

Opgelet

- (1) Dit tentamen bestaat uit zes vraagstukken (inclusief meerkeuzegedeelte).
- (2) Zakrekenmachines, etc., mogen niet gebruikt worden.
- (3) Goede toelichting scoort!
- (4) Op het tweede blad staat een apart gedeelte met meerkeuzevragen. **Schrijf je naam daar** en lever dat blad mee in met je oplossingen van de overige opgaven.
- (5) Het tentamen en een uitwerking verschijnen binnenkort op blackboard.

1. MODULOREKENEN

- (a) Algemene kennis.
 - (i) Definieer de *grootste gemene deler* $d \in \mathbb{N}$ van twee gehele getallen a en b ongelijk 0.
 - (ii) Geef de formule van Bezout voor gehele getallen a en b ongelijk 0.
- (b) Bereken $d = \text{ggd}(221, 143)$ met behulp van het Euclidisch algoritme en druk d in 221 en 143 uit (als in de formule van Bezout).
- (c) Los op met x en y in $\mathbb{Z}/17\mathbb{Z}$:

$$\begin{cases} \bar{3}x + y = \bar{2} \\ \bar{6}x + \bar{12}y = \bar{7} \end{cases}$$

2. GROEPEN

- (a) Algemene kennis.
 - (i) Wanneer is een niet-lege deelverzameling H van een groep G een *deelgroep*?
 - (ii) Definieer de *orde* van een element g in een groep G .
- (b) Bereken 7^{125} modulo 25 als standaardrepresentant $(0, 1, 2, \dots, 24)$ op een economische manier.
- (c) Gebruik de methode van de Chinese reststelling om alle gehele getallen x te vinden die voldoen aan $x \equiv 3$ modulo 4, $x \equiv 2$ modulo 5 en $x \equiv 1$ modulo 7.

3. RINGEN

- (a) Algemene kennis.
 - (i) Geef de definitie van een *nuldeler* in a ring R .
 - (ii) Definieer een *ideaal* I in een ring R .
- (b) Gegeven zijn het lichaam $K = \mathbb{Z}/7\mathbb{Z}$ en het polynoom $D(x) = x^4 + \bar{1}$ in $K[x]$. Codeer $B(x) = x^5 + \bar{2}$ als in CRC (cyclic redundancy check) met sleutel $D(x)$.
- (c) Laat $F = \mathbb{Z}/2\mathbb{Z}$.
 - (i) Bepaal alle irreducibele polynomen van graad 2 in $F[x]$.
 - (ii) Bepaal van $x^4 + x^2 + \bar{1}$ en $x^4 + x + \bar{1}$ in $F[x]$ of ze irreducibel zijn of niet.

4. VECTORRUIMTEN

- (a) Algemene kennis.
 - (i) Wanneer heten $v_1, \dots, v_n$ in een vectorruimte V over een lichaam F *lineair onafhankelijk*, en wanneer *voortbrengend*?
 - (ii) Gegeven zijn vectorruimten V en W over een lichaam F . Wanneer heet een afbeelding $f : V \rightarrow W$ een *lineaire afbeelding*?

(iii) Bereken AB en BA of leg uit waarom het product niet bestaat voor de matrices

$$A = \begin{pmatrix} \overline{2} & \overline{1} & \overline{1} \\ \overline{0} & \overline{1} & \overline{2} \end{pmatrix} \text{ en } B = \begin{pmatrix} \overline{3} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{0} \end{pmatrix}$$

met coëfficiënten in $\mathbb{Z}/5\mathbb{Z}$.

(b) Zij $F = \mathbb{Z}/7\mathbb{Z}$ en $V = \{(x, y, z) \text{ in } F^3 \text{ met } x + \overline{2}y + z = \overline{0}\}$. Laat zien dat V een deelruimte is van F^3 .

(c) Zij M de 2 bij 5 matrix met coëfficiënten in $\mathbb{Z}/5\mathbb{Z}$ gegeven door

$$M = \begin{pmatrix} \overline{1} & \overline{2} & \overline{0} & \overline{4} & \overline{0} \\ \overline{0} & \overline{1} & \overline{2} & \overline{0} & \overline{1} \end{pmatrix}.$$

Bepaal eerst de dimensie van de kolomruimte van M , en vervolgens van de nulruimte van M .

5. EINDIGE LICHAMEN

(a) Algemene kennis.

(i) Definieer een *primitief element* van een eindig lichaam K .

(ii) Voor welke eindige lichamen bestaat zo'n primitief element?

In (b) en (c) nemen we $K = \mathbb{Z}/2\mathbb{Z}$, $f(x) = x^3 + x^2 + \overline{1}$ in $K[x]$ en $F = K[x]/(f(x))$.

(b) Hoeveel elementen heeft F ?

Gegeven is dat F een lichaam is.

(c) Zij $\alpha = \overline{x}$ in F . Maak een tabel om in te zien dat α een primitief element is van F . Gebruik deze tabel om $\alpha^2 + \alpha^6$ rechtstreeks uit te drukken als macht van α .

Naam:

6. MEERKEUZEVRAGEN

- Bij iedere vraag is precies één van de onderdelen juist én (meest) volledig.
- Maak je keuze duidelijk door het vierkantje aan te kruisen of in te kleuren.
- Het antwoord hoeft niet te worden toegelicht.

6.1 Als $n = p_1 p_2 \cdots p_m$ ($m \geq 1$) voor verschillende priemgetallen p_i dan geldt, met ϕ de Euler functie:

- ☐ $\phi(n) = 1$;
- ☐ $\phi(n) = n - 1$;
- ☐ $\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_m - 1)$;
- ☐ geen van de eerste drie keuzes.

6.2 Als $n \geq 2$ dan zegt de stelling van Euler dat, met ϕ de Euler functie:

- ☐ $a^{\phi(n)} \equiv 1$ modulo n voor alle a in $\mathbb{Z}$;
- ☐ $a^{\phi(n)} \equiv 1$ modulo n voor alle a in $\mathbb{Z}$ met $\text{ggd}(a, n) = 1$;
- ☐ $a^n \equiv a$ modulo n voor alle a in $\mathbb{Z}$;
- ☐ $a^n \equiv a$ modulo n voor alle a in $\mathbb{Z}$ met $\text{ggd}(a, n) = 1$.

6.3 Zij R een unitaire ring met eenheidselement (identiteit) 1 en nulelement 0. Als $a \cdot b = 0$ voor zekere a en b in R , dan geldt $a = 0$ of $b = 0$

- ☐ altijd;
- ☐ alleen als $R = \mathbb{Z}$;
- ☐ als R een integriteitsgebied is;
- ☐ als R een integriteitsgebied is maar geen lichaam.

6.4 Zij $F = \mathbb{Z}/7\mathbb{Z}$ en $V = F^4$ als F -vectorruimte. In een lineaire deelruimte W van V

- ☐ zijn 7^4 elementen;
- ☐ zijn $4 \cdot 7 = 28$ elementen;
- ☐ zijn 1, 7, 7^2 , 7^3 of 7^4 elementen;
- ☐ zijn 1, 4, 4^2 , 4^3 , 4^4 , 4^5 , 4^6 of 4^7 elementen.

6.5 Zij K een lichaam en $f(x)$ in $K[x]$. Dan is $K[x]/(f(x))$ een lichaam als

- ☐ $f(x)$ irreducibel is in $K[x]$;
- ☐ $f(x)$ graad tenminste 1 heeft;
- ☐ $f(x)$ graad tenminste 2 heeft;
- ☐ $f(x)$ geen nulpunt heeft in F .

Normering:

1a	4	2a	4	3a	5	4a	7	5a	3	6.1	3
1b	4	2b	4	3b	5	4b	7	5b	2	6.2	3
1c	6	2c	6	3c	8	4c	4	5c	6	6.3	3
										6.4	3
										6.5	3
14		14		18		18		11		15	

Maximum totaal = 90

Cijfer = 1 + Totaal/10