Forelesning 9 — mandag den 15. september

2.6 Største felles divisor

Definisjon 2.6.1. La l og n være heltall. Et naturlig tall d er den *største felles divisoren* til l og n dersom følgende er sanne.

(1) Vi har: $d \mid l$ og $d \mid n$, altså d er en divisor til både l og n.

(2) La c være et naturlig tall slik at $c \mid l$ og $c \mid n$, altså c er en divisor til både l og n. Da er $c \leq d$.

Notasjon 2.6.2. La l og n være heltall. Dersom det finnes naturlig tall som er den største felles divisoren til l og n, betegner vi det som $\mathsf{sfd}(l, n)$.

Merknad 2.6.3. La l og n være heltall. I Definisjon 2.6.1 kan vi bytte rekkefølgen på l og n uten å endre kravene (1) og (2). Dersom det finnes naturlig tall d som er den største felles divisoren til l og n, følger det at d er også den største felles divisoren til n og l. Med andre ord er $\mathsf{sfd}(l, n) = \mathsf{sfd}(n, l)$.

Eksempel 2.6.4. Divisorene til 6 som er naturlige tall er: 1, 2, 3, og 6. Divisorene til 8 som er naturlige tall er: 1, 2, 4, og 8. Dermed ser vi at de eneste naturlige tallene som deler både 6 og 8 er 1 og 2. Siden $1 \leq 2$, er $\mathsf{sfd}(6, 8) = 2$.

Eksempel 2.6.5. Divisorene til 9 som er naturlige tall er: 1, 3, 9. Divisorene til 12 som er naturlige tall er: 1, 2, 3, 4, 6, og 12. Dermed ser vi at de eneste naturlige tallene som deler både 9 og 12 er 1 og 3. Siden $1 \leq 3$, er $\mathsf{sfd}(9, 12) = 3$.

Eksempel 2.6.6. Divisorene til 30 som er naturlige tall er: 1, 2, 3, 5, 6, 10, 15, og 30. Divisorene til 105 som er naturlige tall er: 1, 3, 5, 7, 15, 21, 35, og 105. Dermed ser vi at de eneste naturlige tallene som deler både 30 og 105 er 1, 3, 5, og 15. Siden 15 er den største av disse fire naturlige tallene, er $\mathsf{sfd}(30, 105) = 15$.

Eksempel 2.6.7. Divisorene til 5 som er naturlige tall er: 1 og 5. Divisorene til 7 som er naturlige tall er: 1 og 7. Dermed ser vi at det eneste naturlige tallet som deler både 5 og 7 er 1. Derfor er $\mathsf{sfd}(5, 7) = 1$.

Eksempel 2.6.8. Divisorene til -10 som er naturlige tall er: 1, 2, 5, 10. Divisorene til 18 som er naturlige tall er: 1, 2, 3, 6, 9, 18. Dermed ser vi at de eneste naturlige tallene som deler både -10 og 18 er 1 og 2. Siden $1 \leq 2$, er $\mathsf{sfd}(-10, 18) = 2$.

Eksempel 2.6.9. Divisorene til -21 som er naturlige tall er: 1, 3, 7, 21. Divisorene til -24 som er naturlige tall er: 1, 2, 3, 4, 6, 8, 12, og 24. Dermed ser vi at de eneste naturlige tallene som deler både -21 og -24 er 1 og 3. Siden $1 \leq 3$, er $\mathsf{sfd}(-21, -24) = 3$.

Eksempel 2.6.10. La n være et heltall slik at $n \neq 0$. Siden n er delelig med n, og siden alle andre divisorer til n er mindre enn n, er $\mathsf{sfd}(n, n) = n$.

Merknad 2.6.11. Alle naturlige tall er divisorer til 0. Derfor finnes det ikke et naturlig tall som er den største felles divisoren til 0 og 0. Med andre ord har 0 og 0 ikke en største felles divisor.

Proposisjon 2.6.12. La l og n være heltall. Anta at det finnes et naturlig tall d slik at d er den største felles divisoren til l og n. Da er d den største felles divisoren til $-l$ og n.

Bevis. Siden $\mathsf{sfd}(l, n) = d$, har vi:

(1) $d \mid l$;

(2) $d \mid n$;

(3) dersom c er et naturlig tall slik at $c \mid l$ og $c \mid n$, er $c \leq d$.

Vi gjør følgende observasjoner.

(4) Fra (1) og Proposisjon 2.5.12 følger det at $d \mid -l$.

(5) La c være et naturlig tall slik at $c \mid -l$ og $c \mid n$. Siden $c \mid -l$, følger det fra Proposisjon 2.5.12 at $c \mid l$. Derfor har vi: $c \mid l$ og $c \mid n$. Fra (3) deduserer vi at $c \leq d$.

Fra (4), (2), og (5) konkluderer vi at $\mathsf{sfd}(-l, n) = d$.

□

Eksempel 2.6.13. I Eksempel 2.6.4 fant vi at $\mathsf{sfd}(6, 8) = 2$. Derfor fastslår Proposisjon 2.6.12 at $\mathsf{sfd}(-6, 8) = 2$.

Eksempel 2.6.14. I Eksempel 2.6.9 fant vi at $\mathsf{sfd}(-21, -24) = 3$. Derfor fastslår Proposisjon 2.6.12 at $\mathsf{sfd}(21, -24) = 3$.

Korollar 2.6.15. La l og n være heltall. Anta at det finnes et naturlig tall d slik at d er den største felles divisoren til l og n. Da er d den største felles divisoren til l og $-n$.

Bevis. Utsagnet følger umiddelbart fra Merknad 2.6.3 og Proposisjon 2.6.12. □

Eksempel 2.6.16. I Eksempel 2.6.4 fant vi at $\mathsf{sfd}(6, 8) = 2$. Derfor fastslår Korollar 2.6.15 at $\mathsf{sfd}(6, -8) = 2$.

Eksempel 2.6.17. I Eksempel 2.6.9 fant vi at $\mathsf{sfd}(-21, -24) = 3$. Derfor fastslår Korollar 2.6.15 at $\mathsf{sfd}(-21, 24) = 3$.

Korollar 2.6.18. La l og n være heltall. Anta at det finnes et naturlig tall d slik at d er den største felles divisoren til l og n. Da er d den største felles divisoren til $-l$ og $-n$.

Bevis. Siden d er den største felles divisoren til l og n, følger det fra Proposisjon 2.6.12 at d er den største felles divisoren til $-l$ og n. Da følger det fra Korollar 2.6.15 at d er den største felles divisoren til $-l$ og $-n$. □

Eksempel 2.6.19. I Eksempel 2.6.4 fant vi at $\mathsf{sfd}(6, 8) = 2$. Derfor fastslår Korollar 2.6.18 at $\mathsf{sfd}(-6, -8) = 2$.

Eksempel 2.6.20. I Eksempel 2.6.9 fant vi at $\mathsf{sfd}(-21, -24) = 3$. Derfor fastslår Korollar 2.6.18 at $\mathsf{sfd}(21, 24) = 3$.

Proposisjon 2.6.21. La n være et heltall, og la l være et naturlig tall. Anta at $l \mid n$. Da er l den største felles divisoren til l og n.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har: $l \mid n$;

(2) Siden $l = 1 \cdot l$, har vi: $l \mid l$.

(3) La c være et naturlig tall slik at $c \mid l$ og $c \mid n$. Siden $c \mid l$, følger det fra Proposisjon 2.5.30 at $c \leq l$.

Fra (1) – (3) konkluderer vi at l er den største felles divisoren til l og n.

$\square$

Eksempel 2.6.22. Siden $21 = 7 \cdot 3$, har vi: $3 \mid 21$. Derfor fastslår Proposisjon 2.6.21 at $\mathsf{sfd}(3, 21) = 3$.

Eksempel 2.6.23. Siden $-50 = -2 \cdot 25$, har vi: $25 \mid -50$. Derfor fastslår Proposisjon 2.6.21 at $\mathsf{sfd}(25, -50) = 25$.

Korollar 2.6.24. La l og n være heltall. Anta at $l \mid n$, og at $l \neq 0$. Da er $|l|$ den største felles divisoren til l og n.

Bevis. Ett av følgende utsagn er sant:

(i) $l > 0$;

(ii) $l < 0$.

Anta først at $l > 0$. Da er l et naturlig tall. Ut ifra Proposisjon 2.6.21 er l den største felles divisoren til l og n. I tillegg er $|l| = l$. Dermed er det sant at $|l|$ er den største felles divisoren til l og n.

Anta nå at $l < 0$. Da er $-l$ et naturlig tall. Derfor følger det fra Proposisjon 2.6.21 at $-l$ er den største felles divisoren til $-l$ og n. Vi gjør følgende observasjoner.

(1) Det følger fra Proposisjon 2.6.12, at $-l$ er den største felles divisoren til l og n.

(3) Siden $l < 0$, har vi: $|l| = -l$.

Dermed er det sant at $|l|$ er den største felles divisoren til l og n.

$\square$

Eksempel 2.6.25. Siden $15 = (-5) \cdot (-3)$, har vi: $-3 \mid 15$. Derfor fastslår Korollar 2.6.24 at $\mathsf{sfd}(-3, 15) = 3$.

Eksempel 2.6.26. Siden $-27 = 9 \cdot (-3)$, har vi: $-3 \mid -27$. Derfor fastslår Korollar 2.6.24 at $\mathsf{sfd}(-3, -27) = 3$.

Proposisjon 2.6.27. La l, m, og n være heltall. La d være et naturlig tall slik at d er den største felles divisoren til l og n. Anta at $n \mid m$. Da er d den største felles divisoren til $l + m$ og n.

Bevis. Oppgave O2.1.8. □

Merknad 2.6.28. Dersom $n \mid m$, er med andre ord $\mathsf{sfd}(l + m, n) = \mathsf{sfd}(l, n)$.

Eksempel 2.6.29. Vi har: $\mathsf{sfd}(12, 21) = 3$. I tillegg har vi: $21 \mid 105$. Proposisjon 2.6.27 fastslår at 3 er den største felles divisoren til $12 + 105$ og 21, altså til 117 og 21.

Eksempel 2.6.30. Vi har: $\mathsf{sfd}(-24, 32) = 8$. I tillegg har vi: $32 \mid -192$. Proposisjon 2.6.27 fastslår at 8 er den største felles divisoren til $-24 - 192$ og 32, altså til -216 og 32.

2.7 Euklids algoritme

Merknad 2.7.1. La l og n være heltall, slik at det ikke er sant at både $l = 0$ og $n = 0$. Det ser kanskje opplagt ut at det finnes et naturlig tall d som er den største felles divisoren til l og n: for å finne d, kan vi bare liste alle heltallene som er divisorer til både l og n, og finne den største av disse.

Imidlertid er dette en ineffektiv algoritme. Vi skal nå gi et bevis ved induksjon for at det finnes et naturlig tall som er den største felles divisoren til l og n. Beviset gir oss en mer effektiv algoritme for å finne den største divisoren til l og n.

I tillegg gir beviset en algoritme for å finne heltall u og v slik at

$$\mathsf{sfd}(l, n) = ul + vn.$$

Vi kommer til å se at det er svært viktig fra et teoretisk synspunkt at vi kan finne heltall x og y slik at denne ligningen er sann.

Merknad 2.7.2. Kjernen av beviset, og dermed av de to algoritmene det fører til, er det følgende lemmaet.

Lemma 2.7.3. La k, l, n, og r være heltall slik at $n = kl + r$. Anta at det finnes et naturlig tall som er den største felles divisoren til n og l, og at det finnes et naturlig tall som er den største felles divisoren til l og r. Da er $\mathsf{sfd}(n, l) = \mathsf{sfd}(l, r)$.

Bevis. La d være $\mathsf{sfd}(n, l)$. Fra definisjonen til $\mathsf{sfd}(n, l)$ har vi:

(i) $d \mid n$;

(ii) $d \mid l$;

(iii) dersom c er et naturlig tall slik at $c \mid n$ og $c \mid l$, er $c \leq d$.

Vi gjør følgende observasjoner.

(1) Fra (ii) og Korollar 2.5.18 følger det at $d \mid (-k) \cdot l$.

(2) Siden
$$n = kl + r,$$
er
$$r = n + (-k) \cdot l.$$

Fra (i), (2), og Proposisjon 2.5.24, følger det at $d \mid r$.
La c være et naturlig tall slik at:

(iv) $c \mid l$;

(v) $c \mid r$.

Vi gjør følgende observasjoner.

(3) Det følger fra (iv) og Korollar 2.5.18 at $c \mid kl$.

(4) Siden
$$n = kl + r,$$
følger det fra (3), (v) og Proposisjon 2.5.24 at $c \mid n$.

Fra (4), (iv), og (iii), følger det at $c \leq d$.
Således har vi:

(A) $d \mid l$;

(B) $d \mid r$;

(C) dersom $c \mid l$ og $c \mid r$, er $c \leq d$.

Dermed er d den største felles divisoren til l og r.

□

Merknad 2.7.4. Målet vårt er Korollar 2.7.6. Imidlertid skal vi først bevise Proposisjon 2.7.5. Da skal vi observere at Korollar 2.7.6 følger fra Proposisjon 2.7.5.

Kanskje ser Proposisjon 2.7.5 litt rar ut. For hvert par naturlige tall l og s slik at $s < l$, beviser vi på en måte at (I) og (II) er sanne mange ganger: en gang for hvert naturlig tall større enn eller likt l.

Likevel viser det seg at påstanden i Proposisjon 2.7.5 er bedre for å gjennomføre et bevis ved induksjon enn påstanden i Korollar 2.7.6, i det minste for de variantene av induksjon som vi så på i Kapittel 1.

Proposisjon 2.7.5. La n være et naturlig tall slik at $n \geq 2$. La l og s være naturlige tall slik at $s < l \leq n$. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og s;

(II) det finnes heltall u og v slik at $d = ul + vs$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. La l og s være naturlige tall slik at $s < l \leq 2$. Vi må sjekke om det finnes et naturlig tall d slik at:

(I) d er den største felles divisoren til l og s;

(II) det finnes heltall u og v slik at $d = ul + vs$.

Et par naturlige tall l og s oppfyller kravet $s < l \leq 2$ hvis og bare hvis $s = 1$ og $l = 2$. Derfor emå vi sjekke om det finnes et naturlig tall d slik at:

(A) d er den største felles divisoren til 1 og 2;

(B) det finnes heltall u og v slik at $d = 2u + v$.

Vi gjør følgende observasjoner:

(1) 1 er den største felles divisoren til 1 og 2;

(2) $1 = 0 \cdot 2 + 1 \cdot 1$.

Dermed er (A) og (B) sanne ved å la d være 1, u være 0, og v være 1. Således er proposisjonen sann når $n = 1$.

Anta nå at det har blitt bevist at proposisjonen er sann når n er et gitt naturlig tall m. La l og s være naturlige tall slik at $s < l \leq m + 1$. Vi ønsker å bevise at det finnes et naturlig tall d slik at:

(I) d er den største felles divisoren til l og s;

(II) det finnes heltall u og v slik at $d = ul + vs$.

Ut ifra Proposisjon 1.2.6 finnes det et naturlig tall k og et naturlig tall r slik at:

(i) $l = ks + r$;

(ii) $0 \leq r < s$.

Ett av følgende utsagn er sant:

(A) $r = 0$;

(B) $0 < r < s$.

Anta først at (A) er tilfellet. Vi gjør følgende observasjoner.

(1) Siden $r = 0$, er $l = ks$. Dermed er $s \mid l$. Det følger fra Proposisjon 2.6.21 at s er den største felles divisoren til l og s.

(2) Vi har:
$$s = 0 \cdot l + 1 \cdot s.$$

Dermed er (I) og (II) sanne ved å la d være s', u være 0, og v være 1. Således er proposisjonen sann når $n = m + 1$.

Anta nå at (B) er tilfellet. Siden
$$s < l \leq m + 1,$$
er $s \leq m$. Dermed er $r < s \leq m$. Fra antakelsen at proposisjonen har blitt bevist når $n = m$, følger det at det finnes et naturlig tall d' slik at:

(iii) d' er den største felles divisoren til s og r;

(iv) det finnes heltall u' og v' slik at $d' = u's + v'r$.

Vi gjør følgende observasjoner.

(1) Det følger fra (i), (iii), og Lemma 2.7.3 at d' er den største felles divisoren til l og s.

(2) Fra (i) og (iv) er
$$\begin{aligned} d' &= u's + v'r \\ &= u's - v'(l - ks) \\ &= (-v') \cdot l + (u' + kv')s. \end{aligned}$$

Dermed er (A) og (B) sanne ved å la d være d', u være v', og v være $u' + kv'$. Således er proposisjon sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Korollar 2.7.6. La n være et naturlig tall. La l være et naturlig tall slik at $l \leq n$. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og n;

(II) det finnes heltall u og v slik at $d = ul + vn$.

Bevis. Ett av følgende utsagn er sant:

(1) $l < n$;

(2) $l = n$.

Anta først at (1) er sant. Siden l er et naturlig tall, er $1 \leq l$. Derfor er $n \geq 2$. Da følger det umiddelbart fra Proposisjon 2.7.5, ved å la l i proposisjonen være n og s i proposisjonen være l, at det finnes et naturlig tall d slik at (I) og (II) er sanne.

Anta nå at (2) er sant. Vi gjør følgende observasjoner.

(1) Som fastslått i Eksempel 2.6.10, er n den største felles divisoren til n og n.

(2) Vi har:

$$n = 1 \cdot n + 0 \cdot n.$$

Dermed er (I) og (II) sanne ved å la d være n, u være 1, og v være 0.

□

Korollar 2.7.7. La n være et naturlig tall. La l være et naturlig tall. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og n;

(II) det finnes heltall u og v slik at $d = ul + vn$.

Bevis. Ett av følgende utsagn er sant:

(1) $l \leq n$;

(2) $l > n$.

Anta først at (1) er sant. Da følger det fra Korollar 2.7.6 at det finnes et naturlig tall d slik at (I) og (II) er sanne.

Anta nå at (2) er sant. Da følger det fra Korollar 2.7.6 at det finnes et naturlig tall d' og heltall u' og v' slik at:

(A) d' er den største felles divisoren til n og l;

(B) $d' = u'n + v'l$.

La d være d'. Da følger det fra (A) og Merknad 2.6.3 at (I) er sant. La u være v', og v være u'. Da følger det fra (B) at (II) er sant.

□

Merknad 2.7.8. La n være et naturlig tall, og la l være et naturlig tall slik at $l < n$. I Merknad 1.4.3 så vi at induksjon gir en algoritme for å konstruere et bevis for en matematisk påstand. Således gir beviset for Proposisjon 2.7.5 en algoritme for å få den største felles divisoren til l og n. Denne algoritmen kan fremstilles som følger.

(1) Benytt divisjonsalgoritmen for å få heltall k_0 og r_0 slik at

$$n = k_0 l + r_0.$$

Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(l, n) = \mathsf{sfd}(r_0, l)$.

(2) Benytt divisjonsalgoritmen for å få heltall k_1 og r_1 slik at

$$l = k_1 r_0 + r_1.$$

Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(r_0, l) = \mathsf{sfd}(r_1, r_0)$.

(3) Benytt divisjonsalgoritmen for å få heltall k_2 og r_2 slik at

$$r_0 = k_2 r_1 + r_2.$$

Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(r_1, r_0) = \mathsf{sfd}(r_2, r_1)$.

(4) Benytt divisjonsalgoritmen for å få heltall k_3 og r_3 slik at

$$r_1 = k_3 r_2 + r_3.$$

Ut ifra Lemma 2.7.3, er $\mathsf{sfd}(r_2, r_1) = \mathsf{sfd}(r_1, r_0)$.

(5) Slik fortsetter vi.

La oss betegne n som r_{-2} og l som r_{-1}. Til slutt finnes det et heltall i og et heltall k_i slik at vi får

$$r_{i-2} = k_i r_{i-1} + 0$$

når vi benytter divisjonsalgoritmen, altså $r_{i-1} \mid r_{i-2}$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(r_{i-1}, r_{i-2}) = r_{i-1}$. Dermed er

$$\mathsf{sfd}(l, n) = \mathsf{sfd}(r_0, l) = \mathsf{sfd}(r_1, r_0) = \mathsf{sfd}(r_2, r_1) = \cdots = \mathsf{sfd}(r_{i-1}, r_{i-2}) = r_{i-1}.$$

Således er $\mathsf{sfd}(l, n) = r_{i-1}$.

Terminologi 2.7.9. Algoritmen i Merknad 2.7.8 kalles *Euklids algoritme*.

Merknad 2.7.10. Strengt tatt er algoritmen som vi får fra beviset for Proposisjon 2.7.5 ikke *helt* den samme som algoritmen i Merknad 2.7.8. I hvert steg av algoritmen vi får fra beviset for Proposisjon 2.7.5 beviser vi flere fakta enn vi trenger for å finne den største felles divisoren til et bestemt par naturlige tall.

Alle disse faktaene behøves derimot for å gjennomføre beviset for Proposisjon 2.7.5 betraktet i sin helhet, men når vi ønsker å finne den største felles divisoren til et bestemt par naturlige tall, kan vi plukke ut de faktaene som behøves. Da får vi algoritmen i Merknad 2.7.8.

Eksempel 2.7.11. La oss se hvordan Euklids algoritme ser ut når $n = 6$ og $l = 4$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$6 = 1 \cdot 4 + 2.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(6, 4) = \mathsf{sfd}(4, 2).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$4 = 2 \cdot 2 + 0,$$

altså $2 \mid 4$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(4, 2) = 2$.

Dermed er

$$\mathsf{sfd}(6,4) = \mathsf{sfd}(4,2) = 2.$$

Eksempel 2.7.12. La oss se hvordan Euklids algoritme ser ut når $n = 20$ og $l = 8$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$20 = 2 \cdot 8 + 4.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(20,8) = \mathsf{sfd}(8,4).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 2 \cdot 4 + 0,$$

altså $4 \mid 8$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(8,4) = 4$.

Dermed er

$$\mathsf{sfd}(20,8) = \mathsf{sfd}(8,4) = 4.$$

Eksempel 2.7.13. La oss se hvordan Euklids algoritme ser ut når $n = 18$ og $l = 10$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$18 = 1 \cdot 10 + 8.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(18,10) = \mathsf{sfd}(10,8).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$10 = 1 \cdot 8 + 2.$$

Fra Lemma 2.7.3 deduserer vi at $\mathsf{sfd}(10,8) = \mathsf{sfd}(8,2)$.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 4 \cdot 2 + 0,$$

altså $2 \mid 8$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(8,2) = 2$.

Dermed er

$$\mathsf{sfd}(18,10) = \mathsf{sfd}(10,8) = \mathsf{sfd}(8,2) = 2.$$

Eksempel 2.7.14. La oss se hvordan Euklids algoritme ser ut når $n = 54$ og $l = 15$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$54 = 3 \cdot 15 + 9.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(54, 15) = \mathsf{sfd}(15, 9).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$15 = 1 \cdot 9 + 6.$$

Fra Lemma 2.7.3 deduserer vi at $\mathsf{sfd}(15, 9) = \mathsf{sfd}(9, 6)$.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$9 = 1 \cdot 6 + 3.$$

Fra Lemma 2.7.3 deduserer vi at $\mathsf{sfd}(9, 6) = \mathsf{sfd}(6, 3)$.

(4) Da benytter vi divisjonsalgoritmen for å få:

$$6 = 2 \cdot 3 + 0.$$

Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(6, 3) = 3$.

Dermed er

$$\mathsf{sfd}(54, 15) = \mathsf{sfd}(15, 9) = \mathsf{sfd}(9, 6) = \mathsf{sfd}(6, 3) = 3.$$

Merknad 2.7.15. La n være et naturlig tall, og la l være et naturlig tall slik at $l < n$. Som vi har sett, gir Euklids algoritme oss den største felles divisoren til l og n. La oss betegne $\mathsf{sfd}(l, n)$ som d.

Proposisjon 2.7.5 gir oss i tillegg en algoritme for å finne heltall x og y slik at

$$d = ul + vn.$$

Igjen beviser i hvert steg av denne algoritmen flere fakta enn vi trenger. Ved å plukke ut bare de faktaene som behøves, kan algoritmen fremstilles som følger.

(1) Benytt divisjonsalgoritmen for å få heltall k_0 og r_0 slik at

$$n = k_0 l + r_0.$$

Da er

$$r_0 = -k_0 l + n.$$

La u_0 være $-k_0$, og la v_0 være 1.

(2) Benytt divisjonsalgoritmen for å få heltall k_1 og r_1 slik at

$$l = k_1 r_0 + r_1.$$

Da er

$$\begin{aligned} r_1 &= l - k_1 r_0 \\ &= l - k_1(u_0 l + v_0 n) \\ &= (1 - u_0 k_1)l - (v_0 k_1)n. \end{aligned}$$

La u_1 være $1 - u_0 k_1$, og la v_1 være $-v_0 k_1$.

(3) Benytt divisjonsalgoritmen for å få heltall k_2 og r_2 slik at

$$r_0 = k_2 r_1 + r_2.$$

Da er

$$\begin{aligned} r_2 &= r_0 - k_2 r_1 \\ &= (u_0 l + v_0 n) - k_2(u_1 l + v_1 n) \\ &= (u_0 - u_1 k_2)l + (v_0 - v_1 k_2)n. \end{aligned}$$

La u_2 være $u_0 - u_1 k_2$, og la v_2 være $v_0 - v_1 k_2$.

(4) Benytt divisjonsalgoritmen for å få heltall k_3 og r_3 slik at

$$r_1 = k_3 r_2 + r_3.$$

Da er

$$\begin{aligned} r_3 &= r_1 - k_3 r_2 \\ &= (u_1 l + v_1 n) - k_3(u_2 l + v_2 n) \\ &= (u_1 - u_2 k_3)l + (v_1 - v_2 k_3)n. \end{aligned}$$

La u_3 være $u_1 - u_2 k_3$, og la v_3 være $v_1 - v_2 k_3$.

(5) Slik fortsetter vi.

La oss betegne n som r_{-2} og l som r_{-1}. Til slutt finnes det et heltall i og et heltall k_i slik at vi får

$$r_{i-2} = k_i r_{i-1} + 0$$

når vi benytter divisjonsalgoritmen. Fra Euklids algoritme vet vi at $d = r_{i-1}$. Vi gjør følgende.

(1) Hvis $i = 0$, er $d = l$. I dette tilfellet er $u = 1$ og $v = 0$, altså

$$d = 1 \cdot l + 0 \cdot n.$$

(2) Ellers er
$$r_{i-1} = u_{i-1}l + v_{i-1}r,$$
altså
$$d = u_{i-1}l + v_{i-1}r.$$
I dette tilfellet er $u = u_{i-1}$ og $v = v_{i-1}$.

Eksempel 2.7.16. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 6$ og $l = 4$. Fra Eksempel 2.7.11 vet vi at $\mathsf{sfd}(6, 4) = 2$. Derfor bør algoritmen gi oss heltall u og v slik at
$$2 = u \cdot 6 + v \cdot 4.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:
$$6 = 1 \cdot 4 + 2.$$
Da er
$$2 = -1 \cdot 4 + 6.$$
Vi lar u_0 være -1, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:
$$4 = 2 \cdot 2 + 0,$$
altså $2 \mid 4$.

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(6, 4) = 2$. Dermed er $u = u_0$ og $v = v_0$, altså $u = -1$ og $v = 1$. For å oppsummere, har vi:
$$2 = (-1) \cdot 4 + 1 \cdot 6.$$

Eksempel 2.7.17. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 20$ og $l = 8$. Fra Eksempel 2.7.12 vet vi at $\mathsf{sfd}(20, 8) = 4$. Derfor bør algoritmen gi oss heltall u og v slik at
$$4 = u \cdot 8 + v \cdot 20.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:
$$20 = 2 \cdot 8 + 4.$$
Da er
$$4 = -2 \cdot 8 + 1 \cdot 20.$$
Vi lar u_0 være -2, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:
$$8 = 2 \cdot 4 + 0.$$

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(20,8) = 4$. Dermed er $u = u_0$ og $v = v_0$, altså $u = -2$ og $v = 1$. For å oppsummere, har vi:

$$4 = (-2) \cdot 8 + 1 \cdot 20.$$

Eksempel 2.7.18. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 18$ og $l = 10$. Fra Eksempel 2.7.13 vet vi at $\mathsf{sfd}(18,10) = 2$. Derfor bør algoritmen gi oss heltall u og v slik at

$$2 = u \cdot 10 + v \cdot 18.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$18 = 1 \cdot 10 + 8.$$

Da er

$$8 = -1 \cdot 10 + 1 \cdot 18.$$

Vi lar u_0 være -1, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:

$$10 = 1 \cdot 8 + 1 \cdot 2.$$

Da er

$$\begin{aligned} 2 &= -1 \cdot 8 + 10 \\ &= -1 \cdot (-1 \cdot 10 + 18) + 10 \\ &= 2 \cdot 10 + (-1) \cdot 18. \end{aligned}$$

Vi lar u_1 være 2, og lar v_1 være -1.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 4 \cdot 2 + 0.$$

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(18,10) = 2$. Dermed er $u = u_1$ og $v = v_1$, altså $u = 2$ og $v = -1$. For å oppsummere, har vi:

$$2 = 2 \cdot 10 + (-1) \cdot 18.$$

Eksempel 2.7.19. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 54$ og $l = 15$. Fra Eksempel 2.7.14 vet vi at $\mathsf{sfd}(54,15) = 3$. Derfor bør algoritmen gi oss heltall u og v slik at

$$3 = u \cdot 15 + v \cdot 54.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$54 = 3 \cdot 15 + 9.$$

Da er

$$9 = -3 \cdot 15 + 1 \cdot 54.$$

Vi lar u_0 være -3, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:

$$15 = 1 \cdot 9 + 1 \cdot 6.$$

Da er

$$\begin{aligned} 6 &= -1 \cdot 9 + 15 \\ &= -1 \cdot (-3 \cdot 15 + 54) + 15 \\ &= 4 \cdot 15 + (-1) \cdot 54. \end{aligned}$$

Vi lar u_1 være 4, og lar v_1 være -1.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$9 = 1 \cdot 6 + 1 \cdot 3.$$

Da er

$$\begin{aligned} 3 &= -1 \cdot 6 + 9 \\ &= -1 \cdot (4 \cdot 15 - 54) + (-3 \cdot 15 + 54) \\ &= (-7) \cdot 15 + 2 \cdot 54. \end{aligned}$$

Vi lar u_2 være -7, og lar v_2 være 2.

(4) Da benytter vi divisjonsalgoritmen for å få:

$$6 = 2 \cdot 3 + 0.$$

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(54, 15) = 3$. Dermed er $u = u_2$ og $v = v_2$, altså $u = -7$ og $v = -2$. For å oppsummere, har vi:

$$3 = (-7) \cdot 15 + 2 \cdot 54.$$

Korollar 2.7.20. La n og l være heltall. Anta at det ikke er sant at både n og l er lik 0. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og n;

(II) det finnes heltall u og v slik at $d = ul + vn$.

Bevis. Ett av følgende utsagn er sant:

(1) $l > 0$ og $n > 0$;

(2) $l > 0$ og $n < 0$;

(3) $l < 0$ og $n > 0$;

(4) $l < 0$ og $n < 0$;

(5) $l \neq 0$ og $n = 0$.

(6) $l = 0$ og $n \neq 0$.

Anta først at (1) er sant. Da er l og n naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d slik at (I) og (II) er sanne.

Anta nå at (2) er sant. Da er l og $-n$ naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d' slik at:

(A) d' er den største felles divisoren til l og $-n$;

(B) det finnes heltall u' og v' slik at $d' = u'l + v'(-n)$.

La d være d'. Det følger fra (A) og Korollar 2.6.15 at d er den største felles divisoren til l og $-(-n)$, altså til l og n. Dermed er (I) sant.

La u være u', og la v være $-v'$. Ut ifra (B) er

$$\begin{aligned} d &= u'l + v'(-n) \\ &= u'l + (-v')n \\ &= ul + vn. \end{aligned}$$

Dermed er (II) sant.

Anta nå at (3) er sant. Da er $-l$ og n naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d' slik at:

(A) d' er den største felles divisoren til $-l$ og n;

(B) det finnes heltall u' og v' slik at $d' = u'(-l) + v'n$.

La d være d'. Det følger fra (A) og Proposisjon 2.6.12 at d er den største felles divisoren til $-(-l)$ og n, altså til l og n. Dermed er (I) sant.

La u være $-u'$, og la v være v'. Ut ifra (B) er

$$\begin{aligned} d &= u'(-l) + v'n \\ &= (-u')l + v'n \\ &= ul + vn. \end{aligned}$$

Dermed er (II) sant.

Anta nå at (4) er sant. Da er $-l$ og $-n$ naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d' slik at:

(A) d' er den største felles divisoren til $-l$ og $-n$;

(B) det finnes heltall u' og v' slik at $d' = u'(-l) + v'(-n)$.

La d være d'. Det følger fra (A) og Korollar 2.6.18 at d er den største felles divisoren til $-(-l)$ og $-(-n)$, altså til l og n. Dermed er (I) sant.

La u være $-u'$, og la v være $-v'$. Ut ifra (B) er

$$\begin{aligned} d &= u'(-l) + v'(-n) \\ &= (-u')l + (-v')n \\ &= ul + vn. \end{aligned}$$

Dermed er (II) sant.

Anta nå at (5) er sant. Alle heltall er divisorer til 0. Den største divisoren til l er l. Derfor er l den største felles divisoren til l og 0. La d være l, la x være 1, og la y være 0. Da er

$$l = 1 \cdot l + 0 \cdot 0.$$

Dermed er (I) og (II) sanne.

Anta nå at (6) er sant. Alle heltall er divisorer til 0. Den største divisoren til n er n. Derfor er n den største felles divisoren til 0 og n. La d være n, la x være 0, og la y være 1. Da er

$$n = 0 \cdot 0 + 1 \cdot n.$$

Dermed er (I) og (II) sanne.

□

Eksempel 2.7.21. Beviset for Korollar 2.7.20 fastslår at $\mathsf{sfd}(20, -8)$ kan finnes ved å benytte Euklids algoritme når $n = 20$ og $l = 8$. Vi gjorde dette i Eksempel 2.7.12. Vi har:

$$\mathsf{sfd}(20, -8) = \mathsf{sfd}(20, 8) = 4.$$

I tillegg fastslår beviset for Korollar 2.7.20 at vi kan finne heltall u og v slik at

$$4 = u \cdot (-8) + v \cdot 20$$

på følgende måte.

(1) Benytt algoritmen i Merknad 2.7.15 for å få heltall u' og v' slik at

$$4 = u' \cdot 8 + v' \cdot 20.$$

Vi gjorde dette i Eksempel 2.7.17. Vi har:

$$4 = (-2) \cdot 8 + 1 \cdot 20.$$

(2) La u være 2, og la v være 1.

Da er

$$\begin{aligned} u \cdot (-8) + v \cdot 20 &= 2 \cdot (-8) + 1 \cdot 20 \\ &= (-2) \cdot 8 + 1 \cdot 20 \\ &= 4. \end{aligned}$$

Eksempel 2.7.22. Beviset for Korollar 2.7.20 fastslår at $\mathsf{sfd}(-18, 10)$ kan finnes ved å benytte Euklids algoritme når $n = 18$ og $l = 10$. Vi gjorde dette i Eksempel 2.7.13. Vi har:

$$\mathsf{sfd}(-18, 10) = \mathsf{sfd}(18, 10) = 2.$$

I tilleg fastslår beviset for Korollar 2.7.20 at vi kan finne heltall u og v slik at

$$2 = u \cdot 10 + v \cdot (-18)$$

på følgende måte.

(1) Benytt algoritmen i Merknad 2.7.15 for å få heltall u' og v' slik at

$$2 = u' \cdot 10 + v' \cdot 18.$$

Vi gjorde dette i Eksempel 2.7.18. Vi har:

$$2 = 2 \cdot 10 + (-1) \cdot 18.$$

(2) La u være 2, og la v være 1.

Da er

$$\begin{aligned} u \cdot 10 + v \cdot (-18) &= 2 \cdot 10 + 1 \cdot (-18) \\ &= 2 \cdot 10 + (-1) \cdot 18 \\ &= 2. \end{aligned}$$

Eksempel 2.7.23. Beviset for Korollar 2.7.20 fastslår at $\mathsf{sfd}(-15, -54)$ kan finnes ved å benytte Euklids algoritme når $n = 54$ og $l = 15$. Vi gjorde dette i Eksempel 2.7.14. Vi har:

$$\mathsf{sfd}(-15, -54) = \mathsf{sfd}(54, 15) = 3.$$

I tilleg fastslår beviset for Korollar 2.7.20 at vi kan finne heltall u og v slik at

$$3 = u \cdot (-54) + v \cdot (-15)$$

på følgende måte.

(1) Benytt algoritmen i Merknad 2.7.15 for å få heltall u' og v' slik at

$$3 = u' \cdot 15 + v' \cdot 54.$$

Vi gjorde dette i Eksempel 2.7.19. Vi har:

$$3 = (-7) \cdot 15 + 2 \cdot 54.$$

(2) La u være -2, og la v være 7.

Da er

$$\begin{aligned} u \cdot (-54) + v \cdot (-15) &= (-2) \cdot (-54) + 7 \cdot (-15) \\ &= 2 \cdot 54 + (-7) \cdot 15 \\ &= (-7) \cdot 15 + 2 \cdot 54 \\ &= 3. \end{aligned}$$

Oppgaver

O2.1 Oppgaver i eksamens stil

Oppgave O2.1.8. La l, m, og n være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(l, n) = d$. Anta at $n \mid m$. Bevis at $\mathsf{sfd}(l + m, n) = d$. *Tips*: Benytt ligningen $l = (l + m) - m$ i løpet av beviset ditt.

Oppgave O2.1.9. For hvert av de følgende heltallene l og n, finn $\mathsf{sfd}(l, n)$, og finn heltall u og v slik at $\mathsf{sfd}(l, n) = ul + vn$. Benytt Euklids algoritme i løpet av svarene dine.

(1) $l = 231$, $n = 616$.

(2) $l = -153$, $n = 391$.

(3) $l = -168$, $n = -420$,