \mod m$).

Antag at $a \equiv b \pmod{m}$. Vi ved fra Sætning 4.1.2 at vi kan skrive $a = q_1 m + r_1$ og $b = q_2 m + r_2$, hvor $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ sådan at $0 \leq r_1 < m$ og $0 \leq r_2 < m$.

(Det vi nu ønsker at vise er at $r_1 = r_2$ fordi så er sætningen sand.)

Da $a \equiv b \pmod{m}$ kan vi skrive

$$\begin{aligned} a - b &= (q_1 m + r_1) - (q_2 m + r_2) && \text{(Bruger udtryk for } a \text{ og } b) \\ &= q_1 m - q_2 m + r_1 - r_2 && \text{(Rykker rundt på led)} \\ &= km && (k \in \mathbb{Z};\ \text{vi ved at } m|(a - b)) \end{aligned}$$

så

$$
\begin{aligned}
r_1 - r_2 =& km - q_1 m + q_2 m && \text{(Isolerer } r_1 - r_2\text{)} \\
=& (k - q_1 + q_2)m && \text{(}m\text{ udenfor parentes)}
\end{aligned}
$$

så $m|(r_1 - r_2)$ hvilket vil sige at $r_1 - r_1$ er et multiplum af m og samtidig er $-m < r_1 - r_2 < m$. Derfor må $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$. Det følger at $a \mod m = b \mod m$.

$\square$

Opgave 4.1.33

Oprems alle heltal mellem -100 og 100, der er kongruente med $-1 \mod 25$.

Observér at $-1 \mod 25 = 24$. Så vi skal finde alle heltal mellem -100 og 100, der har en rest på 24 når de divideres med 25. (Alternativt: vi skal finde alle de heltal a mellem -100 og 100 der opfylder at $25|(a+1)$). Disse er

$$
\begin{array}{r}
-76 \\
-51 \\
-26 \\
-1 \\
24 \\
49 \\
74 \\
99
\end{array}
$$

(Bemærk, at der er et 'hop' på præcis 25 hver gang, hvilket netop er den måde modulo fungerer på.)

Opgave 4.1.34

Afgør, hvorvidt disse tal er kongruente til $3 \mod 7$.

a) 37

Ikke kongruent. $7 \nmid (37 - 3)$.

b) 66

Kongruent. $7|(66 - 3)$.

c) -17

Ikke kongruent. $7 \nmid (-17 - 3)$, d.v.s. $7 \nmid -20$.

d) -67

Kongruent. $7|(-67 - 3)$, d.v.s. $7| - 70$.

$\square$

Opgave 4.1.41

Vis at hvis $n|m$, hvor n og m er heltal større end 1 og hvis $a \equiv b \pmod m$, hvor a og b er heltal, så er $a \equiv b \pmod n$.

Vi observerer først at $n|m \Rightarrow m = nc$ for et $c \in \mathbb{Z}$ (Def 4.1.1).

Dernæst ser vi på $a \equiv b \pmod m$, som medfører at $m|(a - b)$ (Def. 4.1.3). Det betyder at $\exists k \in \mathbb{Z} : \ a - b = mk$ (Def 4.1.1).

Vi kan nu substiture udtrykket for m ind i udtrykket for $a - b$, hvilket giver $a - b = nck$, hvilket vil sige at $n|(a - b)$ da $ck \in \mathbb{Z}$. Det følger at $a \equiv b \pmod n$.

$\square$

Opgave 4.3.1

Afgør, hvorvidt disse heltal er primtal.

a) 21

Ikke primtal. $7|21$.

c) 71

Bruger sætning 4.3.7: n ikke er et primtal $\Rightarrow \exists$ primtalsdivisor $\leq \sqrt{n}$ (kontrapos.: $\nexists$ primtalsdivisor $\leq \sqrt{n} \Rightarrow$ n er et primtal).

Vi har $\sqrt{71} \approx 8,43 \leq 9$. Primtallene der er ≤ 9 er $2, 3, 5$ og 7. Det er åbenlyst at $2 \nmid 71$, $5 \nmid 71$ og $7 \nmid 71$. Vi kan desuden også også nemt verificere at $3 \nmid 71$. Derfor: primtal.

Opgave 4.3.3

Find primtalsfaktoriseringen af af disse heltal

(Når vi primtalsfaktoriserer kan det sommetider være en hjælp af skrive tallet som et produkt af mindre tal som man så primtalsfaktoriserer.)

a) 88

$88 = 11 \cdot 8 = 2^3 \cdot 11.$

b) 126

$126 = 2 \cdot 63 = 2 \cdot 7 \cdot 9 = 2 \cdot 3^2 \cdot 7.$

$\square$

Opgave 4.3.5

Find primtalsfaktoriseringen af 10!.

Vi finder denne ved at finde primtalsfaktoriseringen af de mindst mulige delprodukter og så gange dem sammen til sidst

$$\begin{aligned}
10 &= 5 \cdot 2 \\
9 &= 3 \cdot 3 \\
8 &= 2 \cdot 2 \cdot 2 \\
7 &= 7 \\
6 &= 3 \cdot 2 \\
5 &= 5 \\
4 &= 2 \cdot 2 \\
3 &= 3 \\
2 &= 2
\end{aligned}$$

og vi udelader 1, fordi den ikke ændrer produktet. Da 10! er et produkt, kan vi blot tælle primtallene i primtalsfaktoriseringerne ovenfor. Derfor: $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

Opgave 4.3.12

Vis at for ethvert positivt heltal n, er der n på hinanden følgende sammensatte tal.

Til dette bevis skal vi bruge nedenstående sætninger, definitioner m.m.:

1. Et tal m er sammensat, hvis der eksisterer et heltal $k < m$ sådan at $k|m$ og dermed $m = kc$ for et $c \in \mathbb{Z}$.

2. Hvis $m, s \in \mathbb{Z}^+$ og $m \leq s$, så må $m|s!$, fordi m da er en faktor i $s!$, hvorved $s!$ er et multiplum af m. Dette medfører at for alle heltal $2 \leq k \leq (n+1)$, gælder det at $k|(n+1)!$.

3. Sætning 4.1.(i) fortæller os at hvis $a|b$ og $a|c$ så $a|(b+c)$.

4. Alle heltal går op i sig selv, d.v.s. $\forall k \in \mathbb{Z} : k|k$.

Dette kan vi nu bruge til at indse, at det følgende må gælde

$$\begin{gathered} 2|(2+(n+1)!) \\ 3|(3+(n+1)!) \\ 4|(4+(n+1)!) \\ \vdots \\ n|(n+(n+1)!) \\ (n+1)|(n+1+(n+1)!) \end{gathered}$$

Dette viser at alle de n heltal i intervallet $[2+(n+1)!; n+1+(n+1)!]$ er sammensatte. Dette følger at bullet (1) fordi vi viser at alle disse tal har en heltalsdivisor mindre end sig selv. At fx $3|(3+(n+1)!)$ følger af bulltets (2), (3) og (4).

$\square$