



Norges teknisk–naturvitenskapelige
universitet
Institutt for matematiske fag

MA2201/TMA4150

Vår 2013

Øving 11

Oppgavene merket med * er litt mer utfordrende.

Fra boka:

Seksjon 19: 5, 8, 23 og 26*

Seksjon 20: 1, 4, 6, 8, 9, 10, 11, 13, 24, 27*, 28*

Ekstraoppgave

RSA 101 og 113 er primtall, og $7467 \cdot 3 \equiv 1 \pmod{11200}$.

La $(11413, 7467)$ være ditt RSA-nøkkelpar, og anta at $\text{space}=100$, $a=101$, $b=102$, etc.

Du mottar en melding som består av tallene 4654, 676 og 2931. Dekrypter meldingen!

Eksamensoppgave

mai 2004: 4 a) Finn alle abelske grupper av orden 8 opp til isomorfi.

b) La G være gruppen av enheter i den kommutative ringen $\mathbb{Z}_{10} \times \mathbb{Z}_3$. Finn alle elementene i G , og avgjør hvilken av gruppene i a som G er isomorf med.