

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 later vandaag op blackboard.

1. MODULOREKENEN

- (a) Algemene kennis.
 - (i) Definieer de notatie $a|b$ in formules, als a en b gehele getallen zijn.
 - (ii) Formuleer de stelling over deling met rest voor gehele getallen a en b met $b \neq 0$.
- (b) In $\mathbb{Z}/56\mathbb{Z}$ zoeken we de multiplicatieve inverse van een klasse x . Geef die of leg uit waarom die niet bestaat wanneer $x = \overline{22}$ en ook wanneer $x = \overline{23}$.
- (c) Los op met x en y in $\mathbb{Z}/29\mathbb{Z}$:

$$\begin{cases} \overline{4}x + y = \overline{0} \\ \overline{7}x + \overline{13}y = \overline{1} \end{cases}$$

2. GROEPEN

- (a) Algemene kennis.
 - (i) Definieer wanneer een groep *cyclisch* genoemd wordt.
 - (ii) Gegeven is dat een groep G 10 elementen heeft. Welke mogelijkheden laat dit open voor de orde van een element in G ?
- (b) Bereken 11^{123} modulo 41 (als 0, 1, 2, ..., 40) op een economische manier.
- (c) Gebruik de methode van de Chinese reststelling om alle gehele getallen x te vinden die voldoen aan $x \equiv 2$ modulo 5, $x \equiv 3$ modulo 6 en $x \equiv 0$ modulo 7.

3. RINGEN

- (a) Algemene kennis.
 - (i) Gegeven een ring R met een deelverzameling I , definieer (in formules) dat I een ideaal van R is.
 - (ii) Geef de formule van Bezout voor twee polynomen $f(x)$ en $g(x)$ (ongelijk nul) in $K[x]$ als K een lichaam is.
- (b) Gegeven is het lichaam $K = \mathbb{Z}/5\mathbb{Z}$ en het polynoom $f(x) = x^4 + x + \overline{2}$ in $K[x]$. Is $K[x]/(f(x))$ een lichaam? Beargumenteer je antwoord.
- (c) Als $F = \mathbb{Z}/2\mathbb{Z}$, vind de grootste gemene deler van $f(x) = x^4 + \overline{1}$ en $g(x) = x^2 + x$ in $F[x]$ met behulp van het algoritme van Euclides.

4. VECTORRUIMTEN

- (a) Algemene kennis.
 - (i) Gegeven een vectorruimte V over een lichaam F , wanneer is een deelverzameling W van V een lineaire deelruimte?
 - (ii) Gegeven is dat $\{v_1, \dots, v_n\}$ een basis is van een vectorruimte V over een lichaam F . Definieer de coördinaten in deze basis van een vector w in V .

(iii) Voor de matrices

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

met coëfficiënten in $\mathbb{Z}/3\mathbb{Z}$ bereken AB en BA of leg uit waarom het product niet bestaat.

(b) Laat zien dat de vectoren $u = (\frac{\bar{2}}{3})$ en $v = (\frac{\bar{1}}{4})$ een basis vormen van K^2 als vectorruimte over K , waar $K = \mathbb{Z}/7\mathbb{Z}$. Laat ook zien dat dit niet zo is als $K = \mathbb{Z}/5\mathbb{Z}$.

(c) Zij M de 2 bij 5 matrix met coëfficiënten in $\mathbb{Z}/7\mathbb{Z}$ gegeven door

$$M = \begin{pmatrix} \bar{2} & \bar{1} & \bar{4} & \bar{2} & \bar{4} \\ \bar{3} & \bar{4} & \bar{3} & \bar{5} & \bar{6} \end{pmatrix}.$$

Bepaal eerst de dimensie van de kolomruimte van M , en vervolgens van de nulruimte van M . (Hint: de eerste twee kolommen zijn precies de vectoren in (b).)

5. EINDIGE LICHAMEN

(a) Algemene kennis.

(i) Definieer de karakteristiek van een lichaam K .

(ii) Welke getallen komen in aanmerking als aantal elementen van een eindig lichaam?

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

(b) Gegeven is dat $F = K[x]/(f(x))$ een lichaam is. Hoeveel elementen heeft F ?

(c) Zij $\alpha = \bar{x}$ in F . Maak een tabel om in te zien dat α een primitief element is van F . Gebruik deze tabel om $\alpha^4 + \alpha^6$ rechtstreeks uit te drukken als macht van α .

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 Voor $m \geq 2$ bestaat $(\mathbb{Z}/m\mathbb{Z})^*$ uit

- ☐ de restklassen $\bar{a}$ voor $a = 1, \dots, m-1$;
- ☐ de restklassen $\bar{a}$ waarvoor a geen kwadraat is;
- ☐ de restklassen $\bar{a}$ waarvoor a een deler is van m ;
- ☐ de restklassen $\bar{a}$ voor die $a = 1, \dots, m-1$ waarvoor $\text{ggd}(a, m) = 1$;

6.2 Het RSA lemma voor $p_1, \dots, p_k$ verschillende priemgetallen met product m zegt dat

- ☐ $a^{m-1} \equiv a$ modulo m voor elke a in $\mathbb{Z}$;
- ☐ $a^{\phi(m)} \equiv a$ modulo m voor elke a in $\mathbb{Z}$;
- ☐ $a^e \equiv a$ modulo m voor elke a in $\mathbb{Z}$ indien e positief geheel is met $e \equiv 1$ modulo $\phi(m)$;
- ☐ $a^m = a + m$ voor elke a in $\mathbb{Z}$.

6.3 Zij R een unitaire ring met eenheidselement (identiteit) 1. De verzameling van eenheden van R , R^* , is:

- ☐ $\{1\}$;
- ☐ $\{a \text{ in } R \text{ waarvoor een } b \text{ in } R \text{ bestaat zodanig dat } ab = ba = 1\}$;
- ☐ $R \setminus \{0\}$ waar 0 het neutrale element (nul) voor de optelling is;
- ☐ niet gedefinieerd omdat voor de definitie van R^* de ring commutatief moet zijn.

6.4 Zij $F = \mathbb{Z}/5\mathbb{Z}$ en $V = F^3$ als F -vectorruimte. In een lineaire deelruimte W van V

- ☐ zijn $3 + 5 = 15$ elementen;
- ☐ zijn $3 \cdot 5 = 15$ elementen;
- ☐ zijn 1, 5, 5^2 of 5^3 elementen;
- ☐ zijn 1, 3, 3^2 , 3^3 , 3^4 of 3^5 elementen.

6.5 Zij K het lichaam $\mathbb{Z}/3\mathbb{Z}$. In $K[x]$ is $f(x) = x^3 + \bar{2}x + \bar{1}$ irreducibel omdat

- ☐ $f(\bar{a}) = \bar{1}$ voor elke $\bar{a}$ in $\mathbb{Z}/3\mathbb{Z}$;
- ☐ $f(x)$ graad 3 heeft;
- ☐ $f(x)$ geen nulpunt heeft in $\mathbb{Z}/3\mathbb{Z}$;
- ☐ $f(x)$ geen nulpunt heeft in $\mathbb{Z}/3\mathbb{Z}$ en $f(x)$ graad 3 heeft.

Naam:

Normering:

1a	4	2a	4	3a	5	4a	7	5a	4	6.1	3
1b	4	2b	4	3b	5	4b	7	5b	3	6.2	3
1c	6	2c	6	3c	6	4c	4	5c	6	6.3	3
										6.4	3
										6.5	3
14		14		16		18		13		15	

Maximum totaal = 90

Cijfer = 1 + Totaal/10