Forelesning 10 — torsdag den 18. september

2.8 Relativt primiske heltall og Euklids lemma

Merknad 2.8.1. Korollar 2.7.20 er et svært viktig teoretisk verktøy. I denne og neste del av kapittelet skal vi se på noen eksempler som kan hjelpe oss å få en følelse for hvordan Korollar 2.7.20 kan benyttes.

Proposisjon 2.8.2. La l og n være heltall. La k være et naturlig tall. La d være et naturlig tall slik at d er den største felles divisoren til l og n. Da er kd den største felles divisoren til kl og kn.

Bevis. Siden d er den største felles divisoren til l og n, har vi:

(1) $d \mid l$;

(2) $d \mid n$.

Fra (1) og Korollar 2.5.21 deduserer vi at $kd \mid kl$. Fra (2) og Korollar 2.5.21 deduserer vi at $kd \mid kn$.

La c være et naturlig tall slik at:

(i) $c \mid kl$;

(ii) $c \mid kn$.

Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 2.7.20 finnes det heltall u og v slik at

$$d = ul + vn.$$

Det følger at

$$kd = ukl + ukn.$$

(2) Fra (i) og Korollar 2.5.18 følger det at $c \mid ukl$.

(3) Fra (ii) og Korollar 2.5.18 følger det at $c \mid vkn$.

(4) Fra (2), (3), og Proposisjon 2.5.24 følger det at $c \mid ukl + ukn$.

(5) Fra (1) og (4) følger det at

$$c \mid kd.$$

(6) Siden k og d er naturlige tall, er kd et naturlig tall.

(7) Siden c er et naturlig tall, følger det fra (5), (6), og Proposisjon 2.5.30 at $c \leq kd$.

For å oppsummere beviset så langt, har vi bevist at:

(1) $kd \mid kl$;

(2) $kd \mid kn$;

(3) dersom $c \mid kl$ og $c \mid kn$, er $c \leq kd$.

Dersom er kd den største felles divisoren til kl og kn.

□

Eksempel 2.8.3. Vi har: $\mathsf{sfd}(18, 24) = 6$. Siden $90 = 5 \cdot 18$ og $120 = 5 \cdot 24$, følger det fra Proposisjon 2.8.2 at

$$\mathsf{sfd}(90, 120) = 5 \cdot \mathsf{sfd}(18, 24) = 5 \cdot 6 = 30.$$

Eksempel 2.8.4. Vi har: $\mathsf{sfd}(13, -21) = 1$. Siden $91 = 7 \cdot 13$ og $-147 = 7 \cdot -21$, følger det fra Proposisjon 2.8.2 at

$$\mathsf{sfd}(91, -147) = 7 \cdot \mathsf{sfd}(13, -21) = 7 \cdot 1 = 7.$$

Korollar 2.8.5. La l og n være heltall. La k være et heltall slik at $k \neq 0$. La d være et naturlig tall slik at d er den største felles divisoren til l og n. Da er $|k| \cdot d$ den største felles divisoren til kl og kn.

Bevis. Ett av følgende utsagn er sant:

(1) $k > 0$;

(2) $k < 0$.

Anta først at (1) er sant. Da er k et naturlig tall, og $|k|\, k$. Dermed følger utsagnet fra Proposisjon 2.8.2.

Anta nå at (2) er sant. Da er $-k$ et naturlig tall, og $|k| = -k$. Det følger fra Proposisjon 2.8.2 at $|k| \cdot d$ er den største felles divisoren til $(-k) \cdot l$ og $(-k) \cdot n$. Fra Korollar 2.6.18 følger det at $|k|$ er den største felles divisoren til $-(-k) \cdot l$ og $-(-k) \cdot n$, altså til l og n. □

Eksempel 2.8.6. Vi har: $\mathsf{sfd}(14, 63) = 7$. Det følger fra Korollar 2.8.5 at

$$\mathsf{sfd}(-154, -693) = |-11| \cdot 7 = 11 \cdot 7 = 77.$$

Eksempel 2.8.7. Vi har: $\mathsf{sfd}(-76, 20) = 4$. Det følger fra Korollar 2.8.5 at

$$\mathsf{sfd}(380, -100) = |-5| \cdot 4 = 5 \cdot 4 = 20.$$

Proposisjon 2.8.8. La l og n være heltall. Da er $\mathsf{sfd}(l,n) = 1$ hvis og bare hvis det finnes heltall u og v slik at

$$1 = ul + vn.$$

Bevis. Anta først at $\mathsf{sfd}(l,n) = 1$. Da følger det fra Korollar 2.7.20 at det finnes heltall u og v slik at

$$1 = ul + vn.$$

Anta istedenfor at det finnes heltall u og v slik at

$$1 = ul + vn.$$

La c være et naturlig tall slik at:

(i) $c \mid l$;

(ii) $c \mid n$.

Vi gjør følgende observasjoner.

(1) Det følger fra (1) og Korollar 2.5.18 at $c \mid ul$.

(2) Det følger fra (2) og Korollar 2.5.18 at $c \mid vn$.

(3) Det følger fra (1), (2), og Proposisjon 2.5.24 at $c \mid ul + vn$.

Det følger fra (3) og ligningen $1 = ul + vn$ at $c \mid 1$.

Dermed har vi bevist at $c \mid 1$ dersom $c \mid l$ og $c \mid n$. I tillegg har vi: $1 \mid l$ og at $1 \mid n$. Vi konkluderer at $\mathsf{sfd}(l,n) = 1$.

□

Eksempel 2.8.9. Vi har:

$$1 = (-2) \cdot 14 + 29.$$

Derfor fastslår Proposisjon 2.8.8 at $\mathsf{sfd}(14,29) = 1$.

Eksempel 2.8.10. Vi har:

$$1 = 5 \cdot 13 - 8 \cdot 8.$$

Derfor fastslår Proposisjon 2.8.8 at $\mathsf{sfd}(13,8) = 1$.

Merknad 2.8.11. Proposisjon 2.8.8 stemmer ikke om vi bytter 1 med et annet heltall. For eksempel er

$$2 = 3 \cdot 3 + (-1) \cdot 7,$$

men $\mathsf{sfd}(3,7) \neq 2$. Faktisk er $\mathsf{sfd}(3,7) = 1$.

Terminologi 2.8.12. La l og n være heltall slik at $\mathsf{sfd}(l,n) = 1$. Da sier vi at l og n er *relativt primiske*.

Proposisjon 2.8.13. La l og n være heltall, og la d være et heltall slik at $\mathsf{sfd}(l,n) = d$. La k_l være heltallet slik at $l = k_l d$, og la k_n være heltallet slik at $n = k_n d$. Da er $\mathsf{sfd}(k_l, k_n) = 1$.

Bevis. Ut ifra Korollar 2.7.20, finnes det heltall u og v slik at

$$d = ul + vn.$$

Derfor er

$$d = uk_l d + uk_n n,$$

altså

$$d = d(uk_l + uk_n).$$

Det følger fra Proposisjon 2.2.25 at

$$1 = uk_l + uk_n.$$

Fra Proposisjon 2.8.8 konkluderer vi at $\mathsf{sfd}(k_l, k_n) = 1$. □

Merknad 2.8.14. Fra definisjonen til $\mathsf{sfd}(l,n)$ vet vi at $d \mid l$ og at $d \mid r$. Derfor finnes det heltall k_l og k_n slik at ligningene i Proposisjon 2.8.13 er sanne. Ut ifra Korollar 2.2.20 er dessutten k_l og k_n de eneste heltallene slik at disse to ligningene er sanne.

Eksempel 2.8.15. Vi har:

$$\mathsf{sfd}(108, 45) = 9.$$

Derfor fastslår Proposisjon 2.8.13 at

$$\mathsf{sfd}(12, 5) = 1.$$

Eksempel 2.8.16. Vi har:

$$\mathsf{sfd}(-48, 27) = 3.$$

Derfor fastslår Proposisjon 2.8.13 at

$$\mathsf{sfd}(-16, 9) = 1.$$

Proposisjon 2.8.17. La l, l', og n være heltall. Anta at $l \mid n$ og at $l' \mid n$. Dersom $\mathsf{sfd}(l, l') = 1$, har vi: $l \cdot l' \mid n$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $l \mid n$, finnes det et heltall k_l slik at $n = k_l l$.

(2) Siden $l' \mid n$, finnes det et heltall $k_{l'}$ slik at $n = k_{l'} l'$.

(3) Ut ifra Korollar 2.7.20 finnes det heltall u og v slik at

$$1 = ul + vl'.$$

Det følger fra (1) – (3) at

$$\begin{aligned} n &= uln + vl'n \\ &= ulk_{l'}l' + vl'k_l l \\ &= (uk_{l'} + vk_l)ll'. \end{aligned}$$

Dermed har vi: $ll' \mid n$.

□

Eksempel 2.8.18. Vi har: $5 \mid 80$ og $8 \mid 80$. Siden $\mathsf{sfd}(5, 8) = 1$, fastslår Proposisjon 2.8.17 at $5 \cdot 8 \mid 40$, altså at $40 \mid 80$.

Eksempel 2.8.19. Vi har: $-9 \mid 882$ og $-14 \mid 882$. Siden $\mathsf{sfd}(-9, -14) = 1$, fastslår Proposisjon 2.8.17 at $-9 \cdot -14 \mid 882$, altså at $126 \mid 882$.

Merknad 2.8.20. Proposisjon 2.8.17 stemmer ikke om $\mathsf{sfd}(l, n) \neq 1$. For eksempel er $\mathsf{sfd}(9, 15) = 3$, og vi har: $9 \mid 45$ og $15 \mid 45$. Men $9 \cdot 15 = 135$, og det er ikke sant at $135 \mid 45$.

Merknad 2.8.21. Den følgende proposisjonen er kjernen til et teorem vi kommer til å bevise i det neste kapitelet. Det kalles noen ganger *Euklids lemma*.

Proposisjon 2.8.22. La l, n, og n' være heltall slik at $l \mid n \cdot n'$. Dersom $\mathsf{sfd}(l, n) = 1$, har vi: $l \mid n'$.

Bevis. Siden $\mathsf{sfd}(l, n) = 1$, fastslår Korollar 2.7.20 at det finnes heltall u og v slik at

$$1 = ul + vn.$$

Derfor er

$$n' = (u \cdot l) \cdot n' + (v \cdot n) \cdot n') = (u \cdot n') \cdot l + v \cdot (n \cdot n').$$

Vi gjør følgende observasjoner.

(1) Siden $l \mid l$, følger det fra Korollar 2.5.18 at $l \mid (u \cdot n') \cdot l$.

(2) Fra Korollar 2.5.18 og antakelsen at $l \mid n \cdot n'$, har vi: $l \mid v \cdot (n \cdot n')$.

Fra (1), (2), og Proposisjon 2.5.24, følger det at $l \mid l \cdot (u \cdot n') + v \cdot (n \cdot n')$. Dermed har vi: $l \mid n'$.

□

Eksempel 2.8.23. Vi har: $\mathsf{sfd}(9, 25) = 1$. I tillegg har vi: $9 \mid 1125$. Siden $1125 = 25 \cdot 45$, fastslår Proposisjon 2.8.22 at

$$9 \mid 45.$$

Eksempel 2.8.24. Vi har: $\mathsf{sfd}(-17, 24) = 1$. I tillegg har vi: $-17 \mid 2248$. Siden $2248 = 24 \cdot 102$, fastslår Proposisjon 2.8.22 at

$$-17 \mid 102.$$

Merknad 2.8.25. Proposisjon 2.8.22 stemmer ikke om $\mathsf{sfd}(l,n) \neq 1$. For eksempel er $\mathsf{sfd}(2,4) = 2$, og $2 \mid 28$. Vi har: $28 = 4 \cdot 7$, men det er ikke sant at $2 \mid 7$.

Proposisjon 2.8.26. La l, m, og n være heltall. La d være et naturlig tall slik at d er den største felles divisoren til l og m. Anta at $1 = \mathsf{sfd}(l,n)$. Da er d den største felles divisoren til l og mn.

Bevis. Oppgave O2.1.10. □

Merknad 2.8.27. Dersom $1 = \mathsf{sfd}(l,n)$, er med andre ord $\mathsf{sfd}(l,m) = \mathsf{sfd}(l,mn)$.

Eksempel 2.8.28. Vi har: $\mathsf{sfd}(33,44) = 11$. I tillegg har vi: $\mathsf{sfd}(33,50) = 1$. Proposisjon 2.8.26 fastslår at $\mathsf{sfd}(33, 44 \cdot 50) = \mathsf{sfd}(33,44)$, altså at $\mathsf{sfd}(33,2200) = 11$.

Eksempel 2.8.29. Vi har: $\mathsf{sfd}(18,-27) = 9$. I tillegg har vi: $\mathsf{sfd}(18,29) = 1$. Proposisjon 2.8.26 fastslår at $\mathsf{sfd}(18, -27 \cdot 29) = \mathsf{sfd}(18,-27)$, altså at $\mathsf{sfd}(18,-783) = 9$.

Proposisjon 2.8.30. La x, y, og z være heltall. Da er $\mathsf{sfd}(x,yz) = 1$ om og bare om $\mathsf{sfd}(x,y) = 1$ og $\mathsf{sfd}(x,z) = 1$.

Bevis. Anta først at $\mathsf{sfd}(x,y) = 1$ og $\mathsf{sfd}(x,z) = 1$. Siden $\mathsf{sfd}(x,y) = 1$, følger det fra Proposisjon 2.8.26 at $\mathsf{sfd}(x,yz) = \mathsf{sfd}(x,z)$. Siden $\mathsf{sfd}(x,z) = 1$, konkluderer vi at $\mathsf{sfd}(x,yz) = 1$.

Anta istedenfor at $\mathsf{sfd}(x,yz) = 1$. La w være et naturlig tall slik at $w \mid x$ og $w \mid y$. Vi gjør følgende observasjoner.

(1) Siden $w \mid y$, følger det fra Korollar **??** at $w \mid yz$.

(2) Siden $w \mid x$ og $w \mid yz$, følger det fra antakelsen $\mathsf{sfd}(x,yz) = 1$ at $w = 1$.

Således har vi bevist at, dersom w er et naturlig tall slik at $w \mid x$ og $w \mid y$, er $w = 1$. Dermed er $\mathsf{sfd}(x,y) = 1$.

Et lignende argument fastslår at, dersom w er et naturlig tall slik at $w \mid x$ og $w \mid z$, er $w = 1$. Dermed er $\mathsf{sfd}(x,z) = 1$.

□

Eksempel 2.8.31. Ved å benytte Euklids algoritme, finner vi at $\mathsf{sfd}(8,1155) = 1$. Siden $1155 = 33 \cdot 35$, fastslår da Proposisjon 2.8.30 at $\mathsf{sfd}(8,33) = 1$ og $\mathsf{sfd}(8,35) = 1$. Dette er riktignok sant.

Eksempel 2.8.32. Siden $\mathsf{sfd}(9,-26) = 1$ og $\mathsf{sfd}(9,77) = 1$, fastslår Proposisjon 2.8.30 at $\mathsf{sfd}(9,(-26) \cdot 77) = 1$, altså at $\mathsf{sfd}(9,-2002) = 1$. Ved å benytte Euklids algoritme, finner vi at dette riktignok er sant.

2.9 Lineære diofantiske ligninger

Merknad 2.9.1. La oss se på ligningen

$$x + 2y = 0.$$

Det er lett å finne alle heltallene x og y slik at denne ligningen er sann. For hvert heltall z, er $x = -2z$ og $y = z$ en løsning. Disse er de eneste løsningene. Således har vi for eksempel de følgende løsningene:

(1) $x = 2$ og $y = 1$;

(2) $x = 8$ og $y = 4$;

(3) $x = -18$, $y = -9$.

La oss se istedenfor på ligningen

$$2x + 4y = 3.$$

Det finnes ikke noe heltall x og y slik at denne ligningen er sann. For alle heltall x og y er $2x + 4y$ et partall, mens 3 er et oddetall. Derfor er det umulig at $2x + 4y$ kan være lik 3.

La nå a, b, og c være heltall. Ved hjelp av begrepet «største felles divisor», skal vi i denne delen av kapittelet se på hvordan vi kan finne alle heltallsløsningene til en hvilken som helst ligning

$$ax + by = c.$$

Terminologi 2.9.2. La a, b, og c være heltall. Når vi er interessert i heltall x og y slik at

$$ax + by = c,$$

kalles denne ligningen en *lineær diofantisk ligning*.

Merknad 2.9.3. En stor del av tallteori handler om heltallsløsninger til ligninger. Generelt sett er det veldig vanskelig å finne alle heltallsløsningene til en gitt ligningen: i dagens forskning innen tallteori benytter matematikere svært sofistikerte og abstrakte verktøy for å få en forståelse. Likevel er i mange tilfeller løsningene fremdeles et mysterium.

Proposisjon 2.9.4. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vb$. Anta at $d \mid c$, altså at det finnes et heltall k slik at $c = kd$. Da er $x = ku$ og $y = kv$ en løsning til ligningen

$$ax + by = c.$$

Bevis. Vi regner som følger:

$$\begin{aligned} ax + by &= a(ku) + b(kv) \\ &= k(au + bv) \\ &= kd \\ &= c. \end{aligned}$$

□

Merknad 2.9.5. Dette beviset er lett. Imidlertid er proposisjonen langt fra triviell. Det er Korollar 2.7.20, altså Euklids algoritme, som gir oss muligheten til å løse ligningen

$$ax + by = c$$

når $d \mid c$, ved å fastslå at vi kan finne heltall u og v slik at $d = ua + bv$.

Eksempel 2.9.6. Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(63, 49) = 7$;

(2) $7 = (-3) \cdot 63 + 4 \cdot 49$.

Siden $252 = 36 \cdot 7$, har vi i tillegg: $7 \mid 252$. Derfor fastslår Proposisjon 2.9.4 at $x = 36 \cdot (-3)$ og $y = 36 \cdot 4$, altså $x = -108$ og $y = 144$, er en løsning til ligningen

$$63x + 49y = 252.$$

Eksempel 2.9.7. Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(286, 455) = 13$;

(2) $13 = 8 \cdot 286 + (-5) \cdot 455$.

Siden

$$-429 = (-33) \cdot 13,$$

har vi i tillegg: $13 \mid -429$. Derfor fastslår Proposisjon 2.9.4 at $x = (-33) \cdot 8$ og $y = (-33) \cdot (-5)$, altså $x = -264$ og $y = 165$, er en løsning til ligningen

$$286x + 455y = -429.$$

Eksempel 2.9.8. Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(-24, 136) = 8$;

(2) $8 = (-6) \cdot (-24) + (-1) \cdot 136$.

Siden $1072 = 134 \cdot 8$, har vi i tillegg: $8 \mid 1072$. Derfor fastslår Proposisjon 2.9.4 at $x = 134 \cdot (-6)$ og $y = 134 \cdot (-1)$, altså $x = -804$ og $y = -134$, er en løsning til ligningen

$$-24x + 136y = 1072.$$

Proposisjon 2.9.9. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a,b) = d$. La x og y være heltall slik at

$$ax + by = c.$$

Da er $d \mid c$.

Bevis. Ut ifra definisjonen til $\mathsf{sfd}(a,b)$ er $d \mid a$ og $d \mid b$. Derfor finnes det et heltall k_a slik at $a = k_a d$, og et heltall k_b slik at $b = k_b d$. Nå regner vi som følger:

$$\begin{aligned} c &= ax + by \\ &= k_a dx + k_b dy \\ &= (k_a x + k_b y)d. \end{aligned}$$

Dermed er $d \mid c$. □

Eksempel 2.9.10. Ved å benytte Euklids algoritme får vi: $\mathsf{sfd}(57, 133) = 19$. Siden det ikke er sant at $19 \mid 36$, følger det fra Proposisjon 2.9.9 at ligningen

$$57x + 133y = 36$$

har ingen heltallsløsning.

Eksempel 2.9.11. Vi har: $\mathsf{sfd}(-12, -18) = 6$. Siden det ikke er sant at $6 \mid 10$, følger det fra Proposisjon 2.9.9 at ligningen

$$-12x - 18y = 10$$

har ingen heltallsløsning.

Korollar 2.9.12. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a,b) = d$. Ligningen

$$ax + by = c$$

har en heltallsløsning hvis og bare hvis $d \mid c$.

Bevis. Følger umiddelbart fra Proposisjon 2.9.4 og Proposisjon 2.9.9. □

Oppgaver

O2.1 Oppgaver i eksamens stil

Oppgave O2.1.10. La l, m, og n være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(l, m) = d$. Anta at $\mathsf{sfd}(l, n) = 1$. Bevis at $\mathsf{sfd}(l, mn) = d$. *Tips*: Gjør først følgende, og benytt da (3) i løpet av beviset ditt.

(1) La c være et heltall slik at $c \mid l$, og la s være et heltall. Bevis at $\mathsf{sfd}(c, s) \leq \mathsf{sfd}(l, s)$.

(2) La c være et heltall slik at $c \mid l$. Deduser fra (1) og antakelsen at $\mathsf{sfd}(l, n) = 1$ at $\mathsf{sfd}(c, n) = 1$.

(3) Dersom c er et naturlig tall slik at $c \mid mn$, deduser fra (2) og Proposisjon 2.8.22 at $c \mid m$.

Oppgave O2.1.11. For hver av de følgende ligningene, finn en heltall løsning dersom det er mulig. Hvis det ikke er mulig, forklar hvorfor.

(1) $396x - 165y = 462$.

(2) $-546x + 312y = -317$.

(3) $288x + 186y = 6138$.