

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. Modulo rekenen

(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} :

$$M := \begin{bmatrix} \overline{2} & \overline{-3} \\ \overline{3} & \overline{1} \end{bmatrix}; \quad M^{-1} = \begin{bmatrix} \overline{-7} & \overline{5} \\ \overline{-5} & \overline{12} \end{bmatrix}.$$

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" $''*$ '?

(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

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

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: 5	5a: 5	6: 16
1b: 5	2b: 3	3b: 3	4b: 5	b: 4	
1c: 8	2c: 8	3c: 4		c: 7	
		3d: 4			
16	16	16	10	16	16

Totaal = 90; Cijfer = Totaal/10 + 1

naam, studierichting & jaar:

03-04-02

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. De delingsalgoritme 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 monoïde is

- o een semigroep met een neutraal element.
- o een alternatieve benaming voor een unitaire ring.
- o een vector ruimte van dimensie 1.
- o een veeltermring met uitsluitend veeltermen van graad 1.

6.3. De orde van een element g in een eindige groep G met neutraal element e is:

- o het kleinste getal $k > 0$ waarvoor $g^k = e$.
- o het grootste getal $k > 0$ waarvoor $g^k = e$.
- o het rangnummer van g in de opsomming van alle elementen uit G .
- o het aantal elementen in G met dezelfde inverse als g .

6.4. Een ideaal I in een CUR (commutatieve unitaire ring) R is:

- o een additieve en multiplicatieve deelgroep van R .
- o een additieve deelgroep met die stabiel is voor vermenigvuldiging, d.w.z.: $x \cdot y \in I$ voor alle $x, y \in I$.
- o een additieve deelgroep met die "super"stabiel is voor vermenigvuldiging, d.w.z.: $x \cdot y \in I$ voor alle $x \in R$ en $y \in I$.
- o een additieve deelgroep met die "mega"stabiel is voor vermenigvuldiging, d.w.z.: $x \cdot y \in I$ voor alle $x, y \in R$.

6.5. Gegeven een lichaam K en een veelterm M over K , dan is $K[X]/(M)$ een lichaam precies dan als

- o M van graad ≤ 1 is.
- o de graad van M een priemgetal is.
- o M irreducibel is.

☐ M geen nulpunten heeft.

6.6. Er bestaat een lichaam met

☐ 6 elementen.

☐ 9 elementen.

☐ 12 elementen.

☐ 15 elementen.

Normering:

1a: 3	2a: 3	3a: 3	4a: 3	5a: 3	6: 16
1b: 4	2b: 5	3b: 4	4b: 4	b: 5	
1c: 9	2c: 8	3c: 4	3	c: 8	
		3d: 5			
16	16	16	10	16	16

Totaal = 90; Cijfer = Totaal/10 + 1 Multiple choice: -3ptn per fout