Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA2201/TMA4150 Vår 2018

Løsningsforslag — Øving 9

Med forbehold om feil. Gi gjerne beskjed til mads.sandoy alfakrøll ntnu.no hvis en finner noen.

Seksjon 20

2 Her er nok det enkleste å prøve seg fram med ulike elementer i mengden av enheter i $\mathbb{Z}_{11}$. Generatorene er 2, 6, 7 og 8.

8

$$\begin{aligned}\phi(p^2) =& |\{n \in \mathbb{Z}^+ | n \leq p^2 \wedge \gcd(n,p) = 1\}| \\ =& |\{n \in \mathbb{Z}^+ | n \leq p^2\} \setminus \{n \in \mathbb{Z}^+ | n \leq p^2 \wedge \gcd(n,p) \neq 1\}| \\ =& |\{n \in \mathbb{Z}^+ | n \leq p^2\}| - |\{n \in \mathbb{Z}^+ | n \leq p^2 \wedge \gcd(n,p) \neq 1\}| \\ =& p^2 - |\{p, 2p, \dots p^2\}| \\ =& p^2 - p\end{aligned}$$

Sagt med ord: $\phi(p^2$ er antall positive heltall mindre enn eller lik p^2 som er relativt primiske til p^2. Det er p^2 positive heltall mindre enn eller lik p^2, og p av disse (nemlig $p, 2p, \dots p^2$ er ikke relativt primiske til p^2. Dermed har vi at $\phi(p^2) = p^2 - p$.

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

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

Seksjon 22

17 Vi ser etter røtter til polynomet $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$. Vi ser umiddelbart at $x = 0$ er en rot, så anta i det følgende at $x \neq 0$. Da er x relativt primisk til 5, så dermed har vi fra Fermats lille teorem at $x^4 \equiv 1 \mod 5$. Vi skriver derfor om polynomet:

$$2x^{219} + 3x^{74} + 2x^{57} + 3x^{44} = 2(x^4)^{54}x^3 + 3(x^4)^{18}x^2 + 2(x^4)^{14} + 3(x^4)^{11}$$

Det er nå relativt mye enklere å sette inn de restrerende verdiene (x^4-faktorene blir jo alle lik 1), og vi står igjen med at 0, 1, 2 og 3 er røtter i polynomet.

24 La $f(x) = a_n x^n + \cdots + a_1 x + a_0$ og $g(x) = b_m x^m + \cdots + b_1 x + b_0$ være to polynomer i $D[x]$, og anta $a_n \neq 0 \neq b_m$. Da har vi at

$$f(x)g(x) = a_n b_m x^{n+m} + (a_{n-1}b_m + a_n b_{m-1})x^{n+m-1} + \cdots + a_0 b_0$$

Siden D er et integritetsområde, er $a_n b_m \neq 0$; dermed er $f(x)g(x) \neq 0$, og $D[x]$ er et integritetsområde.

25 **a)** Som vi så i forrige oppgave er et produkt av ett polynom av grad m og ett av grad n et polynom av grad $m + n$. Dette kan være lik 1 hvis og bare hvis $m = n = 0$. På den andre siden, dersom $p(x) = a \neq 0$, så vet vi at a har en invers b, og $q(x) = b$ blir da inversen til $p(x)$. Derfor er enhetene i $D[X]$ nettopp alle polynomer av grad 0 som ikke er lik 0.

b) 1 og -1

c) 1, 2, 3, 4, 5 og 6

Seksjon 23

7 Fra Korollar 6.16 vet vi at hvis vi har funnet én generator, kan vi også regne ut resten av generatorene. Merk at $|\mathbb{Z}_{17}^*| = 16$, slik at alle elementer vil ha en orden som er en potens av 2.

Vi starter med å finne en generator. $2^8 \equiv 1 \mod 17$, så 2 er ikke en generator av gruppa. Derimot har vi at $3^8 \equiv 16 \mod 17$, slik at 3 er en generator av gruppa.

Gitt en generator a, er alle andre generatorer gitt som a^r, der r er relativt prim til ordenen til gruppa. I dette tilfellet vil det si at r er et oddetall. Dermed er generatorene (jeg sløyfer fra nå av modulo-notasjon) $3^1 = 3$, $3^3 = 10$, $3^5 = 5$, $3^7 = 11$, $3^9 = 14$, $3^{11} = 7$, $3^{13} = 12$ og $3^{15} = 6$.

9 Fra korrolar 23.3 vet vi at $(x - a)$ er en lineær faktor av $x^4 + 4$ hvis og bare hvis a er en rot av polynomet, det vil si $a^4 + 4 = 0$. Vi merker oss at 1, 2, 3 og 4 alle er røtter av polynomet. Dermed er $x^4 + 4 = (x - 1)(x - 2)(x - 3)(x - 4)$.

35 Vi har $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$. Siden a er en rot av $f(x)$ har vi at

$$f(a) = a_0 + a_1a + \ldots + a_{n-1}a^{n-1} + a_na^n = 0$$

Siden F er en kropp og $a \neq 0$ har a en invers $\frac{1}{a}$. Vi ganger likningen over med $\left(\frac{1}{a}\right)^n$ og får at

$$a_0\left(\frac{1}{a}\right)^n + a_1a\left(\frac{1}{a}\right)^n + \ldots + a_{n-1}a^{n-1}\left(\frac{1}{a}\right)^n + a_na^n\left(\frac{1}{a}\right)^n = 0.$$

Vi forkorter og får

$$a_0\left(\frac{1}{a}\right)^n + a_1\left(\frac{1}{a}\right)^{n-1} + \ldots + a_{n-1}\left(\frac{1}{a}\right) + a_n = 0.$$

Dermed har vi at $\left(\frac{1}{a}\right)^n$ er en rot av $a_n + a_{n-1}x + \ldots + a_1x^{n-1} + a_0x^n$.

Eksamensoppgaver

H2006 - 7 Vi har p et primtall og $0 \leq a < p$ et heltall. Videre lar vi $q(x) \in \mathbb{Z}_p(x)$ være gitt ved $q(x) = x^p - a$. Fermats lille teorem forteller oss at $a^p \equiv a \mod p$. Dermed er a en rot av q, og siden Z_p er en kropp må da $(x - a)$ være en (lineær) faktor av $q(x)$.

K2007 - 6 Vi vet at et produkt av to polynomer, henholdsvis av grad m og n, over en kropp[1] er et polynom av grad $m + n$. Ut ifra det ser vi at enhetene i $\mathbb{Z}_5[x]$ er alle konstante polynomer unntatt 0.

Videre ser vi at $\mathbb{Z}_5[x]$ er et integritetsområde (ingen nulldivisorer), men ikke en kropp (alle polynomer av grad større en null mangler inverser).

V2013 - 3 **a)** Her er det nok å sjekke definisjonen: R er lukket under addisjon og multiplikasjon, og multiplikasjon er kommutativt.

b)
- For å vise ϕ er en ringhomomorfi, må vi vise at ϕ respekterer addisjon og multiplikasjon. Dette er ganske rett frem ved innsetting.
- $\ker\phi = \left\{ \begin{bmatrix} 0 & y & z \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} | x, y, \in \mathbb{Z}_3 \right\}$
- $R/\ker\phi \cong \phi[R] = \mathbb{Z}_3$, i følge fundamentalteoremet for homomorfier (26.17). $\mathbb{Z}_3$ er som kjent en kropp med tre elementer.

[1] Strengt tatt er det nok med et integritetsområde