



Opgelet: Er is een apart multiple-choice gedeelte op de laatste bladzijde (vraag 6). Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!

1. Modulorekenen

(a) Algemene kennis:

- (i) Zij $m \geq 2$ een geheel getal. Geef het relatievoorschrift voor de relatie x is congruent met y modulo m .
- (ii) Laat a, b gehele getallen ongelijk nul zijn. Wat zegt de *Bezout formule* over deze getallen?
- (iii) De *ISBN code* bestaat uit een aantal symbolen (cijfers 0-9 of 'x' voor '10'). Het laatste symbool is een "check" symbool. Wat is de check voorwaarde?

(b) In $\mathbb{Z}/(65)$ met vermenigvuldiging zoeken we naar de inverse van een klasse x . Completeer de volgende tabel.

x is:	inverse ja/nee:	(zo ja) inverse is:
$\overline{25}$		
$\overline{26}$		
$\overline{27}$		

Antwoorden volstaan. Een kopie van de tabel is beschikbaar achterop het multiple-choice blad.

(c) In een ISBN code werden het eerste en het derde symbool omgewisseld. Laat zien hoe je ontdekt dat er een fout is opgetreden (goede toelichting scoort).

2. Groepen

(a) Algemene kennis:

- (i) Je heb een groep van orde 29 en een element x wat niet het neutrale element is. Wat weet je van de *orde van x* ?
- (ii) Laat $m \geq 2$ geheel zijn. Wat wordt er weergegeven met de *Euler functie* $\phi(m)$?
- (iii) Formuleer de *Chinese reststelling* in een situatie waar je precies twee moduli m_1, m_2 hebt.

(b) Zoek een geheel getal x dat tegelijk voldoet aan $x \equiv 11 \pmod{14}$ en $x \equiv 8 \pmod{15}$ (goede toelichting scoort).

(c) Bereken $10^{74} \pmod{51}$ op een economische manier (goede toelichting scoort).

3. Veeltermringen

(a) Algemene kennis:

- (i) Wat bedoelt men met de *graad van een veelterm*?
- (ii) In sommige veeltermringen $R[X]$ geldt de *gradenformule*. Wat zegt deze formule en voor welk type van ringen R is ze geldig?
- (iii) Gegeven een lichaam K en twee veeltermen A, B ongelijk nul in de veeltermring $K[X]$, zegt de *Delingsalgoritme* iets over een formule van de vorm $A = B \cdot Q + R$. Wat wordt er precies gezegd?

- (b) Zij K een lichaam. Laat zien dat een veelterm $P \in K[X]$ van graad ≥ 1 geen (multiplicatieve) inverse kan hebben in $K[X]$ (goede toelichting scoort).
- (c) Zij $K := \mathbb{Z}/(5)$. Controleer of de veelterm $X^3 + X + 1$ in $K[X]$ irreducibel is (goede toelichting scoort).
- (d) Zij $K := \mathbb{Z}/(2)$. Bepaal quotiënt en rest in $K[X]$ bij deling van de veelterm $M := X^4 + X + 1$ door $X^2 + X + 1$. (N.B.: de rest moet ongelijk nul zijn.) Het is bekend dat $X^2 + X + 1$ de enige tweedegraadse irreducibele veelterm is in $K[X]$ (niet aantonen). Probeer nu af te leiden dat M irreducibel is in $K[X]$.

4. Vector ruimten

(a) Algemene kennis:

- (i) Wat bedoelt men met een *lineair onafhankelijk stel vectoren* $\{v_1, \dots, v_n\}$ in een vector ruimte V over een lichaam $\mathbb{F}$?
- (ii) Wat bedoelt men met een *voortbrengend stel vectoren* $\{v_1, \dots, v_n\}$ in een vector ruimte V over een lichaam $\mathbb{F}$?
- (iii) Wat bedoelt men met een *basis* in een vector ruimte V over een lichaam $\mathbb{F}$?

(b) We bekijken volgende drie vectoren achtereenvolgens in $\mathbb{Z}/(3)$ en in $\mathbb{Z}/(5)$:

$$u := \begin{pmatrix} \overline{0} \\ \overline{1} \\ \overline{2} \end{pmatrix}, \quad v := \begin{pmatrix} \overline{1} \\ \overline{2} \\ \overline{0} \end{pmatrix}, \quad w := \begin{pmatrix} \overline{2} \\ \overline{0} \\ \overline{1} \end{pmatrix}.$$

Laat zien dat $\{u, v, w\}$ lineair afhankelijk is in $(\mathbb{Z}/(3))^3$, maar lineair onafhankelijk in $(\mathbb{Z}/(5))^3$. Beredeneer dat het in dit geval zelfs om een basis gaat.

(c) Neem nu volgende 3 bij 5 matrix over $\mathbb{Z}/(5)$ (de eerste drie kolommen zijn precies de vectoren uit deel (b)):

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

Bepaal de dimensie van de nulruimte van M (goede toelichting scoort).

5. Eindige lichamen

(a) Algemene kennis.

- (i) Waar staat "GF(27)" precies voor?
- (ii) Wat is de orde van de multiplicatieve groep $GF(27)^*$?
- (iii) Leg uit: het *Diffie-Hellman protocol* voor sleuteluitwisseling.

De veelterm $M := X^4 + X + 1$ is irreducibel in $\mathbb{Z}/(2)[X]$ (dit is het resultaat van Opgave 3(d)). Volgens de theorie is $\mathbb{F} := (\mathbb{Z}/(2)[X]) / (M)$ een lichaam.

- (b) Bepaal het aantal elementen in $\mathbb{F}^*$ (antwoord volstaat).
- (c) Welke ordes zijn er effectief mogelijk voor een element van $\mathbb{F}^*$ (goede toelichting scoort)?
- (d) Controleer nu op efficiënte wijze dat de klasse $\bar{X}$ (modulo M) een generator is van $\mathbb{F}^*$.
Aanwijzing: $\bar{X}^4 + \bar{X} + \bar{1} = \bar{0}$.

Normering:

1a:	4	2a:	4	3a:	3	4a:	4	5a:	4	6:	15
1b:	6	2b:	6	3b:	3	4b:	5	5b:	3		
1c:	5	2c:	5	3c:	4	4c:	5	5c:	4		
				3d:	5			5d:	5		
15		15		15		14		16		15	

Totaal = 90; Cijfer = Totaal/10 + 1

Leeg blad ten behoeve van apart multiple-choice gedeelte.

naam, studierichting & jaar:

18-12-02

6. Multiple-choice gedeelte

- Bij iedere vraag is precies één van de onderdelen juist én (meest) volledig.
- Het antwoord (aangekruist of zwartgemaakt bolletje) hoeft niet te worden toegelicht.

6.1. Over priemrestklassen.

- o $\overline{13}$ is een priemrestklasse modulo 26.
- o De som van twee priemrestklassen modulo 26 is weer een priemrestklasse modulo 26.
- o Het product van twee priemrestklassen modulo 26 is weer een priemrestklasse modulo 26.
- o Er zijn geen priemrestklassen modulo 26 want 26 is niet priem.

6.2. Een deelgroep H van een groep $(G, *)$ is

- o Een deelverzameling H van G met een operatie $x \# y$, zó dat $(H, \#)$ een groep is.
- o Een deelverzameling H van G die stabiel is onder de operatie $x * y$ van G .
- o Een deelverzameling H van G die stabiel is onder de operatie y^{-1} (inverse) van G .
- o Een deelverzameling H van G die stabiel is onder de operatie $x * y^{-1}$ van G .

6.3. Een ideaal van een commutatieve unitaire ring R is een deelverzameling van R die

- o stabiel is onder de optelling $x + y$ en de vermenigvuldiging $x \cdot y$ van R .
- o stabiel is onder de optelling $x + y$ van R en "super"stabiel is onder de vermenigvuldiging $x \cdot y$ van R .
- o stabiel is onder de aftrekking $x - y$ en de vermenigvuldiging $x \cdot y$ van R , en die het eenheidselement van R bevat.
- o stabiel is onder de aftrekking $x - y$ van R en "super"stabiel is onder de vermenigvuldiging $x \cdot y$ van R , en die het eenheidselement van R bevat.

N.B.: Een verzameling $A \subseteq R$ is superstabiel onder een bewerking $x \# y$ in R wanneer geldt: als $x \in R$ en $y \in A$ dan $x \# y \in A$.

6.4. Zij V een vectorruimte van dimensie 3 over een lichaam $\mathbb{F}$ met 4 elementen. Dan is

- o $\#V = 64 (= 4^3)$.
- o $\#V = 81 (= 3^4)$.
- o $\#V = 12 (= 3 \cdot 4)$.
- o $\#V$ onbepaald want er zijn onvoldoende gegevens.

6.5. Een primitief element van een lichaam K is

- o een irreducibele veelterm in $K[X]$.
- o een generator van de additieve groep van K .
- o een generator van de multiplicatieve groep van K .
- o een element van K zonder multiplicatieve inverse.

x is:	inverse ja/nee:	(zo ja) inverse is:
---------	-----------------	---------------------

$\overline{25}$		
-----------------	--	--

$\overline{26}$		
-----------------	--	--

$\overline{27}$		
-----------------	--	--

Tabel bij Opgave 1(b): $\mathbb{Z}/(65)$		
--	--	--