

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.**

1. MODULOREKENEN

- (a) Algemene kennis.
 - (i) Wanneer heten twee gehele getallen $a \neq 0$ en $b \neq 0$ *relatief priem*?
 - (ii) Stel $m \geq 2$ is een geheel getal. Wat is $(\mathbb{Z}/m\mathbb{Z})^*$?
- (b) Bereken $d = \text{ggd}(234, 198)$ met behulp van het Euclidisch algoritme en druk d in 234 en 198 uit (als in de formule van Bezout).
- (c) Los op met x en y in $\mathbb{Z}/13\mathbb{Z}$:

$$\begin{cases} \bar{2}x + \bar{3}y = \bar{1} \\ \bar{3}x + \bar{8}y = \bar{2} \end{cases}$$

2. GROEPEN

- (a) Algemene kennis.
 - (i) Wanneer heet een groep G *cyclisch*?
 - (ii) Wat zegt de *stelling van Lagrange* over de orde van een ondergroep H van een eindige groep G ?
- (b) Bereken 13^{2009} modulo 40 als standaardrepresentant $(0, 1, 2, \dots, 39)$ op een economische manier.
- (c) Gebruik de methode van de Chinese reststelling om alle gehele getallen x te vinden die voldoen aan $x \equiv 0$ modulo 3, $x \equiv 2$ modulo 5 en $x \equiv 1$ modulo 8.

3. RINGEN

- (a) Algemene kennis.
 - (i) Definieer de *grootste gemene deler* van twee veeltermen $F_1(x)$ en $F_2(x)$ ongelijk nul in $K[x]$, waar K een lichaam is.
 - (ii) Wanneer is een afbeelding $f : R \rightarrow S$ van de ring R naar de ring S een *ringhomomorfisme*?
- (b) Gegeven zijn het lichaam $K = \mathbb{Z}/5\mathbb{Z}$ en het polynoom $D(x) = x^3 + x^2 + \bar{1}$ in $K[x]$. Codeer $B(x) = x^4 + \bar{2}$ als in CRC (cyclic redundancy check) met sleutel $D(x)$.
- (c) Laat $F = \mathbb{Z}/3\mathbb{Z}$.
 - (i) Bepaal alle *monische* irreducibele polynomen van graad 2 in $F[x]$.
 - (ii) Bepaal van $x^4 + \bar{1}$ en $x^4 + \bar{2}$ in $F[x]$ of ze irreducibel zijn of niet.

4. VECTORRUIMTEN

(a) Algemene kennis.

Stel V is een vectorruimte over het lichaam F .

(i) Wanneer heet een niet-lege deelverzameling W van V een *lineaire deelruimte*?

(ii) Definieer wanneer $\{v_1, \dots, v_n\}$ een *basis* is van V . Wat zijn dan de *coördinaten* van een vector v met betrekking tot deze basis? En wat is de *dimensie* van V ?

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

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

met coëfficiënten in $\mathbb{Z}/3\mathbb{Z}$.

(c) Zij $F = \mathbb{Z}/5\mathbb{Z}$ en $V = \{(x, y, z) \text{ in } F^3 \text{ met } x + \bar{2}y + \bar{3}z = \bar{0}\}$. Gegeven is dat V een lineaire deelruimte is van F^3 . Laat zien dat $\{(\bar{1}, \bar{3}, \bar{1}), (\bar{0}, \bar{1}, \bar{1})\}$ een basis is van V .

(d) Zij M de 2 bij 3 matrix met coëfficiënten in $\mathbb{Z}/3\mathbb{Z}$ gegeven door

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

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

5. EINDIGE LICHAMEN

(a) Algemene kennis.

(i) Definieer de *karacteristiek* van een lichaam K .

(ii) Bestaan er eindige lichamen met 4, 5, 6 of 7 elementen? Licht je antwoord toe.

In (b) en (c) nemen we $K = \mathbb{Z}/2\mathbb{Z}$, $f(x) = x^4 + x^3 + \bar{1}$ in $K[x]$ en $F = K[x]/(f(x))$.

(b) Hoeveel elementen heeft F ?

Gegeven is dat F een lichaam is.

(c) Zij $\alpha = \bar{x}$ in F . Bereken α^3 en α^5 . Is α primitief? Licht je antwoord toe.

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 $m = p_1 p_2 \cdots p_n$ ($n \geq 2$) voor verschillende priemgetallen p_i dan zegt het RSA lemma voor $e \geq 1$ dat, met ϕ de Euler ϕ -functie:

- ☐ $a^e \equiv a$ modulo $\phi(m)$ voor elk geheel getal a ;
- ☐ $a^e \equiv a$ modulo m voor elk geheel getal a als $e \equiv 1$ modulo m ;
- ☐ $a^e \equiv a$ modulo m voor elk geheel getal a als $e \equiv 1$ modulo $m - 1$;
- ☐ $a^e \equiv a$ modulo m voor elk geheel getal a als $e \equiv 1$ modulo $\phi(m)$.

6.2 Als $n = 100$ dan zegt de stelling van Euler dat

- ☐ $a^{99} \equiv 1$ modulo n voor alle a in $\mathbb{Z}$;
- ☐ $a^{72} \equiv 1$ modulo n voor alle a in $\mathbb{Z}$ ongelijk 0;
- ☐ $a^{40} \equiv 1$ modulo n voor alle a in $\mathbb{Z}$ met $\text{ggd}(a, n) = 1$;
- ☐ $a^{99} \equiv 1$ modulo n voor alle a in $\mathbb{Z}$ niet deelbaar door 10.

6.3 Zij R een unitaire ring met eenheidselement (identiteit) 1 en nulelement 0. Dan is een eenheid van R

- ☐ een andere naam voor 1;
- ☐ elk element ongelijk 0;
- ☐ een element a in R waarvoor b in R bestaat met $ab = 1 = ba$;
- ☐ een element a in R waarvoor $b \neq 0$ in R bestaat met $ba = a = ab$.

6.4 Zij F een lichaam met 16 elementen en $V = F^3$ als F -vectorruimte. Een lineaire deelruimte W van V

- ☐ heeft 1, 2, 4, 8 of 16 elementen;
- ☐ heeft 1, 16, 16^2 of 16^3 elementen;
- ☐ kan alleen $\{(0, 0, 0)\}$ zijn omdat 3 geen deler is van 16;
- ☐ heeft 1, 3, 3^2 , 3^3 , 3^4 , $3^5, \dots, 3^{13}$, 3^{14} , 3^{15} of 3^{16} elementen.

6.5 Zij $R = \mathbb{Q}[x]/(x^3 - 1)$. Dan is $\overline{x - 1} \cdot \overline{x^2 + 1}$ in R gelijk aan

- ☐ $\overline{-x^2 + x}$;
- ☐ $\overline{-x^2 + x - 2}$;
- ☐ niet gedefinieerd omdat $x^3 - 1$ een nulpunt heeft in $\mathbb{Q}$;
- ☐ niet gedefinieerd omdat 1 nulpunt is van zowel $x - 1$ als $x^3 - 1$.

Normering:

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

Maximum totaal = 90

Cijfer = 1 + Totaal/10