Noregs teknisk–naturvitskaplege universitet
Institutt for matematiske fag

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

Eksamen i MA1301-Talteori

Onsdag 30. november 2005
Tid: 09.00 – 13.00

Ingen hjelpemiddel tillatne.
Oppgåvesettet er på to sider.
Du skal grunngi alle svar.

Oppgåve 1

a) Rekn ut $\gcd(788, 116)$. Finn alle løysingane i heile tal til likninga

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

b) Ein antikvar sel ein dag nokre bøker for 116 kroner stykket, og kjøper nokre bøker for 788 kroner stykket. Når dagen er over har ho 24 kroner meir enn ho hadde om morgonen. Kva er det minste antallet bøker ho kan ha selt denne dagen? Og kva er det minste antallet bøker ho kan ha kjøpt?

Oppgåve 2

a) Finn alle løysingane til dei samtidige kongruensane

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 6 \pmod 7. \end{aligned}$$

b) Forklar kvifor likningssystemet

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

har ei og berre ei løysing modulo 8. Løys systemet.

Oppgåve 3

a) Du skal setje opp eit RSA-system for å motta hemmelege meldingar. Den hemmelege nøkkelen vel du til å vere $\{n, d\} = \{91, 29\}$. Kva vert den offentlege nøkkelen $\{n, e\}$?

b) Den første hemmelege meldinga du får er 9. Dekrypter denne meldinga.

Oppgåve 4

a) Formuler Eulers teorem (du treng ikkje vise det).

b) La a vere eit heiltal 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 vere heile tal. Når er ordenen til a modulo n definert? Kva er definisjonen? Kva er ordenen til 8 modulo 19?

Oppgåve 5 Wilsons teorem seier at $(p-1)! \equiv -1 \,(\text{mod } p)$ for alle primtal p. Vis Wilsons teorem.

Oppgåve 6 La (x, y, z) vere eit primitivt pytagoreisk trippel (altså er $x^2 + y^2 = z^2$ og $\gcd(x, y, z) = 1$). Vis at akkurat eitt av tala x, y, z kan delast på 5. Finn eit døme der $5|x$, og eit døme der $5|z$.

Trygve Johnsen Jon Eivind Vatne