ÖVNING 9 - DISKRET MATEMATIK

ERIC AHLQVIST

1. Polynom

Biggs 22.4.4. För vilka värden på n gäller det i $\mathbb{Z}_n[x]$ att

$$(x+1)^n = x^n + 1\,?$$

Lösning. Vi har att

$$(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

så för att påståendet ska vara sant måste n dela $\binom{n}{i}$ för alla $0 \leq i \leq n$. Antag att n har primtalsfaktorisering

$$n = p_1^{e_1} \cdots p_s^{e_s}\,.$$

Vi har att

$$\binom{n}{p_i} = \frac{n!}{p_i!(n-p_i)!}$$

vilket inte är delbart med n. Dvs $(x+1)^n = x^n + 1$ om och endast om $\binom{n}{p_i}$ är koefficienten för x^n, alltså om och endast om $n = p_i$, dvs om och endast om n är ett primtal.

2. Faktorisering av polynom

Biggs 22.5.2. Hitta kvot och rest då $x^5+x^4+2x^3+x^2+4x+2$ delas med x^2+2x+3 i ringen $\mathbb{Z}_5[x]$.

Lösning. Polynomdivision ger

$$\begin{array}{rl}
 & x^3 - x^2 + x + 2 \\
\cline{2-2}
x^2+2x+3 \big) & x^5 + x^4 + 2x^3 + x^2 + 4x + 2 \\
 & \underline{-x^5 - 2x^4 - 3x^3} \\
 & \quad -x^4 - x^3 + x^2 \\
 & \quad \underline{x^4 + 2x^3 + 3x^2} \\
 & \qquad x^3 + 4x^2 + 4x \\
 & \qquad \underline{-x^3 - 2x^2 - 3x} \\
 & \qquad\quad 2x^2 + x + 2 \\
 & \qquad\quad \underline{-2x^2 - 4x - 6} \\
 & \qquad\quad -3x - 4
\end{array}$$

och eftersom vi är i ringen $\mathbb{Z}_5$ kan vi skriva om kvoten som

$$x^3 + 4x^2 + x + 2$$

och resten som

$$2x + 1\,.$$

3. Euklides algoritm för polynom

Biggs 22.6.1. Hitta den monisk *sgd* av $x^3 + x^2 + x + 1$ och $x^2 + 2$ i $\mathbb{Z}_3[x]$ och uttryck resultatet som

$$\lambda(x)(x^3 + x^2 + x + 1) + \mu(x)(x^2 + 2)$$

där $\lambda(x)$ och $\mu(x)$ är polynom i $\mathbb{Z}_3[x]$.

Lösning. Vi använder Euklides algoritm. Polynomdivision ger

$$\begin{array}{rr|l} & & x+1 \\ \hline x^2+2 & x^3+x^2+x+1 & \\ & -x^3 \quad -2x & \\ \hline & x^2-x+1 & \\ & -x^2 \quad -2 & \\ \hline & -x-1 & \end{array}$$

där resten kan skrivas om till $2x + 2$. Nästa steg är att dela $x^2 + 2$ med resten $2x + 1$. För att förenkla beräkningarna skriver vi nu $-x - 1$ istället för $2x + 2$.

$$\begin{array}{rr|l} & & -x+1 \\ \hline -x-1 & x^2 \quad +2 & \\ & -x^2-x & \\ \hline & -x+2 & \\ & x+1 & \\ \hline & 3 & \end{array}$$

Eftersom $3 = 0$ så är vi klara. En största gemensamma delare ges alltså av $2x + 2$ vilken inte är monisk. Men och vi multiplicerar med 2 får vi fortfarande en största gemensamma delare, vilken är $x + 1$ (monisk). Vi kan skriva denna som

$$\begin{aligned} x + 1 &= 2(x^3 + x^2 + x + 1) - 2(x + 1)(x^2 + 2) \\ &= 2(x^3 + x^2 + x + 1) + (x + 1)(x^2 + 2)\,. \end{aligned}$$

Dvs $\lambda(x) = 2$ och $\mu(x) = x + 1$.

4. Irreducibla polynom och unik faktorisering

Biggs 22.7.6. Verifiera att i $\mathbb{Z}_{15}[x]$ har vi

$$(x + 1)(x + 14) = (x + 4)(x + 11)\,.$$

Vad säger detta om ringen $\mathbb{Z}_{15}$ och ringen $\mathbb{Z}_{15}[x]$ i förhållande till teorin i Biggs Kapitel 22.7 ?

Lösning. Vi har att

$$\begin{aligned} (x + 1)(x + 14) &= x^2 + 15x + 14 \\ &= x^2 + 14 \end{aligned}$$

och att

$$\begin{aligned} (x + 4)(x + 11) &= x^2 + 15x + 44 \\ &= x^2 + 14\,. \end{aligned}$$

Detta betyder att $\mathbb{Z}_{15}[x]$ inte är en *UFD (unique factorization domain)*. Detta betyder att teorin i Kapitel 22.7 inte håller generellt för alla ringar eftersom den inte håller för $\mathbb{Z}_{15}$. Generellt gäller att $R[x]$ är en UFD om R är en UFD. Notera att $\mathbb{Z}_{15}$ inte är en UFD eftersom den har nolldelare, t.ex., $3 \cdot 5 = 0$.

5. Faktorsatsen

Sats 5.1. *Låt k vara en kropp och låt $p(x)$ vara ett polynom i $k[x]$. Om $\alpha \in k$ så är följande påståenden ekvivalenta:*

(1) *Vi har $p(\alpha) = 0$;*
(2) *Polynomet $x - \alpha$ är en faktor i $p(x)$.*

Biggs 22.8.1. Hitte de irreducibla faktorerna av
(a) $x^2 + 1$ i $\mathbb{Z}_5[x]$;
(b) $x^3 + 5x^2 + 5$ i $\mathbb{Z}_{11}[x]$;

Lösning. Enligt satsen ovan räcker det att söka efter rötter till polynomen.
(a) Vi har 2 och 3 är rötter och därmed har vi $x^2 + 1 = (x + 2)(x + 3)$.
(b) Först ser vi att 1 är en rot och $(x - 1 = x + 10)$ vi kan faktorisera

$$x^3 + 5x^2 + 5 = (x + 10)(x^2 + 6x + 6)\,.$$

Den sista faktorn har 2 som rot vilket ger

$$x^3 + 5x^2 + 5 = (x + 10)(x + 9)(x + 8)\,.$$

6. En kropp med 9 element

Ringen

$$\mathbb{Z}_3[x]/(x^2 + 1)$$

är en kropp av ordning 9 som vi kallar för $\mathbb{F}_9$.

Biggs 23.1.2. Vilka element i $\mathbb{F}_9$ har en kvadratrot?

Lösning. Vi har att

$$\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 1 \\ x^2 &= 2 \\ (x+1)^2 &= 2x \\ (x+2)^2 &= x \\ (2x)^2 &= 2 \\ (2x+1)^2 &= x \\ (2x+2)^2 &= 2x\,. \end{aligned}$$

Elementen som har en kvadratrot är alla element som förkommer som högerled.

7. Karaktäristiken hos en kropp

Låt k vara en kropp. Det minsta positiva heltal p sådant att $p \cdot 1 = 0$ i k kallas för *karaktäristiken* hos k och kan skrivas som $\mathrm{char}(k)$. Vi säger att k har karaktäristik p. Om inget sådant heltal existerar säger vi att k har karaktäristik 0.

Om karaktäristiken hos en kropp k är positiv så är den ett primtal vilket är ordningen av den minsta delkroppen till k. Om k har karaktäristik 0 så är $\mathbb{Q}$ den minsta delkroppen till k.

Biggs 23.2.4. Visa att i en kropp k av karaktäristik p så gäller att

$$(x+y)^p = x^p + y^p\,.$$

Lösning. Vi har att

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

och eftersom p är ett primtal så delar p heltalet $\binom{p}{i}$ för alla $1 \leq i \leq p-1$. Dvs $\binom{p}{i} = 0$ förutom då $i = 0$ och då $i = p$.

8. Konstruktion av ändliga kroppar

Sats 8.1. *Om f är ett irreducibelt polynom av grad r i $\mathbb{Z}_p[x]$ så är*

$$\mathbb{Z}_p[x]/(f)$$

en kropp av ordning p^r.

Biggs 23.3.1. Visa att $x^3 + x^2 + 1$ är irreducibelt i $\mathbb{Z}_2[x]$ och konstruera en kropp av ordning 8.

Lösning. Om polynomet inte var irreducibelt skulle vi kunna faktorisera det så att en av faktorerna har grad 1, vilket skulle ge en rot till polynomet. Eftersom varken 0 eller 1 är en rot så är detta ej möjligt.

9. Multiplikativa gruppen hos en ändlig kropp

Sats 9.1. *Den multiplikativa gruppen k^* av varje ändlig kropp k är cyklisk.*

Om k är en kropp så kallas en generator till dess multiplikativa grupp k^* för ett *primitivt element.*

Biggs 23.4.2. Visa att då x är ett primitivt element i

$$\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)\,.$$

Lösning. Vi har att x genererar gruppen $\{x, x^2, x^3 = x^2 + 1, x^4 = x^3 + x = x^2 + x + 1, x^5 = x^3 + x^2 + x = x + 1, x^6 = x^2 + x, x^7 = x^3 + x^2 = 1\}$, vilket är hela multiplikativa gruppen.

10. Summering för ändliga kroppar

Vi har att

(1) Varje ändlig kropp har ordning $q = p^r$ för något primtal p och något $r \in \mathbb{N}$.
(2) Alla kroppar av ordning q är isomorfa.
(3) Additiva gruppen är $(C_p)^r$.
(4) Multiplikativa gruppen är C_{q-1}.