Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Førsteamanuensis Jon Eivind Vatne (90 20 31 17)

Eksamen i MA1301-Tallteori

Onsdag 30. november 2005
Tid: 09.00 – 13.00

Ingen hjelpemidler tillatt.
Oppgavesettet er på to sider.
Du skal grunngi alle svar.

Oppgave 1

a) Regn ut $\gcd(788, 116)$. Finn alle løsningene i hele tall til likningen

$$788x + 116y = \gcd(788, 116).$$

b) En antikvar selger en dag noen bøker for 116 kroner stykket, og kjøper noen bøker for 788 kroner stykket. Når dagen er over har hun 24 kroner mer enn hun hadde om morgenen. Hva er det minste antall bøker hun kan ha solgt denne dagen? Og hva er det minste antallet bøker hun kan ha kjøpt?

Oppgave 2

a) Finn alle løsningene til de samtidige kongruensene

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\ 5) \\ x &\equiv 2 \,(\mathrm{mod}\ 6) \\ x &\equiv 6 \,(\mathrm{mod}\ 7). \end{aligned}$$

b) Forklar hvorfor likningssystemet

$$3x + 7y \equiv 2 \,(\text{mod } 8)$$
$$4x + 5y \equiv 7 \,(\text{mod } 8)$$

har en og bare en løsning modulo 8. Løs systemet.

Oppgave 3

a) Du skal sette opp et RSA-system for å motta hemmelige meldinger. Den hemmelige nøkkelen velger du til å være $\{n, d\} = \{91, 29\}$. Hva blir den offentlige nøkkelen $\{n, e\}$?

b) Den første hemmelige meldingen du får er 9. Dekrypter denne meldingen.

Oppgave 4

a) Formuler Eulers teorem (du trenger ikke vise det).

b) La a være et heltall med $\gcd(a, 5) = 1$. Vis at

$$a^{61} \equiv a \,(\text{mod } 8525).$$

Hint: $8525 = 5^2.11.31$.

c) La $n \geq 2$ og a være hele tall. Når er ordenen til a modulo n definert? Hva er definisjonen? Hva er ordenen til 8 modulo 19?

Oppgave 5 Wilsons teorem sier at $(p-1)! \equiv -1 \,(\text{mod } p)$ for alle primtall p. Vis Wilsons teorem.

Oppgave 6 La (x, y, z) være et primitivt pytagoreisk trippel (altså er $x^2 + y^2 = z^2$ og $\gcd(x, y, z) = 1$). Vis at akkurat ett av tallene x, y, z kan deles på 5. Finn et eksempel der $5|x$, og et eksempel der $5|z$.

Trygve Johnsen Jon Eivind Vatne