



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) Wat bedoelt men met: een priemrestklasse modulo m (waar $m \in \mathbb{Z}$, $m \geq 2$, de modulus is)?
 - (ii) Hoeveel elementen heeft de verzameling priemrestklassen $(\mathbb{Z}/(14))^*$?
- (b) Bereken de (multiplicatieve) inverse van 33 modulo 46. Geef toelichting bij de onderdelen van je berekening (goede toelichting scoort).
- (c) Modulo 26 beschikken we over de volgende matrix M en zijn inverse M^{-1} :

$$M := \begin{pmatrix} \bar{2} & \bar{-3} \\ \bar{3} & \bar{1} \end{pmatrix}, \quad M^{-1} = \begin{pmatrix} \bar{-7} & \bar{5} \\ \bar{-5} & \bar{12} \end{pmatrix}$$

Iedere letter wordt door zijn rangnummer weergegeven ($a=1, \dots, z=26$). Codeer "zo" en decodeer "qk"

2. De stelling van Euler en exponentenrekening modulo m

- (a) Algemene kennis:
- (i) Wat bedoelt men met de orde van een element in een groep G met "vermenigvuldiging" $''\cdot''$?
 - (ii) Wat bedoelt men met de orde van een (eindige) groep G ?
 - (iii) Als een groep orde 14 heeft, welke ordes zijn dan mogelijk voor een element van die groep?
- (b) Wat zegt de stelling van Euler over machten van elementen van $(\mathbb{Z}/(m))^*$?
- (c) Bereken op economische wijze: 7^{116} modulo 39. Geef toelichting bij je berekeningen (goede toelichting scoort).

3. Veeltermringen

- (a) Algemene kennis:
- (i) Wat is een nulpunt van een veelterm over een lichaam?
 - (ii) Wat is een irreducibele veelterm over een lichaam?
 - (iii) Wat is het verband tussen de onderwerpen uit (i) en (ii)?
- (b) Bepaal de nulpunten van de veelterm $F := X^3 + X + 1$ over de lichamen $\mathbb{Z}/(3)$ en $\mathbb{Z}/(5)$.
- (c) Hoeveel elementen heeft het quotiënt $K[X]/(F)$ als $K := \mathbb{Z}/(3)$ en als $K := \mathbb{Z}/(5)$?
- (d) Is $K[X]/(F)$ een lichaam als $K := \mathbb{Z}/(3)$? En als $K := \mathbb{Z}/(5)$?

4. Vectorruimten

(a) Algemene kennis:

- (i) Wat bedoelt men met een lineaire deelruimte W van een vectorruimte V (over een gegeven lichaam $\mathbb{F}$)?
- (ii) In de "dimensiestelling" voor een lineaire afbeelding $f: V \rightarrow W$ tussen twee vectorruimten V, W over een lichaam $\mathbb{F}$ is sprake van de kern van f (genoteerd $\ker(f)$) en het beeld van f (genoteerd $\text{beeld}(f)$). Formuleer deze stelling.
- (iii) Een n bij m matrix M (n rijen, m kolommen) met getallen uit een lichaam $\mathbb{F}$ produceert een lineaire afbeelding $\mathbb{F}^m \rightarrow \mathbb{F}^n$ op de "standaard wijze": een kolom m -vector v wordt getransformeerd in een kolom n -vector $w := M \cdot v$. Wat bedoelt men met "kolomruimte" en met "nulruimte" van een matrix M ?

(b) Gegeven is de 3 bij 5 matrix

$$M := \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Bepaal eerst de dimensie van de kolomruimte, en dan de dimensie van de nulruimte.

5. Primitieve elementen. We werken in deze opgave met de quotiëntring $K := (\mathbb{Z}/(3))[X]/(X^2 + 1)$.

(a) Algemene kennis:

- (i) Leg uit waarom K een lichaam is.
- (ii) Welke multiplicatieve ordes zijn er effectief mogelijk voor elementen van K^* ?
- (iii) Wat bedoelt men met "een primitief element van een lichaam"?
- (b) Eén van de elementen $\bar{X}$, $\overline{X+1}$ uit K is primitief. Zoek uit welk van beide, en noem dit element α .
- (c) Maak een tabel van de machten van α , geschreven met standaard representanten (d.w.z. met veeltermen van graad kleiner dan de graad van de modulus $X^2 + 1$).

Normering:

1a: 3	2a: 5	3a: 5	4a: 6	5a: 5	6: 14
1b: 5	2b: 3	3b: 3	4b: 6	b: 4	
1c: 8	2c: 8	3c: 4		c: 7	
		3d: 4			
16	16	16	12	16	14

Totaal = 90; Cijfer = Totaal/10 + 1

naam, studierichting & jaar:

3-2-2004

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. De formule van Bezout in $\mathbb{Z}$ stelt dat:

- o bij iedere $a, b \neq 0$ een uniek stel getallen q, r bestaat met $b = a \cdot q + r$ en $0 \leq r < a$.
- o bij iedere $a, b \neq 0$ geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .
- o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
- o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$.

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

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

6.3. Een cyclische groep is:

- o een deelgroep van de cirkelgroep (complexe getallen van modulus 1).
- o een groep bestaande uit cyclische permutaties.
- o een groep die een generator (voortbrenger) heeft.
- o een groep die géén generator (voortbrenger) heeft.

6.4. Een nuldeeler in een ring is

- o een element a dat 0 deelt.
- o een synoniem voor 0.
- o een element a met $a \cdot b = 0$ voor zekere b .
- o een element $a \neq 0$ met $a \cdot b = 0$ voor zekere $b \neq 0$.

6.5. Volgende verzameling is een ideaal in de ring $\mathbb{Z}, +, \cdot$:

- o De verzameling van alle drievouden.
- o De verzameling van alle oneven getallen.
- o De verzameling van alle niet-priemgetallen.
- o De verzameling $\{0, 1, -1\}$.

6.6. Een basis in een vectorruimte (lineaire ruimte) V is:

- o Een zo klein mogelijke lineaire deelruimte.
- o Een zo groot mogelijke lineaire deelruimte.
- o Een lineair onafhankelijke deelverzameling die heel V voortbrengt.
- o Een verzameling van eenheidsvectoren.

6.7. Een vectorruimte van dimensie 3 over het lichaam $\mathbb{Z}/(2)$ heeft

- o $2 + 3 = 5$ elementen.
- o $2 \cdot 3 = 6$ elementen.
- o $2^3 = 8$ elementen.
- o $3^2 = 9$ elementen.