Oppgaver, tallteori

Oppgave 1.

a) Bruk Euklids algoritme til å vise at tallene 155 og 224 er innbyrdes primiske.

b) Finn hele tall x og y slik at

$$1 = 155x + 224y$$

c) Finn en løsning av den lineære kongruensen $155x \equiv 2 \pmod{224}$, slik at $0 \leq x < 224$.

Oppgave 2.

a) Bruk Euklids algoritme til å vise at største felles faktor for 93 og 273 er 3.

b) Finn hele tall x og y slik at

$$3 = 93x + 273y$$

c) Løs den lineære kongruensen $93x \equiv 6 \pmod{273}$, hvor $0 \leq x < 273$.

Oppgave 3.

a) Bruk Euklids algoritme til å vise at største felles faktor for 238 og 161 er 7.

b) Finn hele tall x og y slik at

$$7 = 161x + 238y$$

c) Forklar hvorfor den lineære kongruensen $161x \equiv 3 \pmod{238}$ ikke har noen løsning. Forklar også hvorfor $161x \equiv 14 \pmod{238}$ har løsning. Finn alle løsningene x slik at $0 \leq x < 238$.

Oppgave 4.

a) Bruk Euklids algoritme til å vise at største felles faktor for 1803 og 357 er 3.

b) Finn hele tall x og y slik at

$$3 = 1803x + 357y$$

c) Finn et tall n mellom 0 og 1803 slik at $357n \equiv 3 \pmod{1803}$.

Oppgave 5.

a) Bruk Euklids algoritme til å finne største felles faktor $F = \gcd(61, 247)$ for 61 og 247.

b) Finn hele tall a og b slik at

$$F = a \cdot 61 + b \cdot 247$$

c) Finn et helt tall x mellom 0 og 247 slik at

$$61x \equiv 4 \pmod{247}$$

Oppgave 6.

a) Bruk Euklids algoritme til å vise at 142 og 95 er innbyrdes primiske.

b) Finn hele tall x og y slik at

$$1 = 95x + 142y$$

c) Løs den lineære kongruensen $95x \equiv 3 \pmod{142}$.

Oppgave 7.

a) Bruk Euklids algoritme til å vise at 100 og 121 er innbyrdes primiske.

b) Finn hele tall x og y slik at

$$1 = 100x + 121y$$

c) Beregn $\phi(121)$ og bruk dette og Eulers generalisering av Fermats lille teorem til å vise at 121 deler $100^{110} - 1$.

Oppgave 8.

a) Forklar hvorfor $\phi(4331) = 4200$ ved å bruke at $4331 = 61 \cdot 71$ (61 og 71 er primtall).

b) Bruk Eulers generalisering av Fermats lille sats til å forklare hvorfor

$$2^{4200} - 1$$

er delelig med 61 og 71.

Oppgave 9.

a) Forklar hvorfor $\phi(1952) = 960$ ved å bruke at $1952 = 61 \cdot 32$ (61 er et primtall og $32 = 2^5$).

b) Bruk Eulers generalisering av Fermats lille sats til å forklare hvorfor

$$5^{960} - 1$$

er delelig med 61.

Oppgave 10. Forklar hvorfor tverrsummen til et tall som er delelig med 3 også er delelig med 3.

Oppgave 11.

a) Formuler Diofants teorem.

b) Det finnes fire primitive pytagoreiske tripler med katet 180. Bruk Diofants teorem til å finne alle fire. (Hint: 90 kan skrives som et produkt av to innbyrdes primiske tall på fire forskjellige måter.)

Oppgave 12. Bruk Diofants teorem til å finne et primitivt pythagoreisk trippel der den ene kateten er 40. (to mulige svar)

Oppgave 13. Bruk Diofants teorem til å finne et primitivt pythagoreisk trippel der den ene kateten er 88.

Oppgave 14.

a) Forklar hva vi mener med et primitivt pythagoreisk trippel og gi et eksempel på et slikt trippel.

b) Bruk Diofants teorem til å finne et primitivt pythagoreisk trippel der den ene kateten er 33.

Oppgave 15. Diofants teorem sier at alle primitive pytagoreiske tripler er på formen

$$(p^2 - q^2, 2pq, p^2 + q^2)$$

for hele tall p og q. Forklar hvorfor vi ikke får et primitivt pytagoreisk trippel når både p og q er oddetall.

Oppgave 16.

a) Løs den lineære kongruensen $5x \equiv 1 \pmod{72}$

b) I en tenkt RSA-katalog står et firma oppført med tallene $(91, 5)$. Vi skal sende meldingen 15 til dette firmaet og bruke tallene i RSA-katalogen til å kryptere meldingen. Svaret skal bli 71. Vis hvordan vi kommer fram til dette tallet

c) Ved å faktorisere 91 og bruke Eulers ϕ-funksjon har vi nok informasjon til å dekryptere meldingen. Bruk svaret i a) og vis hvordan firmaet kan regne seg fram til den opprinnelige (ukrypterte) meldingen.

Oppgave 17. En strekkode består av 10 sifre, hvorav det siste sifret er et kontrollsiffer. Dette sifferet er beregnet ved å ta 9 minus tverrsummen av de 9 første sifrene, slik at vi får et tall mellom 0 og 9.

a) Tallet $152396401m$ hvor m er et helt tall mellom 0 og 9 er en korrekt strekkode. Finn m.

b) Forklar hvorfor et tall med 10 siffer er en korrekt strekkode i dette kodesystemet dersom tallet er delelig med 9.

Oppgave 18. Et kodesystem består av 4-sifrede koder, der de tre første sifrene er meldingen og det siste sifferet er et kontrollsiffer. Kontrollsifferet framkommer ved å multiplisere første siffer med 5, andre siffer med 2, tredje siffer med 3, legge sammen de tre tallene man da får og ta resten av det modulo 10.

a) En mottaker mottar meldingen 539-3. Er dette en korrekt melding? Forklar.

b) En annen melding er gitt ved 247-1. Hvis vi antar at kontrollsifferet i denne koden er rett og kun ett av de tre første sifrene er feil, hvilket er da feil og hva skulle det ha vært?

Oppgave 19. Et kodesystem består av 4-sifrede koder, der de tre første sifrene er meldingen og det siste sifferet er et kontrollsiffer. Kontrollsifferet framkommer ved å multiplisere første siffer med 1, andre siffer med 2, tredje siffer med 4, legge sammen de tre tallene man da får og ta resten av det modulo 10.

a) En mottaker mottar meldingen 3141. Er dette en korrekt melding? Forklar.

b) En annen melding er gitt ved 5226. Hvis vi antar at kontrollsifferet i denne koden er rett og kun ett av de tre første sifrene er feil, hvlket er da feil og hva skulle det ha vært?