



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

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

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 $x^4 \equiv 1 \pmod{5}$. 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 restrende 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 $f(x) = a_nx^n + \dots + a_1x + a_0$ og $g(x) = b_mx^m + \dots + b_1x + b_0$ være to polynomer i $D[x]$, og anta $a_n \neq 0 \neq b_m$. Da har vi at

$$f(x)g(x) = a_nb_mx^{n+m} + (a_{n-1}b_m + a_nb_{m-1})x^{n+m-1} + \dots + a_0b_0$$

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

- 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

Eksamensoppgaver

- H2011-2 a) I denne oppgaven skal vi vise at enhetene (elementene med multiplikativ invers) i en ring R med enhet (multiplikativ identitet) danner en abelsk gruppe under multiplikasjon. Vi sjekker derfor gruppeaksiomene:

Mengde med binæroperasjon: Før vi kan bruke aksiomene må vi sjekke det nulte aksiomet: At enhetene i R er en mengde, og at multiplikasjonen fra R er en binæroperasjon. Det første følger av at elementene i R utgjør er en mengde. Det andre er oppfylt dersom mengden av enheter i R er lukket under multiplikasjon; la derfor a og b være enheter, med a' og b' som deres respektive inverser. Vi har da at $(ab)(b'a') = 1$, så ab er igjen en enhet i R .

\mathcal{G}_1 Multiplikasjonen er assosiativ i R (fordi R er en ring), så da er den det her også.

\mathcal{G}_2 Det multiplikative identitetselementet er en enhet, og fungerer som identitetselement også i gruppa.

\mathcal{G}_3 Inversen av en enhet er igjen en enhet.

- b) \mathbb{Z}_n er en kommutativ ring. Enhetene i \mathbb{Z}_n er elementene som er relativt primiske til n , og som vi har sett i (a) danner disse en abelsk gruppe U . Per definisjon er $|U| = \phi(n)$. Dermed har vi at for $u \in U$, så er $u^{\phi(n)} = u^{|U|} = 1$, identiteten i U - dette følger for eksempel fra Lagranges teorem. Altså har vi at for a relativt primisk til n så er $a^{\phi(n)} \equiv 1 \pmod{n}$.

H2006-1 a) Det finnes to abelske grupper av orden 12 opp til isomorfi: $\mathbb{Z}_4 \times \mathbb{Z}_3$ og $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

- b) Det finnes 12 enheter i \mathbb{Z}_{21} , nemlig $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Ingen av disse har orden 4. Dermed må gruppen være isomorf til $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.