MA-EVU1 - Mer Matematikk, nettbasert videreutdanningskurs i tallteori

Oppgaver pr. 10. desember 2002

Her er noen flere oppgaver.

Oppgave 1.

I denne oppgaven skal vi øve på å bruke Euklids algoritme. I hvert punkt skal du finne største felles faktor (gcd) for de to tallene og også gcd uttrykt som en lineærkombinasjon av de to tallene. Eksempel: Dersom de to tallene er 27 og 42 så vil gcd være 3 og 3 kan skrives som 3 = 2 x 42 - 3 x 27.

a) 91 og 156

b) 356 og 8 911

c) 22 471 og 3 266

d) 49 349 og 15 555

e) 2^n og 2^m

Oppgave 2.

Vi har $gcd(30, 21) = 3$. Finn alle hele tall x og y som er slik at $3 = 30x + 21y$.

Oppgave 3.

Løs de lineære kongruensene.

a) $4x \equiv 1 \pmod 7$

b) $17x \equiv 1 \pmod{32}$

c) $4x \equiv 4 \pmod{39}$

d) $3266x \equiv 23 \pmod{22471}$

Oppgave 4.

a) (Eksamen januar 2002) Forklar hvorfor et tall N er delelig med 9 hvis og bare hvis tverrsummen av tallet er delelig med 9.

b) I dette punktet jobber vi i 8-tallssystemet. Forklar hvorfor et tall N er delelig med 7 hvis og bare hvis tverrsummen av tallet er delelig med 7.

c) Prøv å gi et argument for at dersom vi jobber i N-tallsystemet for et naturlig tall N, så er et tall delelig med $N-1$ hvis og bare hvis tverrsummen til tallet er delelig med $N-1$.

Oppgave 5.

I denne oppgaven følger vi samme oppskrift som i eksemplet med dyrenavn i bolk 2, leksjon 2, men nå tar vi med oss hele alfabetet bortsett fra Å, nummerert fra 1 til 28, slik at A er 1 og Ø er 28. All regning foregår modulo 29.

a) Prøv å gi en forklaring på hvorfor det er mye mer effektivt å droppe en bokstav og å gjøre regningene modulo 29 enn å ta med alle bokstavene og regne modulo 30.

b) Fire mottakere, vi kan kalle dem Putin, Bush, Bondevik og Hu har hver sin kodenøkkel. Putin har 7, Bush har 12, Bondevik har 24 og Hu har 3. Følgende melding blir sendt (i kryptert form) ut over hele verden fra et sted i Midt-Østen:

OIVM SWI

Hvem er meldingen myntet på og hva sier den?

Oppgave 6.

Kan noen av neste års nyttårsbarn få personnummeret 010103-25337 ? Hvis nei, hva burde de to siste sifrene ha vært?

Oppgave 7.

a) Anta at a og N ikke har felles faktorer. Vis at dersom to tall to tall x_1 og x_2 oppfyller likningen $aX \equiv b$ (modulo N), så må $x_1 \equiv x_2$ (modulo N).

b) Antakelsen i a) om at a og N ikke har felles faktorer er helt essensiell for at konklusjonen skal være sann. Finn et eksempel som viser at konklusjonen ikke er sann dersom denne antakelsen ikke er riktig.