

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) Wat betekent $a \equiv b$ modulo m voor gehele getallen a, b, m met $m \geq 2$?
 - (ii) Wat is de grootste gemene deler van twee gehele getallen x en y , beide ongelijk nul?
- (b) Bereken $d = \text{ggd}(345, 245)$ met behulp van het Euclidisch algoritme en druk d in 345 en 245 uit (als in de formule van Bezout).
- (c) Los op met x en y in $\mathbb{Z}/19\mathbb{Z}$:

$$\begin{cases} \bar{2}x + \bar{4}y = \bar{3} \\ \bar{3}x + \bar{7}y = \bar{5} \end{cases}$$

2. GROEPEN

- (a) Algemene kennis.
 - (i) Wanneer heet een niet-lege deelverzameling H van een groep G een ondergroep?
 - (ii) Formuleer de stelling van Lagrange voor een ondergroep H van een eindige groep G .
- (b) Bereken 3^{2011} modulo 200 als standaardrepresentant $(0, 1, 2, \dots, 199)$ op een economische manier.
- (c) Gebruik de methode van de Chinese reststelling om alle gehele getallen x te vinden die voldoen aan $x \equiv 1$ modulo 5, $x \equiv 2$ modulo 6 en $x \equiv 4$ modulo 7.

3. RINGEN

- (a) Algemene kennis.
 - (i) Welke extra eigenschap heeft een integriteitsgebied (ITG) ten opzichte van een commutatieve unitaire ring (CUR)?
 - (ii) Wanneer is een afbeelding $f: R \rightarrow S$ tussen twee unitaire ringen een homomorfisme van ringen?
- (b) Gegeven zijn $p = 5$ en $q = 31$. Als $e = 113$, vind dan een geschikte d als in het RSA-lemma, en ontcijfer $b = 2$ hiermee als $0, 1, 2, \dots, 164$.
- (c) Laat $F = \mathbb{Z}/2\mathbb{Z}$.
 - (i) Bepaal alle *monische* irreducibele polynomen van graad 2 en 3 in $F[x]$.
 - (ii) Ontbind de veelterm $x^4 + x^3 + x^2 + \bar{1}$ in irreducibele factoren in $F[x]$.

4. VECTORRUIMTEN

(a) Algemene kennis.

Zij V een vectorruimte over een lichaam F .

(i) Wanneer heet een deelverzameling $\{v_1, \dots, v_n\}$ van V een *basis* van V ?

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

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

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

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

(c) Zij $F = \mathbb{Z}/7\mathbb{Z}$, $v = (\overline{1}, \overline{3})$ en $w = (\overline{4}, \overline{5})$. Is $\{v, w\}$ een basis is van F^2 ?

(d) Zij M de 2 bij 4 matrix met coëfficiënten in $\mathbb{Z}/3\mathbb{Z}$ gegeven door

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

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 karakteristiek van een lichaam K .

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

In (b) en (c) nemen we $K = \mathbb{Z}/2\mathbb{Z}$, $f(x) = x^3 + x^2 + \overline{1}$ in $K[x]$ en $F = K[x]/(f(x))$. Gegeven is dat F een lichaam is.

(b) Hoeveel elementen heeft F ?

(c) Zij $\alpha = \overline{x}$ in F . Maak een tabel om in te zien dat α een primitief element is van F .

Gebruik deze tabel om $\alpha^3 + \alpha^5$ rechtstreeks uit te drukken als macht van α .

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 Voor $m \geq 2$ zegt de *stelling van Euler* dat

- ☐ $a^m \equiv a$ modulo m voor elk geheel getal a ;
- ☐ $a^{m-1} \equiv 1$ modulo m voor elk geheel getal a dat relatief priem is met m ;
- ☐ $a^{\phi(m)} \equiv a$ modulo m voor elk geheel getal a ;
- ☐ $a^{\phi(m)} \equiv 1$ modulo m voor elk geheel getal a dat relatief priem is met m .

6.2 De orde van een element g in een groep G met neutraal element e is

- ☐ het kleinste positieve getal n met $g^n = e$, en oneindig als zo'n n niet bestaat;
- ☐ alleen gedefinieerd voor G eindig, en is dan het kleinste positieve getal n met $g^n = e$;
- ☐ een andere naam voor de *inverse* van g in G ;
- ☐ 1 als $gh = hg$ voor alle h in G , en oneindig als dit niet geldt.

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 8 elementen en $V = F^3$ als F -vectorruimte. Een lineaire deelruimte W van V

- ☐ heeft 1, 2, 4 of 8 elementen;
- ☐ heeft 1, 8, 8^2 of 8^3 elementen;
- ☐ moet $\{(0, 0, 0)\}$ of V zijn;
- ☐ heeft 1, $3, 3^2, 3^3, \dots, 3^7$ of 3^8 elementen.

6.5 Zij K een lichaam en $f(x)$ in $K[x]$. Dan is $K[x]/(f(x))$ een lichaam als

- ☐ $f(x)$ irreducibel is in $K[x]$;
- ☐ $f(x)$ graad tenminste 1 heeft;
- ☐ $f(x)$ graad tenminste 2 heeft maar geen nulpunt heeft in K ;
- ☐ $f(x)$ geen nulpunt heeft in K .

Normering:

1a	4	2a	4	3a	4	4a	4	5a	4	6.1	3
1b	4	2b	4	3b	5	4b	4	5b	3	6.2	3
1c	6	2c	6	3c	8	4c	4	5c	7	6.3	3
						4d	4			6.4	3
										6.5	3
14		14		17		16		14		15	

Maximum totaal = 90

Cijfer = 1 + Totaal/10