Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 2

$\boxed{\text{2.3.3}}$ Usant. Et enkelt moteksempel er at $2 \mid (1+1)$, men $2 \nmid 1$.

$\boxed{\text{2.3.12}}$ Vi skriver $d = \gcd(a, a+n)$. Per definisjon betyr dette at $d \mid a$ og $d \mid a+n$. Så det finnes k og l slik at $a = dk$ og $a + n = dl$. Videre får vi at $n = (a+n) - a = dl - dk = d(l-k)$, og dette betyr at $d \mid n$, som var det vi skulle vise. For $n = 1$ betyr dette spesielt at $\gcd(a, a+1) \mid 1$. Det eneste, og dermed største, positive heltallet med denne egenskapen er 1, så fra definisjonen er $\gcd(a, a+1) = 1$.

$\boxed{\text{2.3.14b}}$ La $d = \gcd(5a+2, 7a+3)$. Da vil $d \mid (5a+2)$ og $d \mid (7a+3)$, som impliserer at

$$d \mid [3(5a+2) - 2(7a+3)] = a.$$

Nå har vi at $d \mid a$, $d \mid 5a+2$ og $d \mid 7a+3$, som gir at

$$d \mid (7a+3) - (5a+2) - 2a = 1.$$

Vi vet at $d \mid 1 \iff d = \pm 1$, og siden $d > 0$ betyr dette at $d = 1$, som var det vi ville vise.

$\boxed{\text{2.3.14c}}$ La $d = \gcd(3a, 3a+2)$. Siden a er et oddetall, så er $a = 2k+1$ for en $k \in \mathbb{Z}$, som betyr at $d = \gcd(6k+3, 6k+5)$. Dette impliserer at $d \mid 6k+3$ og $d \mid 6k+5$, som igjen impliserer at

$$d \mid [(6k+5) - (6k+3)] = 2.$$

Siden $d \mid 2$ impliserer at $d \mid 2(3k+1)$, kan vi også si at

$$d \mid [(6k+3) - 2(3k+1)] = 1.$$

Dermed har vi at $d \mid 1$, og som i forrige oppgave betyr det at $d = 1$.

Alternativ løsning:

$$\begin{aligned} d = \gcd(3a, 3a+2) &\implies d \mid 3a \text{ og } d \mid 3a+2 \\ &\implies d \mid (3a+2) - 3a = 2 \\ &\implies d = 1 \text{ eller } d = 2 \end{aligned}$$

Hvis $d = 2$ må $3a$ være et partall, siden $d \mid 3a$. Men dersom $3a$ er et partall må også a være et partall. Dette gir en motsigelse, siden vi antar at a er et oddetall. Dermed slutter vi at $d = 1$.

$\boxed{\text{2.3.17}}$ Vi ønsker å vise at $\frac{(3n)!}{(3!)^n}$ er et heltall for alle $n \geq 0$. Legg merke til at $3! = 2 \cdot 3$, så $(3!)^n = 2^n \cdot 3^n$. Det betyr at vi kun trenger vise at $(3n)!$ inneholder $\geq n$ kopier av faktorene 2 og 3. For å se dette, legg merke til at $(3n)! = 3n \cdot (3n-1) \cdot (3n-2) \cdots 3 \cdot 2 \cdot 1$ inneholder:

$$\begin{aligned} 3, 6, 9, \ldots, 3(n-1), 3n, &\quad \text{som alle inneholder (minst) en faktor 3} \\ 2, 4, 6, \ldots 2(n-1), 2n, &\quad \text{som alle inneholder (minst) en faktor 2} \end{aligned}$$

Dermed inngår 2 og 3 som faktorer i $(3n)!$ mer enn n ganger hver, som betyr at $\frac{(3n)!}{(3!)^n}$ er et heltall for alle $n \geq 0$.

$\boxed{\text{2.3.21}}$ Merk at $d \mid n \iff n = qd$ for en $q \in \mathbb{Z}$. Vi bruker hintet, med $x = 2^d$ og $k = q$, som gir

$$2^n - 1 = 2^{qd} - 1 = (2^d)^q - 1 = (2^d - 1)((2^d)^{q-1} + (2^d)^{q-2} + \cdots + 2^d + 1)$$

Vi ser at $2^d - 1$ er en faktor i $2^n - 1$ som betyr at $2^d - 1 \mid 2^n - 1$.

For deloppgave b er det nok å observere at $31 = 2^5 - 1$, at $127 = 2^7 - 1$ og at $2^{35} - 1 = 2^{5 \cdot 7} - 1$, og så anvende resultatet fra a.

$\boxed{\text{2.4.1}}$ Vi finner $\gcd(143, 227)$ ved å bruke Euklids algoritme på 227 og 143:

$$\begin{aligned} 227 &= 1 \cdot 143 + 84 \\ 143 &= 1 \cdot 84 + 59 \\ 84 &= 1 \cdot 59 + 25 \\ 59 &= 2 \cdot 25 + 9 \\ 25 &= 2 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

Så $\gcd(227, 143) = 1$. De andre regnes ut på samme måte, og vil gi $\gcd(306, 657) = 9$ og $\gcd(272, 1479) = 17$.

$\boxed{\text{2.4.2c}}$ Vi bruker Euklids algoritme på 272 og 119:

$$\begin{aligned} 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

Så $\gcd(119, 272) = 17$. Vi nøster oss bakover, og får:

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3 \cdot (272 - 2 \cdot 119) \\ &= 7 \cdot 119 - 3 \cdot 272 \end{aligned}$$

2.4.2d Vi bruker Euklids algoritme på 2378 og 1769:

$$\begin{aligned}
2378 &= 1 \cdot 1769 + 609 \\
1769 &= 2 \cdot 609 + 551 \\
609 &= 1 \cdot 551 + 58 \\
551 &= 9 \cdot 58 + 29 \\
58 &= 2 \cdot 29 + 0
\end{aligned}$$

Så $\gcd(1769, 2378) = 29$. Vi nøster oss bakover, og får:

$$\begin{aligned}
29 &= 551 - 9 \cdot 58 \\
&= 551 - 9 \cdot (609 - 1 \cdot 551) \\
&= 10 \cdot 551 - 9 \cdot 609 \\
&= 10 \cdot (1769 - 2 \cdot 609) - 9 \cdot 609 \\
&= 10 \cdot 1769 - 29 \cdot 609 \\
&= 10 \cdot 1769 - 29 \cdot (2378 - 1 \cdot 1769) \\
&= 39 \cdot 1769 - 29 \cdot 2378
\end{aligned}$$

2.4.6 Vi antar at $\gcd(a, b) = 1$. Fra oppgave 2.3.12 får vi at $\gcd(a, a + b) \mid b$, og per definisjon har vi at $\gcd(a, a + b) \mid a$. Dermed vil $\gcd(a, a + b) \mid \gcd(a, b)$, og siden $\gcd(a, b) = 1$ medfører det at $\gcd(a, a + b) = 1$. Et tilsvarende argument viser at $\gcd(b, a + b) = 1$. Dette betyr at vi kan finne $s, t, u, v \in \mathbb{Z}$ slik at

$$\begin{aligned}
as + (a + b)t &= 1 \\
bu + (a + b)v &= 1.
\end{aligned}$$

Ved å gange sammen de to ligningene får vi at

$$\begin{aligned}
(as + (a + b)t)(bu + (a + b)v) &= 1 \cdot 1 \\
absu + (a + b)(asv + but + (a + b)tv) &= 1.
\end{aligned}$$

Som vi ser er det siste uttrykket på formen $ab \cdot x + (a + b)y = 1$, som betyr at $\gcd(ab, a + b) = 1$.