

Vak : Algebra voor TW/INF/BIT
 Vakcode : 151139
 Datum : 20 juni 2007
 Tijd : 9.00 - 12.00 uur

Alle antwoorden dienen gemotiveerd te worden.

Onderdelen waar u niet geheel uitkomt, kunt u zonder meer toch in het vervolg gebruiken. Mocht u door onverschillig welke omstandigheid een onderdeel niet geheel kunnen behandelen, dan verdient het in ieder geval aanbeveling om de aanpak te beschrijven.

1. Zij p een priemgetal. In $M_3(\mathbb{Z}_p)$, de 3×3 -matrices met coëfficiënten uit $\mathbb{Z}_p$, beschouwen we:

$$G = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ \beta & \gamma & \delta \end{pmatrix} \mid \alpha, \beta, \gamma \text{ en } \delta \in \mathbb{Z}_p, \alpha\delta \neq 0 \right\}$$

- (a) Laat zien dat G met de matrixvermenigvuldiging als bewerking een groep is.

Neem vanaf nu $p = 7$.

- (b) Boodschappen worden weergegeven in woorden uit $\mathbb{Z}_7^4$. Aan elke rij van 4 getallen $[a_1, a_2, a_3, a_4]$ voegen we 2 check-digits a_5 en a_6 toe, die voldoen aan

$$\begin{aligned} a_1 + a_2 + a_3 + a_4 + a_5 + a_6 &= [0]_7 \\ a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 &= [0]_7 \end{aligned}$$

Laat zien dat een dergelijke a_5 en a_6 altijd bestaan en dat deze geheel vastliggen bij gegeven $[a_1, a_2, a_3, a_4]$.

- (c) Aannemend dat er op hoogstens één plaats een fout gemaakt wordt in het woord $[a_1, \dots, a_6]$, laat zien hoe men die fout kan corrigeren.
 (d) We schrijven voor elke 3×1 -matrix

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}^T := (\alpha \quad \beta \quad \gamma).$$

Zij $g \in G$. Men codeert elk woord $[a_1, \dots, a_6]$ volgens

$$[a_1, \dots, a_6] \mapsto \left[\left(g \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \right)^T, \left(g \begin{pmatrix} a_4 \\ a_5 \\ a_6 \end{pmatrix} \right)^T \right]$$

Stel nu dat men $g = \begin{pmatrix} [2]_7 & [0]_7 & [0]_7 \\ [0]_7 & [1]_7 & [0]_7 \\ [2]_7 & [3]_7 & [1]_7 \end{pmatrix}$ heeft gebruikt om te coderen en dat men de rij

$$[[3]_7, [2]_7, [3]_7, [2]_7, [1]_7, [4]_7]$$

ontvangt. Decodeer dit woord en corrigeer hem evt., aannemende dat er hoogstens één fout gemaakt is bij de transmissie.

2. (a) Laat zien dat er drie verschillende irreducibele veeltermen zijn in $\mathbb{Z}_3[x]$ van de vorm $x^2 + ax + b$ en geef deze veeltermen.
- (b) Zij $g(x) = x^4 + x^3 + x^2 + x + 1$ en zij $F = \mathbb{Z}_3[x] / \langle g(x) \rangle$ de quotiëntring (factor ring) naar het ideaal $\langle g(x) \rangle := g(x)\mathbb{Z}_3[x]$. Laat zien dat F een lichaam is.
- (c) Zij $f = [x^2 + 1]_g \in F$, de klasse van $x^2 + 1$ in F . Bepaal een $h \in F$ met $fh = 1$.

1	a	:	3	2	a	:	2		
	b	:	2		b	:	2		
	c	:	2		c	:	2		
	d	:	3						

totaal = 16 + 4 = 20 punten