MATEMATIK
Göteborgs universitet

Lösningar tenta MAN011 Aritmetik & Algebra del 2, 990529

4. Det gäller att visa att $p(x) = x^3+2x+4 \in \mathbb{Z}/5[x]$ är irreducibelt. Etftersom polynomet är av grad 3 räcker det, enligt faktorsatsen, att kontrollera att det saknar nollställe i $\mathbb{Z}/5$. Vi har $p(0) = 4,\ p(1) = 2,\ p(2) = 1,\ p(3) = p(-2) = 2,\ p(4) = p(-1) = 1$. Därmed är $\mathbb{Z}/5(\alpha)$ en kropp.
Vi bestämmer inversen med Euklides algoritm för en största gemensam delare till polynomen $\alpha^3 + 2\alpha + 4$ och $\alpha^2 + 2\alpha + 3$ och får

$$\begin{aligned}\alpha^3 + 2\alpha + 4 &= (\alpha + 3)(\alpha^2 + 2\alpha + 3) + 3\alpha \\ \alpha^2 + 2\alpha + 3 &= (2\alpha + 4)(3\alpha) + 3\end{aligned}$$

Baklänges ger detta:

$$\begin{aligned}3 = (\alpha^2 + 2\alpha + 3) - (2\alpha + 4)3\alpha &= (\alpha^2 + 2\alpha + 3) - (2\alpha + 4)(-(\alpha + 3)(\alpha^2 + 2\alpha + 3)) \\ &= (\alpha^2 + 2\alpha + 3)(1 + (2\alpha + 4)(\alpha + 3)),\end{aligned}$$

så $(\alpha^2 + 2\alpha + 3)^{-1} = 2(1 + (2\alpha + 4)(\alpha + 3)) = 1 + 4\alpha^2$ i $\mathbb{Z}/5(\alpha)$.

5. Polynomet $x^4+3x^3+6x^2+3x+2 \in \mathbb{Z}/7[x]$ saknar linjärfaktorer, ty $p(0) = 2$, $p(1) = 1$, $p(2) = 4$, $p(3) = 3$, $p(-3) = 5$, $p(-2) = 3$, $p(-1) = 3$. För att undersöka en eventuell faktor av grad 2 ansätter vi $p(x) = (x^2 + ax + b)(x^2 + cx + d)$, där a, b, c och d är i $\mathbb{Z}/7$. Identifiering av koefficienter ger ekvationssystemet

$$\begin{cases} 3 = a + c \\ 6 = b + ac + d \\ 3 = ad + bc \\ 2 = bd. \end{cases}$$

Den nedersta ekvationen ger $(b, d) = (1, 2)$, $(3, 3)$, $(4, 4)$ eller $(5, 6)$. Fallen där $b = d$ ger motstridiga första och tredje ekvationer. Om $(b, d) = (1, 2)$ ger första och tredje ekvationer att $a = 0$, $c = 3$, men då är andra ekvationen inte uppfyld. Slutligen ger $(b, d) = (5, 6)$ att $a = 2$ och $c = 1$, så vi har faktoriseringen

$$p = (x^2 + 2x + 5)(x^2 + x + 6)\ .$$

Vi sätter $K = \mathbb{Z}/7(\alpha)$, där $\alpha^2 = 5\alpha + 2$. Vi har $(\alpha + 1)^2 = 3$. Vi faktoriserar $x^2 + 2x + 5 = (x - \alpha)(x + 2 + \alpha)$. Lösningen till $x^2 + x + 6$ är enligt formeln $3 \pm \sqrt{3}$. Vi faktoriserar $x^2 + x + 6 = (x - 2 + \alpha)(x + 3 - \alpha)$ och därmed är

$$p(x) = (x - \alpha)(x + 2 + \alpha)(x - 2 + \alpha)(x + 3 - \alpha)\ .$$

6. Att skriva vektorn som linjärkombination ger ett ekvationssystem med utökad koefficientmatris:

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 1 \\ 2 & -2 & 3 & 9 \\ 3 & 3 & -1 & -4 \\ 4 & -4 & -1 & 11 \end{array}\right)$$

Med radoperationer överför vi den till trappstegsform:

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 1 \\ 2 & -2 & 3 & 9 \\ 0 & 0 & -7 & -7 \\ 0 & 0 & -7 & -7 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & 1 \\ 0 & -4 & -1 & 7 \\ 0 & 0 & -7 & -7 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Vi konkluderar att vektorerna är linjärt oberoende över $\mathbb{Q}$, men inte över $\mathbb{Z}/7$, och att

$$\begin{pmatrix} 1 \\ 9 \\ -4 \\ 11 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} + 2\begin{pmatrix} 1 \\ -2 \\ 3 \\ -4 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \\ -1 \\ -1 \end{pmatrix}.$$

Likheten gäller fortfarande modulo 7.

7. Vi beräknar först egenvärdena till A:

$$\begin{pmatrix} -\lambda & 7 & -6 \\ 1 & -\lambda & 0 \\ 0 & 1 & -\lambda \end{pmatrix} \sim \begin{pmatrix} 0 & 7-\lambda^2 & -6 \\ 1 & -\lambda & 0 \\ 0 & 1 & -\lambda \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & -6+7\lambda-\lambda^3 \\ 1 & -\lambda & 0 \\ 0 & 1 & -\lambda \end{pmatrix}$$

och egenvärdena är rötterna till $\lambda^3-7\lambda+6=(\lambda-1)(\lambda^2+1-6)=(\lambda-1)(\lambda-2)(\lambda+3)$. En egenvektor till $\lambda=1$ är $(1,1,1)$, till $\lambda=2$ $(4,2,1)$ och till $(\lambda=-3$ $(9,-3,1)$. Vi har

$$D=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{pmatrix}, \qquad C=\begin{pmatrix} 1 & 4 & 9 \\ 1 & 2 & -3 \\ 1 & 1 & 1 \end{pmatrix}.$$

Vi inverterar C:

$$\left(\begin{array}{ccc|ccc} 1 & 4 & 9 & 1 & 0 & 0 \\ 1 & 2 & -3 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 4 & 9 & 1 & 0 & 0 \\ 0 & 1 & -4 & 0 & 1 & -1 \\ 0 & -3 & -8 & -1 & 0 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 25 & 1 & -4 & 4 \\ 0 & 1 & -4 & 0 & 1 & -1 \\ 0 & 0 & -20 & -1 & 3 & -2 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 4 & 0 & 0 & -1 & -1 & 6 \\ 0 & 5 & 0 & 1 & 2 & -3 \\ 0 & 0 & -20 & -1 & 3 & -2 \end{array}\right)$$

Alltså är

$$C^{-1}=\frac{1}{20}\begin{pmatrix} -5 & -5 & 30 \\ 4 & 8 & -12 \\ 1 & -3 & 2 \end{pmatrix}$$

och $A^n=CD^nC^{-1}$ blir

$$\begin{pmatrix} -5+4\cdot 2^{n+2}+(-3)^{n+2} & -5+4\cdot 2^{n+3}+(-3)^{n+3} & -30-12\cdot 2^{n+2}+2(-3)^{n+2} \\ -5+4\cdot 2^{n+1}+(-3)^{n+1} & -5+4\cdot 2^{n+2}+(-3)^{n+2} & -30-12\cdot 2^{n+1}+2(-3)^{n+1} \\ -5+4\cdot 2^{n}+(-3)^{n} & -5+4\cdot 2^{n+1}+(-3)^{n+1} & -30-12\cdot 2^{n}+2(-3)^{n} \end{pmatrix}.$$

8. Monomer i utvecklingen har formen $x_1^{n_1}\cdot\ldots\cdot x_k^{n_k}$ med $n_1+\cdots+n_k=n$ och all sådana förekommer. Svaret är alltså antalet icke-negativa heltalslösningar till $n_1+\cdots+n_k=n$, som är $\binom{n+k-1}{k-1}=\binom{n+k-1}{n}$.