Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen: Petter Andreas Bergh
Telefon: 7359 0483

Eksamen i fag MA1301 Tallteori

Bokmål
Fredag 5. desember 2003
Kl. 09.00-13.00

Hjelpemidler: ingen hjelpemidler tillatt

Sensur faller 05.01.2004.

Oppgave 1

a) Benytt Euklids algoritme til å finne største felles divisor av tallene 675 og 285.

b) Forklar hvorfor den diofantiske ligningen

$$675x + 285y = 30$$

er løsbar, og finn alle løsningene.

Oppgave 2 Finn alle heltall $x \in \mathbb{Z}$ som gir rest 1, 2 og 3 ved divisjon med henholdsvis 5, 7 og 8. Hva er det minste positive slike tallet?

Oppgave 3

a) Formuler Eulers Teorem (uten bevis).

b) Finn det siste sifferet i tallet 63^{81}.

c) Fermats Teorem sier at dersom a er et heltall og p er et primtall som ikke deler a, så gjelder $a^{p-1} \equiv 1 (\bmod p)$. Vis dette ved hjelp av Eulers Teorem.

Oppgave 4

a) Avgjør om den lineære kongruensen $7x \equiv 1 (\bmod 40)$ er løsbar, og finn eventuelt alle løsningene.

b) I et RSA-krypteringssystem er den offentlige krypteringsnøkkelen gitt ved $\{n, e\} = \{55, 7\}$, hvor $55 = 5 \cdot 11$. Finn den hemmelige dekrypteringsnøkkelen $\{n, d\}$.

c) Krypter meldingen $M = 13$.

Oppgave 5 La p og q være tvillingprimtall. Vis at da gjelder enten $p! \equiv 1 (\bmod q)$ eller $q! \equiv 1 (\bmod p)$.