Oversikt over lineære kongruenser og lineære diofantiske ligninger

Richard Williamson

3. desember 2014

Oppgave 1

Finn et heltall x slik at

$$462x \equiv 27 \pmod{195}.$$

Hvordan løse oppgaven?

Benytt først Euklids algoritme for å finne heltall u og v slik at

$$462u + 195v = \mathsf{sfd}(462, 195).$$

Hvordan gjør jeg det?

Vi benytter Euklids algoritme som følger for a finne $\mathsf{sfd}(462, 195)$.

$$\begin{aligned} 462 &= 2 \cdot 195 + 72 \\ 195 &= 2 \cdot 72 + 51 \\ 72 &= 1 \cdot 51 + 21 \\ 51 &= 2 \cdot 21 + 9 \\ 21 &= 2 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 \end{aligned}$$

Hvordan kommer vi fram til disse ligningene?

Vi gjør følgende.

(1) Vi begynner med å dele 462 med 195. Vi får 2 som kvotient, og 72 som rest, altså får vi ligningen

$$462 = 2 \cdot 195 + 72.$$

(2) Da deler vi 195 med 72. Vi får 2 som kvotient og 51 som rest, altså får vi ligningen

$$195 = 2 \cdot 72 + 51.$$

(3) Da deler vi 72 med 51: vi får 1 som kvotient og 21 som rest, altså får vi ligningen

$$72 = 1 \cdot 51 + 21.$$

Slik fortsetter vi til får 0 som rest.

Teorien for Euklids algoritme i kurset fastslår at heltallet vi deler med når vi får 0 til rest, nemlig 3 i dette tilfellet, er den største felles divisoren til de to heltallene vi begynte med, nemlig 462 og 195 i dette tilfellet. Det vil si: vi har funnet at $\mathsf{sfd}(462, 195) = 3$.

Hva gjør jeg nå?

Vi jobber på følgende måte med ligningene vi fikk fra Euklids algoritme.

$$\begin{aligned}
72 &= 462 - 2 \cdot 195 \\
51 &= 195 - 2 \cdot 2 \\
&= 195 - 2 \cdot (462 - 2 \cdot 195) \\
&= (-2) \cdot 462 + 5 \cdot 195 \\
21 &= 72 - 1 \cdot 51 \\
&= (462 - 2 \cdot 195) - 1 \cdot ((-2) \cdot 462 + 5 \cdot 195) \\
&= 3 \cdot 462 + (-7) \cdot 195 \\
9 &= 51 - 2 \cdot 21 \\
&= ((-2) \cdot 462 + 5 \cdot 195) - 2 \cdot (3 \cdot 462 - 7 \cdot 195) \\
&= (-8) \cdot 462 + 19 \cdot 195 \\
3 &= 21 - 2 \cdot 9 \\
&= (3 \cdot 462 - 7 \cdot 195) - 2 \cdot ((-8) \cdot 462 + 19 \cdot 195) \\
&= 19 \cdot 462 + (-45) \cdot 195.
\end{aligned}$$

Hva er metoden her?

Vi gjør følgende.

(1) Trekk $2 \cdot 195$ fra begge sidene av den første ligningen

$$462 = 2 \cdot 195 + 72$$

som vi fikk da vi gjennomførte Euklids algoritme, for å få resten alene. Vi får ligningen

$$462 - 2 \cdot 195 = 72,$$

altså

$$72 = 462 - 2 \cdot 195.$$

(2) Trekk $2 \cdot 72$ fra begge sidene av den andre ligningen

$$195 = 2 \cdot 72 + 51$$

som vi fikk da vi gjennomførte Euklids algoritme, for å få resten alene. Vi får ligningen

$$195 - 2 \cdot 72 = 51,$$

altså

$$51 = 195 - 2 \cdot 72.$$

Så erstatter vi 72 med den høyre siden av ligningen vi fikk i (1), altså med

$$462 - 2 \cdot 195.$$

Vi får ligningen

$$51 = 195 - 2 \cdot (462 - 2 \cdot 195)\,.$$

Da manipulerer den høyre siden av denne ligningen for å få «noe ganger med 462» pluss «noe ganger med 195». Vi får:

$$51 = (-2) \cdot 462 + 5 \cdot 195.$$

(3) Trekk $1 \cdot 51$ fra begge sidene av den tredje ligningen

$$72 = 1 \cdot 51 + 21$$

som vi fikk da vi gjennomførte Euklids algoritme, for å få resten alene. Vi får ligningen

$$72 - 1 \cdot 51 = 21,$$

altså

$$21 = 72 - 1 \cdot 51.$$

Så erstatter vi 72 med den høyre siden av ligningen vi fikk i (1), altså med

$$462 - 2 \cdot 72,$$

og vi erstatter 51 med den høyre siden av ligningen vi fikk i (2), altså med

$$(-2) \cdot 462 + 5 \cdot 195.$$

Vi får ligningen

$$21 = (462 - 2 \cdot 72) - 1 \cdot ((-2) \cdot 462 + 5 \cdot 195)\,.$$

Da manipulerer den høyre siden av denne ligningen for å «noe ganger med 462» pluss «noe ganger med 195». Vi får:

$$21 = 3 \cdot 462 + (-7) \cdot 195.$$

Slik fortsetter vi.

(I) For hver ligning som vi fikk da vi gjennomførte Euklids algoritme, trekker vi det første leddet til høyre fra begge sidene for å få resten alene på én side av en ligning.

(II) Da benytter vi de to foregående ligningene som vi har kommet fram til for å få «noe ganger med 462» pluss «noe ganger med 195» på den andre siden av denne ligningen.

Til slutt får vi en ligning med $\mathsf{sfd}(462, 195)$, altså 3, på én side av en ligning, og «noe ganger med 462» pluss «noe ganger med 195» på den andre siden av denne ligningen. Vi får nemlig:

$$3 = 19 \cdot 462 + (-45) \cdot 195.$$

Så langt

Vi har funnet at

$$462 \cdot 19 + 195 \cdot (-45) = 3.$$

Hva gjør jeg nå?

Observer at det følger fra denne ligningen at

$$462 \cdot 19 \equiv 3 \pmod{195}.$$

Hvorfor følger det?

Vi kan argumentere på flere måter. Vi kan for eksempel manipulere ligningen

$$462 \cdot 19 + 195 \cdot (-45) = 3$$

for å få:

$$462 \cdot 19 - 3 = 45 \cdot 195.$$

Denne ligningen fastslår at

$$195 \mid 462 \cdot 19 - 3.$$

Ut ifra definisjonen av en kongruens, konkluderer vi da at

$$462 \cdot 19 \equiv 3 \pmod{195}.$$

Vi kan alternativt observere at

$$195 \cdot (-45) \equiv 0 \pmod{195},$$

siden $195 \mid 195 \cdot (-45)$. Derfor er

$$462 \cdot 19 = 462 \cdot 19 + 0 \equiv 462 \cdot 19 + 195 \cdot (-45) \pmod{195},$$

altså er

$$462 \cdot 19 \equiv 462 \cdot 19 + 195 \cdot (-45) \pmod{195}.$$

Det følger fra denne kongruensen og ligningen

$$462 \cdot 19 + 195 \cdot (-45) = 3$$

at

$$462 \cdot 19 \equiv 3 \pmod{195}.$$

Hva gjør jeg nå?

Sammenlign kongruensen

$$462 \cdot 19 \equiv 3 \pmod{195}$$

med kongruensen i oppgaven, altså med

$$462x \equiv 27 \pmod{195}.$$

Ved å gange begge sidene av kongruensen

$$462 \cdot 19 \equiv 3 \pmod{195}$$

med 9, får vi den riktige høyre siden. Vi får nemlig:

$$462 \cdot 19 \cdot 9 \equiv 3 \cdot 9 \pmod{195},$$

altså

$$462 \cdot 19 \cdot 9 \equiv 27 \pmod{195}.$$

Er det alltid mulig å gange med noe slik at vi får den riktige høyre siden?

Ja, så lenge kongruensen i oppgaven er løsbar. Se nedenfor for mer om dette. Når det står ≪Finn en løsning≫ i oppgaven, kan du regne med at kongruensen er løsbar, altså at det *er* mulig å gange med noe slik at vi får den riktige høyre siden.

Konklusjon

Vi har: $x = 19 \cdot 9$, altså $x = 171$, er en løsning til kongruensen

$$462x \equiv 27 \pmod{195}.$$

Oppsummering

Vi gjør følgende for å løse en kongruens

$$ax \equiv c \pmod{n}.$$

(1) Gjennomfør Euklids algoritme for å finne $\mathsf{sfd}(a, n)$. I dette tilfellet fikk vi $\mathsf{sfd}(462, 195) = 3$.

(2) Benytt ligningene vi får når vi gjennomfører Euklids algoritme får finne heltall u og v slik at

$$au + nv = \mathsf{sfd}(a, n).$$

I dette tilfellet fikk vi:

$$462 \cdot 19 + 195 \cdot (-45) = 3.$$

(3) Observer at det følger at

$$au \equiv \mathsf{sfd}(a, n) \pmod{n}.$$

I dette tilfellet fikk vi:

$$462 \cdot 19 \equiv 3 \pmod{195}.$$

(4) Gang begge sidene av kongruensen i (3) med et heltall for å få den samme høyre siden som i den opprinnelige oppgaven, altså c. La oss betegne dette heltallet som k_c. I dette tilfellet ganger vi begge sidene av kongruensen

$$462 \cdot 19 \equiv 3 \pmod{195}$$

med 9, altså $k_c = 9$. Vi får:

$$462 \cdot 19 \cdot 9 \equiv 27 \pmod{195}.$$

(5) Da har vi:

$$auk \equiv c \pmod{n}.$$

Dermed er $x = uk$ en løsningen til kongruensen

$$ax \equiv c \pmod{n}.$$

I dette tilfellet har vi: $x = 19 \cdot 9$, altså $x = 171$, er en løsning til kongruensen

$$462x \equiv 27 \pmod{195}.$$

Dersom $c = 1$, som for eksempel i krypotografi når en lineær kongruens må løses for å dekryptere en melding som har blitt kryptert av RSA-algoritmen, kan vi stoppe etter (3). Da konkluderer vi: $x = u$ er en løsning.

Oppgave 2

Finn alle heltallene x slik at

$$462x \equiv 27 \pmod{195}$$

og $0 \leq x < 195$.

Hvordan løse oppgaven?

Først finner vi én løsning. Det har vi gjort: $x = 171$ er en løsning. For å finne de andre løsningene, deler vi 195 med $\mathsf{sfd}(462, 195)$. Siden $\mathsf{sfd}(462, 195) = 3$ i dette tilfellet, får vi 65. Da er alle heltallene som er løsninger til kongruensen i oppgaven: $x = 171 + 65t$.

De eneste av disse løsningene som oppfyller kravet at $0 \leq x < 195$ er: $x = 41$, $x = 106$, og $x = 171$.

Vær forsiktig

Når man gjennomfører metoden vi benyttet for å løse Oppgave 1, kommer vi ikke nødvendigvis fram til en løsning som oppfyller kravet i oppgaven. Metoden vi har gått gjennom for å løse Oppgave 2 virker allikevel.

Oppsummering

Vi gjør følgende for å finne alle heltallene x slik at

$$ax \equiv c \pmod{n}$$

og $0 \leq x < n$.

(1) Først finner vi $\mathsf{sfd}(a, n)$ og én løsning $x = b$ til kongruensen. I dette tilfellet er $\mathsf{sfd}(462, 195) = 3$, og $x = 171$ er en løsning.

(2) Vi deler n med $\mathsf{sfd}(a, n)$. La oss betegne heltallet vi får som k_n. Da er alle heltallene som er er en løsning til kongruensen: $x = b + k_n t$, hvor t er et hvilket som helst heltall. I dette tilfellet er k_n likt 27 delt med 3, altså 9. Vi får: alle heltallene som er en løsning til kongruensen

$$462x \equiv 27 \pmod{195}$$

er $x = 171 + 9t$, hvor t er et hvilket som helst heltall.

(3) Vi finner de av disse løsningene som oppfyller kravet $0 \leq x < n$. Det finnes akkurat $\mathsf{sfd}(a, n)$ av disse. I dette tilfellet har vi: $x = 41$, $x = 106$, og $x = 171$.

Oppgave 3

Har kongruensen

$$42x \equiv 15 \pmod{54}$$

en løsning?

Hvordan løse oppgaven?

Vi må regne ut $\mathsf{sfd}(42, 54)$, og sjekke om den deler 15. Kongruensen har en løsning om det er sant at $\mathsf{sfd}(42, 54) \mid 15$, og har ikke en løsning om det ikke er sant at $\mathsf{sfd}(42, 54) \mid 15$.

Konklusjon

Vi har: $\mathsf{sfd}(42, 54) = 6$. Siden det ikke er sant at $6 \mid 15$, konkluderer vi at kongruensen i oppgaven har ingen løsning.

Er det nødvendig å benytte Euklids algoritme for å finne $\mathsf{sfd}(42, 54)$?

Nei. Euklids algoritme *er* nødvendig når vi ønsker å *finne* en løsning til en lineær kongruens

$$42x \equiv c \pmod{54},$$

fordi vi da trenger heltallene u og v slik at

$$42x + 54v = c,$$

og Euklids algoritime er den beste metoden for å komme fram til disse.

Når vi er kun interessert i om en lineær kongruens

$$42x \equiv c \pmod{54}$$

er løsbar, det vil si i om det finnes en løsning, kan vi imidlertid benytte en hvilken som helst metode for å finne $\mathsf{sfd}(42, 54)$, for eksempel den hvor vi finner en primtallsfaktorisering til 42 og en primtallsfaktorisering til 54.

Oppgave 4

Finn et heltall x slik at

$$7x \equiv 3 \pmod{11}.$$

Hvordan løse oppgaven?

Metoden vi benyttet for å løse Oppgave 1 virker alltid. Når vi jobber modulo et lite heltall, kan vi imidlertid kommer typisk fortere til en løsning ved å ganske enkelt gå gjennom heltallene 0, 1, 2, ..., 10 og sjekke om vi har en løsning.

Hvordan gjør jeg det?

Vi gjør følgende.

(1) Hvis vi erstatter x med 0, får vi 0 til venstre, som ikke er kongruent til 3 modulo 11.

(2) Hvis vi erstatter x med 1, får vi 7 til venstre, som ikke er kongruent til 3 modulo 11.

(3) Hvis vi erstatter x med 2, får vi 14 til venstre, som *er* kongruent til 3 modulo 11. Det vil si:

$$7 \cdot 2 \equiv 3 \pmod{11},$$

altså $x = 2$ er en løsning til kongruensen i oppgaven.

Når bør jeg benytte denne metoden?

Det kan alltid benyttes, men det blir slitsomme å gjennomføre denne metoden når vi jobber modulo et heltall som ikke er lite, og da er det best å gjennomføre metoden vi benyttet for å løse Oppgave 1.

Finnes det andre måter å løse lineære kongruenser?

Ja, det finnes i forelesningsnotatene flere triks som kan benyttes. Imidlertid er de to metodene vi har sett på her de viktigste, og jeg anbefaler at du fokuserer først og fremst på disse. Husk spesielt at metoden vi gjennomførte for å løse Oppgave 1 *alltid* kan benyttes: hvis du ikke kommer fort fram på en annen måte til en løsning, gjennomfør denne metoden.

Oppgave 5

Finn et heltall x og et heltall y slik at

$$462x + 195y = 27.$$

Hvordan løse oppgaven?

Akkurat som da vi løste Oppgave 1, finner vi heltall u og v slik at

$$462u + 195v = \mathsf{sfd}(462, 195).$$

Som i Oppgave 1, er $\mathsf{sfd}(462, 195) = 3$, $u = 19$, og $v = -45$. Dermed har vi:

$$462 \cdot 19 + 195 \cdot (-45) = 3.$$

Da deler vi 27 med $\mathsf{sfd}(462, 195)$, altså med 3, og vi ganger begge sidene av ligningen

$$462 \cdot 19 + 195 \cdot (-45) = 3$$

med resultatet. Vi har: 27 delt med 3 er 9. Når vi ganger begge sidene av ligningen

$$462 \cdot 19 + 195 \cdot (-45) = 3$$

med 9, får vi

$$462 \cdot 19 \cdot 9 + 195 \cdot (-45) \cdot 9 = 3 \cdot 9,$$

altså

$$462 \cdot 171 + 195 \cdot (-405) = 27.$$

Dermed er $x = 171$ og $y = -405$ en løsning til ligningen i oppgaven.

Oppsummering

Vi gjør følgende for å finne en heltallsløsning til en ligning

$$ax + by = c,$$

hvor a, b, og c er heltall.

(1) Gjennomfør Euklids algoritme for å finne $\mathsf{sfd}(a, n)$. I dette tilfellet fikk vi $\mathsf{sfd}(462, 195) = 3$.

(2) Benytt ligningene vi får når vi gjennomfører Euklids algoritme får finne heltall u og v slik at

$$au + nv = \mathsf{sfd}(a, n).$$

I dette tilfellet fikk vi:

$$462 \cdot 19 + 195 \cdot (-45) = 3.$$

(3) Gang begge sidene av ligningen i (2) med et heltall for å få den samme høyre siden som i den opprinnelige oppgaven, altså c. La oss betegne dette heltallet som k_c. I dette tilfellet ganger vi begge sidene av ligningen

$$462 \cdot 19 + 195 \cdot (-45) = 3.$$

med 9, altså $k_c = 9$. Vi får:

$$462 \cdot 19 \cdot 9 + 195 \cdot (-45) \cdot 9 = 27.$$

(5) Da har vi:

$$auk_c + bvk_c = c.$$

Dermed er $x = uk_c$ og $y = vk_c$ en heltallsløsning til ligningen

$$ax + by = c.$$

I dette tilfellet har vi: $x = 19 \cdot 9$ og $y = (-45) \cdot 9$, altså $x = 171$ og $y = -405$, en heltallsløsning til ligningen

$$462x + 195y = 27.$$

Har jeg det rett at lineære diofantiske ligninger kan løses på nesten den samme måten som lineære kongruenser?

Ja! Teorien for lineære diofantiske ligninger er i alt vesentlig den samme som teorien for lineære kongruenser.

Oppgave 6

Finn alle heltallene x og y slik at

$$462x + 195y = 27.$$

Hvordan løse oppgaven?

Først finner vi én løsning. Det har vi gjort: $x = 171$ og $y = -405$ er en løsning. For å finne de andre løsningene, gjør vi følgende.

(1) Del 462 med $\mathsf{sfd}(462, 195)$. Siden $\mathsf{sfd}(462, 195) = 3$ i dette tilfellet, får vi 154.

(2) Del 195 med $\mathsf{sfd}(462, 195)$. Siden $\mathsf{sfd}(462, 195) = 3$ i dette tilfellet, får vi 65.

Da er alle løsningene: $x = 171 + 65t$ og $y = 171 - 154t$, hvor t er et hvilket som helst heltall t.

Vær forsiktig

Meningen her er et t er det samme heltallet i uttrykket for x og uttrykket for y. For eksempel når $t = 1$, får vi at $x = 171 + 65$ og $y = 171 - 154$, altså $x = 236$ og $y = 17$, en løsning til ligningen i oppgaven,

Pass på tegnene! Det er nødvendig at vi har $+65t$ og $-154t$.

Hvorfor virker dette?

Vi har: $154 = \frac{462}{3}$ og $65 = \frac{195}{3}$. Ved å erstatte x med $171 + 65t$ og y med $171 - 154t$ i ligningen i oppgaven, får vi:

$$\begin{aligned}
&462 \cdot (171 + 65t) + 195 \cdot (-405 - 154t) \\
&= 462 \cdot 171 + 195 \cdot (-405) + (462 \cdot 65 - 195 * 154)\, t \\
&= 462 \cdot 171 + 195 \cdot (-405) + \left(\frac{462 \cdot 195}{3} - \frac{195 \cdot 462}{3} \right) t \\
&= 462 \cdot 171 + 195 \cdot (-405) + 0t \\
&= 462 \cdot 171 + 195 \cdot (-405) \\
&= 27.
\end{aligned}$$

Dette viser at $x = 171 + 65t$ og $y = -405 - 154t$ er en løsning til ligningen i oppgaven for hvert heltall t. At disse er de eneste løsningene kan også vises, men vi skal ikke gå gjennom dette her.