Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

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

Eksamen i fag MA1301 Tallteori

Bokmål
Torsdag 2. desember 2004
Kl. 09.00-13.00

Hjelpemidler: ingen hjelpemidler tillatt

Sensur faller 23.12.2004.

Alle svar skal begrunnes.

Oppgave 1 Det matematiske instituttet ved Universitetet i Nidaros har 118 ansatte fordelt på administrasjonen, professorer og stipendiater. Samtlige ansatte kom på instituttets julefest, som kostet 70 kroner for professorer og 30 kroner for stipendiater. Medlemmene av administrasjonen, som arrangerte festen, kom inn gratis. Til sammen ble det betalt inn 5060 kroner i inngangspenger. Instituttet har minst 10 flere stipendiater enn professorer, og minst 10 medlemmer i administrasjonen. Hvor mange professorer har instituttet? Hvor mange stipendiater? Hvor mange medlemmer har administrasjonen?

Oppgave 2 Finn de to siste sifrene i tallet

$$\sum_{n=1}^{10} 3^{40n+1} = 3^{40+1} + 3^{40\cdot 2+1} + \cdots + 3^{40\cdot 10+1}.$$

Oppgave 3 Finn alle løsningene av systemet

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 1 \pmod 6 \\ x &\equiv 1 \pmod 7. \end{aligned}$$

Oppgave 4 Formuler Wilsons Teorem (uten bevis). Hva får vi til rest når vi deler

$$35! - 35$$

på 37?

Oppgave 5

a) I et RSA-krypteringssystem er den offentlige krypteringsnøkkelen gitt ved

$$\{n, e\} = \{85, 15\},$$

hvor $85 = 5 \cdot 17$. Finn den hemmelige dekrypteringsnøkkelen.

b) Krypter meldingen $M = 7$.

Oppgave 6 La $a \in \mathbb{Z}$ og $n \in \mathbb{N}$ være to relativt primiske tall. Et tall $b \in \mathbb{Z}$ sies å være *en invers av a modulo n* dersom $ab \equiv 1 (\bmod n)$. Finn den minste positive inversen av 31 modulo 131.

Oppgave 7

a) La $a \in \mathbb{Z}$ og $n \in \mathbb{N}$ være to relativt primiske tall, og la k være ordenen til a modulo n. Vis at for en $t \geq 1$ gjelder da

$$a^t \equiv 1 (\bmod n) \Leftrightarrow k \mid t.$$

b) Avgjør om 7 er en primitiv rot av 11. Hvor mange primitive røtter har 37?

Oppgave 8 For hver $k \in \mathbb{N}$, la S_k betegne summen

$$\sum_{i=1}^{k} \frac{1}{i} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}.$$

Vis at

$$S_{2^n} \geq \frac{n}{2} + 1$$

for alle $n \geq 1$.