E4 opgavesæt 4

Jogvan M. Poulsen

11. december 2000

Opgave 16.10.2

Vi skal vise, at polynomiet $f(s) = x^4 + x^3 + x^2 + x + 1$ er irreducibelt i $\mathbf{Z}_2[x]$, men ikke primitivt.

Det ses umiddelbart at der ikke er nogle linæere faktorer, da for $x = 0$ gælder at $f(x) = 1$, som også betyder at der ikke er nogle kubiske faktorer. Hvis der heller ikke er nogle kvadratiske fakrorer der kan faktorisere polynimiet, må der være irreducibelt. Det vil sige, at vi kan opskrive $f(x)$ på følgende måde.

$$\begin{aligned}(x^4 + x^3 + x^2 + x + 1) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd\end{aligned}$$

Da koefficienterne kommer fra $\mathbf{Z}_2$ kan de kun antage værdierne 0 og 1, hvilket betyder, at

$$\begin{aligned} a + c = 1 &\Rightarrow ac = 0 \\ b + d + ac = 1 &\Rightarrow b + d = 1 \\ bd = 1 &\Rightarrow b = d = 1 \quad \text{Modstrid!}\end{aligned}$$

Modstriden består i, at når $b + d = 1$ kan $b = d = 1$ ikke lade sig gøre. Altså er $f(x)$ irreducibelt. Med hensyn til om det er et primitivt element, så kan vi liste alle elementerne op i legemet $\mathbf{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$(Dette er et legeme siden $f(x)$ er irreducibelt). Hvis x selv nu er et primitivt element i vores nye legeme, vil $f(x)$ være et primitivt element (s.352Biggs). Elementerne i legemet er som følger

$$\begin{array}{cccc} 0 & 1 & x & x+1 \\ x^2 & x^2+1 & x^2+x & x^2+x+1 \\ x^3 & x^3+1 & x^3+x & x^3+x+1 \\ x^3+x^2 & x^3+x^2+1 & x^3+x^2+x & x^3+x^2+x+1 \end{array}$$

Dvs. at x^p skal kunne generere alle elementerne i legemet på nær 0. Det forsøger vi nu at opskrive

$$\begin{array}{ccc} x^1 = x & x^2 = x^2 & x^3 = x^3 \\ x^4 = x^3 + x^2 + x + 1 & x^5 = 1 & \end{array}$$

siden der ialt er 15 elementer i legemet (2^4 minus 0-elementet), og $x^5 = 1$, er x ikke et primitive element i legemet, hvilket betyder at $x^4 + x^3 + x^2 + 1$ ikke er et primitivt element

Opgave 16.10.8

Lad b være et primitivt element i F_q, og for hvert naturligt tal n således, at $b^n \neq -1$, og lad $J(n)$ være defineret ved $b^n + 1 = b^{J(n)}$. Da skal vi opstille en tabel over $J(n)$ for henholdsvis F_9 og F_{13} med passende primitive elementer.

F_9 For at gøre det let for os selv, 'låner' vi Biggs F_9 på side 352, som er defineret ved $F_9 = \mathbf{Z}_3/x^2 - x - 1$. Elementerne i F_9 er

$$\begin{array}{cccc} x^1 = x & x^2 = x + 1 & x^3 = -x + 1 & x^4 = -1 \\ x^5 = -x & x^6 = -x - 1 & x^7 = x - 1 & x^8 = 1 \end{array}$$

Nu er det nemt at opskrive tabellen for $J(n)$

n	x^n	x^n+1	$J(n)$
1	x	$x+1=x^2$	2
2	$x+1$	$x-1=x^7$	7
3	$-x+1$	$-x-1=x^6$	6
4	-1	$0=$ikke def.	ikke def.
5	$-x$	$-x+1=x^3$	3
6	$-x-1$	$-x=x^5$	5
7	$x-1$	$x=x^1$	1
8	1	$-1=x^4$	4

(En tilsyneladende nok mest ubrugelige tabel i matematikkens anvendelse)

F_{13} Vi låner igen fra Biggs side. 325, denne gang legemet $\mathbf{Z}_{13}$. Det primitive element p findes ved at $p^{12}=1$, eller rættere $p^q \neq 1$ for $q \neq 12$. Dvs at $p^6=-1$. Det viser sig ved at prøve sig fren fro $n=1,2,\cdots,6$, at $2^6=-1$, altaå er 2 et primitivt element i F_{13}. Nu kan vi opstille tabellen for $J(n)$ tilsvarende som før.

n	2^n	2^n+1	$J(n)$
1	2	$3=2^2$	2
2	4	$5=2^9$	9
3	8	$9=2^8$	8
4	3	$4=2^2$	2
5	6	$7=2^{11}$	11
6	$12=(-1)$	$0=$ikke def.	ikke def.
7	11	$12=2^6$	6
8	9	$10=2^{10}$	10
9	5	$6=2^5$	5
10	10	$11=2^7$	7
11	7	$8=2^3$	3
12	1	$2=2^1$	1

Opgave 16.10.9

Vi skal vise, at hvis $J(n)$ er som givet i opgaven fra før, vil der for hver gang $J(n-m)$ er defineret, gælde

$$b^m + b^n = b^{m+J(n-m)}$$

Det er 'ren incasso' (øøh. hvem er det nu der plejer at sige det?)

$$\begin{aligned} b^{m+J(n-m)} &= b^m \cdot b^{J(n-m)} \\ &= b^m \cdot (b^{n-m}+1) \\ &= b^m \cdot (b^n \cdot b^{-m}+1) \\ &= b^m \cdot b^n \cdot b^{-m} + b^m \\ &= b^{m-m+n} + b^m \\ &= b^n + b^m \end{aligned}$$

Og det var det vi skulle vise

Opgave 17.7.13

Lad C_1 og C_2 være cykliske koder i V^n med generator hhv. $g_1(x)$ og $g_2(x)$. Da skal vi vise, at

$$C = C_1 + C_2 = \{c \in V^n | c = c_1 + c_2 \quad \text{,hvor } c_1 \in C_1 \text{ og } c_2 \in C_2\}$$

er en cyklisk kode med generator $\gcd(g_1(x), g_2(x))$.

Dette viser vi ved først at vise at $C \subseteq C_1 + C_2$ og derefter $C_1 + C_2 \subseteq C$. Først kan vi omskrive C_1 hhv C_2

$$\begin{aligned} C_1 &= < g_1(x) > \Rightarrow c_1(x) = p_1(x)g_1(x) \\ C_2 &= < g_2(x) > \Rightarrow c_2(x) = p_2(x)g_2(x) \\ C_1 + C_2 &= p_1(x)g_1(x) + p_2(x)g_2(x) \quad \forall p_i \in V^n[x] \end{aligned}$$

Da $\gcd(g_1(x), g_2(x)) = d(x)$, og som følge heraf

$$g_1(x) = g_1'(x)d(x) \qquad g_2(x) = g_2'(x)d(x)$$

kan vi opstille følgende

$$C_1 + C_2 = (p_1(x)g_1'(x) + p_2(x)g_2'(x))d(x)$$

Vi skal først sikre os, at $d(x)$ kan være en generator. Det gør vi ved at se om det kan faktorisere $x^n - 1$

$$x^n - 1 = g_1(x)h_1(x) = d(x)g_1'(x)h_1(x)$$

Vi ved at der eksisterer et sådant $h_1(x)$. Her kan vi se, at $d(x)$ er en kanonisk generator, hvor $h(x) = g_1'(x)h_1(x)$. Vi kan så definere idealet $C =< d(x) >$ Nu vender vi tilbage og ser, at $C_1 + C_2 \subseteq C$

$$C_1 + C_2 = (p_1(x)g_1'(x) + p_2(x)g_2'(x))d(x) \subseteq q(x)d(x)$$

Her kan vi se, at siden ringen er lukket, vil ethvert polynomium at typen $(p_1(x)g_1'(x) + p_2(x)g_2'(x))$ findes i ringen, nemlig som $q(x)$. Vi har her viset at $C_1 + C_2 \subseteq C$. Vi skal så vise den anden vej at $C \subseteq C_1 + C_2$. Dvs

$$\begin{aligned} < d(x) > &\subseteq < g_1(x) > + < g_2(x) > \\ q(x)d(x) &\subseteq (p_1(x)g_1'(x) + p_2(x)g_2'(x))d(x) \\ q(x) &\subseteq (p_1(x)g_1'(x) + p_2(x)g_2'(x)) \end{aligned}$$

Vi ved, at siden $\gcd(g_1(x), g_2(x)) = d(x)$ eksisterer der to polynomier $\mu(x)$ og $\lambda(x)$ sådan at

$$\begin{aligned} d(x) &= \mu(x)g_1(x) + \lambda(x)g_2(x) \\ 1 &= \mu(x)g_1'(x) + \lambda(x)g_2'(x) \end{aligned}$$

Lad os lige samle op på hvad vi har

$$\begin{aligned} q(x) &\subseteq (p_1(x)g_1'(x) + p_2(x)g_2'(x)) \\ 1 &= \mu(x)g_1'(x) + \lambda(x)g_2'(x) \\ q(x) &= q(x)\mu(x)g_1'(x) + q(x)\lambda(x)g_2'(x) \end{aligned}$$

Det kan ikke være svære at overbvise op om, at ethvert polynomium i ringen $q(x)$ kan skrives som $(p_1(x)g_1'(x) + p_2(x)g_2'(x))$ hvor

$$\begin{aligned} p_1 &= q(x)\mu(x) \\ p_2 &= q(x)\lambda(x) \end{aligned}$$

Nu er det klart at $C \subseteq C_1 + C_2$ som alt i alt betyder at $C = C_1 + C_2$

Opgave (Nedenstående)

Opgave a Samtlige idealer i $\mathbf{Z}_{15}$ Her har vi en møngde bestående at 15 elementer, nemlig $0, 1, \cdots, 14$. De mulige idealer fremkommer ved at vælge en generator som faktoriserer 15, og det er der 4 faktorer der gør nemlig 1,3,5 og 15. At vælge 1 eller 15 giver os de trivielle idealer nemlig hhv ringen selv og kun 0. Derfor fristes vi at lede efter dem der fremkommer ved $< 3 >$ og $< 5 >$ og som er

$$\begin{aligned} < 3 > &= 0, 3, 6, 9, 12 \\ < 5 > &= 0, 5, 10 \end{aligned}$$

Opgave b Her skal vi bestemme elementerne i ringen $R = \mathbf{Z}_3[x]/(x^2 - 1)$, og finde et ikke trivielt ideal $S \in R$.

Vi kan begynde med at finde de kanoniske generatorer, hvor vi tillader os med lidt guddommelig inspiration at se om ikke $(x^2 - 1) = (x + 1)(x - 1)$, og det viser sig at være tilfældet. Derfor kan vi lave 2 idealer som er ikke-trivielle med det samme, nemlig

$p(x)$	$p(x)(x+1)/(x^2-1)$	$p(x)(x-1)/(x^2-1)$
0	0	0
1	$1+x$	$-1+x$
-1	$1-1x$	$1-x$
x	$1+x$	$1-x$
$-x$	$-1-x$	$-1+x$
$x+1$	$-1-x$	0
$x-1$	0	$-1+x$
$-x+1$	0	$1+-x$
$-x-1$	$1+x$	0

Opgave c Vi skal vise, at der findes netop 2 ikke trivielle idealer i R. Vi har vist at der findes 2, vi skal så vise at der ikke er flere. Det kan vi vise ved at de elementer der indgår i et ikke-trivielt ideal, ikke har noget inverse element i ringen, thi ville det have et, ville 1-elementer fremkomme i idealet, og da uanset hvilket element fra et ideale vælger som generator vil få et nyt ideale som er en delmængde af det forrige ideale (S er lukket med hensyn til addition), vil det sige, at $< 1 > \subseteq S$ som derfor må være trivielt. Både $1, -1, x$ og $-x$ er sin egen inverse, hvilket betyder at de ikke kan generere andre idealer end et trivielt.