Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA2201/TMA4150 Vår 2013

Løsningsforslag — Øving 11

Seksjon 19

26 I hele denne oppgaven antar vi at $a \in R \setminus \{0\}$, og at $b \in R$ er det unike elementet slik at $aba = a$.

a) La $c \in R$. Dersom $ac = 0$, så har vi at

$$a(b+c)a = aba + aca = aba = a.$$

Det følger da av unikheten til b at $b + c = b$, og dermed er $c = 0$. Dermed har R ingen nulldivisorer.

b) Fra at $aba = a \neq 0$ vet vi at $b \neq 0$. Om vi ganger med b på venstre side får vi $baba = ba$, og siden vi ikke har nulldivisorer i R, vet vi fra Teorem 19.5 at vi kan forkorte med a på høyre side: $bab = b$.

c) La $c \in R$. Siden $ca = caba$, har vi $c = cab$. Siden $babc = bc$, har vi også at $abc = c$. Dermed er ab multiplikativ identitet i R.

d) Vi vet at $ab = 1_R$, og med et bevis symmetrisk til det i c kan vi også vise at $ba = 1_R$. Dermed har vi at $b = a^{-1}$.

Seksjon 20

27 Hvis a er sin egen invers, har vi $a^2 = 1$, og dermed

$$0 = a^2 - 1 = (a-1)(a+1).$$

Siden $\mathbb{Z}_p$ er en kropp har vi ingen nulldivisorer; dermed må vi ha $a = 1$ eller $a = -1 = p - 1$.

28 Vi vet at:

$$(p-1)! = (p-1)(p-2)\cdots(2)(1).$$

For $p = 2$ har vi $(p-1)! = 1! = p - 1$.

For $p \geq 3$ vet vi at for hver faktor i $(p-1)!$ er også inversen en faktor ($\mathbb{Z}_p$ er en kropp, og alle dens elementer unntatt null er faktorer i $(p-1)!$). For alle faktorer unntatt $p-1$ og 1 er inversen en annen faktor; vi kan dermed gjøre om uttrykket for $(p-1)!$ til

$$(p-1)! = (p-1)(1)\cdots(1)(1) = p - 1$$

Annet

RSA Meldingen er "hei".

mai 2004: 4 **a)** De abelske gruppene av orden åtte er, opp til isomorfi, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ og $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

b) Vi observerer at $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_3$ er en enhet hvis og bare hvis a er en enhet i $\mathbb{Z}_{10}$ og b er en enhet i $\mathbb{Z}_3$.

Enhetene i $\mathbb{Z}_{10}$ er 1, 3, 7 og 9.

Enhetene i $\mathbb{Z}_3$ er 1 og 2.

Dermed får vi $G = \{(1,1), (1,3), (1,7), (1,9), (2,1), (2,3), (2,7), (2,9)\}$.

G har kun 4 idempotente elementer, så $G \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. G har ikke noe generende element, så $G \ncong \mathbb{Z}_8$. Dermed har vi $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Eventuelt kan vi observere at gruppen $\mathbb{Z}_3^*$ av enheter i $\mathbb{Z}_3$ er isomorf med $\mathbb{Z}_2$, og gruppen $\mathbb{Z}_{10}^*$ av enheter i $\mathbb{Z}_{10}$ er isomorf med $\mathbb{Z}_4$. Da har vi

$$G \cong \mathbb{Z}_3^* \times \mathbb{Z}_{10}^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$