

Vak : **Opdrachten Algebra**
Vakcode : **151039**

Alle antwoorden dienen gemotiveerd te worden. I.h.b. moeten uitkomsten voorzien zijn van de stappen en berekeningen die tot het betreffende resultaat geleid hebben.

Onderdelen van een opdracht die U niet kan maken, kunnen wel verderop in de opdracht gebruikt worden.

Vragen: helminckgf@cs.utwente.nl

Zij F een lichaam. Voor $g = g(x) \in F[x]$ beschouwen we de ring $R = F[x]/(g(x)F[x])$ van veeltermen modulo g -vouden. De klasse waartoe $h \in F[x]$ behoort noteren we als $[h]_g$.

1. Laat m de graad van g zijn. Laat zien dat de elementen van R uniek te schrijven zijn als $[\sum_{i=0}^{m-1} a_i x^i]$, met $a_i \in F$. Dit bepaalt een identificatie $\varphi : R \mapsto F^m$ via

$$\varphi([\sum_{i=0}^{m-1} a_i x^i]) = (a_0, \dots, a_{m-1})$$

2. Laat zien m.b.v. de algorithmen van Euclides dat elk ideaal I van de ring $F[x]$ de vorm heeft

$$I = f(x)F[x] = \{f(x)h(x) \mid h(x) \in F[x]\}.$$

3. Zij $\pi : F[x] \mapsto R$ gedefinieerd door $\pi(h) = [h]_g$ en zij J een ideaal in R . Laat zien dat de afbeelding π een ringmorfisme is, dat

$$\pi^{-1}(J) = \{f \mid \pi(f) \in J\}$$

een ideaal in $F[x]$ vormt en dat

$$J = \{[d(x)h(x)]_g \mid h = h(x) \in F[x]\}$$

met $d(x)$ een deler van $g(x)$.

4. Neem van nu af aan $F = \mathbb{Z}_2$ en $g(x) = x^m - 1$. Een cyclische code $C \subset R$ is een lineaire deelruimte van R over $\mathbb{Z}_2$ waarvoor geldt

$$[\sum_{i=0}^{m-1} a_i x^i] \in C \Rightarrow [a_{m-1} + \sum_{i=0}^{m-2} a_i x^{i+1}] \in C.$$

Laat zien dat C een cyclische code is dan en slechts dan als C een ideaal is in de ring R .

5. Bepaal alle irreducibele factoren van $g(x) = x^6 - 1$.
6. Bereken alle cyclische codes voor het geval $g(x) = x^6 - 1$. Bereken de dimensie van elke cyclische code en geef voor elke $C \neq R$ een parity check matrix H_C , d.w.z.

$$C = \{[\sum_{i=0}^5 a_i x^i] \mid H_C \begin{pmatrix} a_0 \\ \vdots \\ a_5 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$$

7. Bepaal voor alle cyclische codes $C \neq \{0\}$ uit het voorafgaande onderdeel de minimumafstand tussen 2 vectoren c_1 en c_2 uit C met $c_1 \neq c_2$. Bespreek hoeveel fouten U met elk van deze codes kan detecteren resp. corrigeren.