Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

TMA4140 Diskret Matematikk Høst 2021

Løsningsforslag — Øving 4

Seksjon 4.1

6 Dersom $a \mid c$ og $b \mid d$, betyr dette at det eksisterer heltall s og t slik at $c = as$ og $d = bt$. Multipliserer vi ligningene med hverandre får vi $cd = ab(st)$, som betyr at $ab \mid cd$, som ønsket.

17 **d)** Setter inn for $a \equiv 4 \pmod{13}$ og $b \equiv 9 \pmod{13}$, og får

$$2a + 3b \equiv 2 \cdot 4 + 3 \cdot 9 \equiv 35 \equiv 9 \pmod{13}.$$

44 Vi har to tilfeller; enten er n et partall eller så er n et oddetall. Dersom n er et partall kan det skrives $n = 2k$, hvor k er et heltall. Dermed er $n^2 = (2k)^2 = 4k^2$, som betyr at $n^2 \equiv 0 \pmod 4$. Dersom n er et oddetall kan det skrives $n = 2k+1$, hvor k er et heltall. Dermed er $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, som betyr at $n^2 \equiv 1 \pmod 4$. □

Seksjon 4.2

3 **b)** $(10\,0000\,0001)_2 = (2^9 + 1)_{10} = (513)_{10}$.

7 **b)** Bruker Table 1 på side 325 og får $(135AB)_{16} = (1\,0011\,0101\,1010\,1011)_2$.

24 **a)** Vi summerer "for hånd" i base 16:

$$\begin{array}{r} {\scriptstyle 1\ 1} \\ 1\ A\ \mathrm{E} \\ +\ \mathrm{B}\ \mathrm{B}\ \mathrm{C} \\ \hline \mathrm{D}\ 6\ \mathrm{A} \end{array}$$

For å regne ut produktet er det enklest å gå via base 10. Det gir

$$(1AE)_{16} \cdot (BBC)_{16} = (430)_{10} \cdot (3004)_{10} = (1291720)_{10} = (13\mathrm{B}5\mathrm{C}8)_{16}.$$

Seksjon 4.3

6 Antall nuller på slutten av et tall tilsvarer antall ganger $10\,(= 2 \cdot 5)$ opptrer som en faktor i tallet. Faktoren 2 opptrer flere ganger som faktor i 100! enn 5. Dermed er antall faktorer

av 10 i 100! likt antall faktorer av 5. Hver av de tjue tallene $5, 10, 15, \ldots, 95, 100$ inneholder en faktor av 5. Men blant disse inneholder de fire tallene $25, 50, 75, 100$ en faktor av 5 mer (Eks: $25 = 5 \cdot 5$), altså disse har 5^2 som faktor og vi må følgelig telle disse to ganger. Ingen faktorer i 100! har 5^3 som faktor siden $5^3 = 125 > 100$. Det er altså 24 faktorer av 5 (og dermed 10) i 100!, som betyr at det er eksakt 24 nuller på slutten av 100!.

12 Vi følger hintet. Det er n tall i følgen $(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+(n+1)$. Det første av disse er sammensatt fordi det deles av 2. Det andre er sammensatt fordi det deles av 3. Det tredje er sammensatt fordi det deles av 4 osv... Dermed er det siste tallet sammensatt fordi det deles av $n+1$. Dette viser at det finnes n sammensatte tall for enhver n. □

33 **c)** Bruker Euklids algoritme:

$$\begin{aligned} 1331 &= 1 \cdot 1001 + 330 \\ 1001 &= 3 \cdot 330 + 11 \\ 330 &= 30 \cdot 11 + 0 \end{aligned}$$

Altså er $\gcd(1331, 1001) = 11$.

d) Bruker Euklids algoritme:

$$\begin{aligned} 54321 &= 4 \cdot 12345 + 4941 \\ 12345 &= 2 \cdot 4941 + 2463 \\ 4941 &= 2 \cdot 2463 + 15 \\ 2463 &= 164 \cdot 15 + 3 \\ 15 &= 5 \cdot 3 + 0 \end{aligned}$$

Altså er $\gcd(54321, 12345) = 3$.

39 **e)** Bruker først Euklids algoritme for å finne $\gcd(213, 117)$:

$$\begin{aligned} 213 &= 1 \cdot 117 + 96 \\ 117 &= 1 \cdot 96 + 21 \\ 96 &= 4 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Største felles divisor er altså 3. For å skrive den som en linærkombinasjon av de originale

tallene går vi nå "baklengs" gjennom utregningene over.

$$\begin{aligned}
3 &= 12 - 1 \cdot 9 \\
&= 12 - 1 \cdot (21 - 1 \cdot 12) \\
&= 2 \cdot 12 + (-1) \cdot 21 \\
&= 2 \cdot (96 - 4 \cdot 21) + (-1) \cdot 21 \\
&= (-9) \cdot 21 + 2 \cdot 96 \\
&= (-9) \cdot (117 - 1 \cdot 96) + 2 \cdot 96 \\
&= 11 \cdot 96 + (-9) \cdot 117 \\
&= 11 \cdot (213 - 1 \cdot 117) + (-9) \cdot 117 \\
&= 11 \cdot 213 + (-20) \cdot 117
\end{aligned}$$

Vi har dermed $3 = 11 \cdot 213 + (-20) \cdot 117$.

49 Fordi annenhvert tall er delelig med 2 må $n(n+1)(n+2)$ deles av 2. Ettersom hvert tredje tall deles av 3 må $n(n+1)(n+2)$ deles av 3. Siden $n(n+1)(n+2)$ har 2 og 3 i sin primtallsfaktorisering må det også deles av $2 \cdot 3 = 6$. □

Seksjon 4.4

5 **b)** Euklids algoritme gir

$$\begin{aligned}
141 &= 7 \cdot 19 + 8 \\
19 &= 2 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1.
\end{aligned}$$

Går baklengs og får

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= 3 \cdot 3 + (-1) \cdot 8 \\
&= 3 \cdot (19 - 2 \cdot 8) + (-1) \cdot 8 \\
&= (-7) \cdot 8 + 3 \cdot 19 \\
&= (-7) \cdot (141 - 7 \cdot 19) + 3 \cdot 19 \\
&= (-7) \cdot 141 + 52 \cdot 19.
\end{aligned}$$

Altså er 52 en invers til 19 modulo 141. Forøvrig er alle andre tall som er kongruent med 52 modulo 141 også inverser til 19, altså alle tall x som kan skrives på formen $x = 52 + 141k$, hvor k er et heltall.

c) Euklids algoritme gir

$$\begin{aligned}
89 &= 1 \cdot 55 + 34 \\
55 &= 1 \cdot 34 + 21 \\
34 &= 1 \cdot 21 + 13 \\
21 &= 1 \cdot 13 + 8 \\
13 &= 1 \cdot 8 + 5 \\
8 &= 1 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Går baklengs og får

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - (5 - 1 \cdot 3) \\
&= 2 \cdot 3 + (-1) \cdot 5 \\
&= 2 \cdot (8 - 1 \cdot 5) + (-1) \cdot 5 \\
&= (-3) \cdot 5 + 2 \cdot 8 \\
&= (-3) \cdot (13 - 1 \cdot 8) + 2 \cdot 8 \\
&= (-3) \cdot 13 + 5 \cdot 8 \\
&= (-3) \cdot 13 + 5 \cdot (21 - 1 \cdot 13) \\
&= (-8) \cdot 13 + 5 \cdot 21 \\
&= (-8) \cdot (34 - 1 \cdot 21) + 5 \cdot 21 \\
&= (-8) \cdot 34 + 13 \cdot 21 \\
&= (-8) \cdot 34 + 13 \cdot (55 - 1 \cdot 34) \\
&= (-21) \cdot 34 + 13 \cdot 55 \\
&= (-21) \cdot (89 - 1\dot{5}5) + 13 \cdot 55 \\
&= (-21) \cdot 89 + 34 \cdot 55
\end{aligned}$$

Altså er 34 en invers til 55 modulo 89, dvs. $55^{-1} \equiv 34 \pmod{89}$. Den observante leser legger kanskje merke til at Fibonacci tallene gjør en opptreden her. Vi ser fra dette at $F_{10}^{-1} \equiv F_9 \pmod{F_{11}}$, der F_n er det n'te Fibonacci-tallet.

8 Vi ønsker å vise at når a og m er heltall slik at $m > 2$ og $\gcd(a, m) \geq 2$ så har ikke a noen invers modulo m. Vi utfører et selvmotsigelsesbevis.

Anta nå at påstanden er sann, dvs. at det finnes et tall b slik at $ab \equiv 1 \pmod{m}$. Dette betyr per definisjon at $m \mid (ab - 1)$, som igjen betyr at $ab - 1 = mk$, for et heltall k. Flytter over og får $1 = ab - mk$. La nå $d = \gcd(a, m)$. Siden d er en felles divisor har vi at $d \mid a$ og $d \mid m$. Ved Korollar 4.1.1 får vi at $d \mid (ab - mk)$, så $d \mid 1$. Dette er en selvmotsigelse for vi vet at $d \geq 2$, og de eneste tallene som deler 1, er -1 og 1. Dette viser at påstanden er usann, altså har ikke a noen invers modulo m. □

11 **a)** Vi vil løse kongruensen $19x \equiv 4 \pmod{141}$. Fra oppgave **4b)** vet vi at $19^{-1} \equiv 52 \pmod{141}$. Ganger vi med 52 på begge sider av kongruensen får vi

$$52 \cdot 19x \equiv 1 \cdot x \equiv x \equiv 52 \cdot 4 \equiv 208 \equiv 67 \pmod{141}.$$

Løsningen er $x \equiv 67 \pmod{141}$.