

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) Geef de definitie van een *priemrestklasse* modulo m , met $m \geq 2$.
- (ii) Wanneer heeft een restklasse modulo m met $m \geq 2$ een *multiplicatieve inverse* en hoe bepaal je deze?

(b) Bereken $d = \text{ggd}(361, 681)$ met behulp van het Euclidisch algoritme en druk d in 361 en 681 uit (als in de formule van Bezout).

(c) Los op met x en y in $\mathbb{Z}/29\mathbb{Z}$:

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

2. GROEPEN

(a) Algemene kennis.

- (i) Definieer de *orde* van een element g in een groep G .
- (ii) Definieer de *Euler functie* $\phi(m)$ voor een geheel getal $m \geq 2$.

(b) Bereken 33^{2010} modulo 52 als standaardrepresentant $(0, 1, 2, \dots, 51)$ 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 4, $x \equiv 3$ modulo 5 en $x \equiv 5$ modulo 7.

3. RINGEN

(a) Algemene kennis.

- (i) Geef de definitie van een *eenheid* in een (unitaire) ring R .
- (ii) Wanneer is een verzameling S een *deelring* van een (unitaire) ring R ?

(b) Gegeven zijn $p = 7$ en $q = 13$. Als $e = 29$, vind dan een geschikte d als in het RSA-lemma, en ontcijfer $b = 3$ hiermee als $0, 1, 2, \dots, 90$.

(c) Laat $F = \mathbb{Z}/3\mathbb{Z}$.

- (i) Bepaal alle *monische* irreducibele polynomen van graad 2 in $F[x]$.
- (ii) Ontbind de veelterm $X^8 - \bar{1}$ in irreducibele factoren.

4. VECTORRUIMTEN

(a) Algemene kennis.

- (i) Wanneer heten $v_1, \dots, v_n$ in een vectorruimte V over een lichaam F *lineair onafhankelijk*, en wanneer *voortbrengend*?
- (ii) Als V en W vectorruimten zijn over een lichaam F , wanneer is een functie $f : V \rightarrow W$ *lineair*?

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

$$A = \begin{pmatrix} \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{2} & \overline{0} \end{pmatrix} \text{ en } B = \begin{pmatrix} \overline{4} & \overline{1} \\ \overline{0} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}$$

met coëfficiënten in $\mathbb{Z}/5\mathbb{Z}$.

(c) Zij $F = \mathbb{Z}/7\mathbb{Z}$, $v = (\overline{1}, \overline{2})$ en $w = (\overline{2}, \overline{1})$. Laat zien dat $\{v, w\}$ een basis is van F^2 .

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

$$M = \begin{pmatrix} \overline{4} & \overline{1} & \overline{0} & \overline{3} & \overline{0} \\ \overline{5} & \overline{2} & \overline{2} & \overline{2} & \overline{1} \end{pmatrix}.$$

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

5. EINDIGE LICHAMEN

(a) Algemene kennis.

- (i) Definieer een *primitief element* van een eindig lichaam K .
- (ii) Voor welke eindige lichamen bestaat zo'n primitief element?

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

(b) Gegeven is dat $F = K[x]/(f(x))$ een lichaam is. 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 $\alpha^3 + \alpha^7$ 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 Als $n = p_1 p_2 \cdots p_m$ ($m \geq 1$) voor verschillende priemgetallen p_i dan geldt, met ϕ de Euler functie:

- ☐ $\phi(n) = 1$;
- ☐ $\phi(n) = n - 1$;
- ☐ $\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_m - 1)$;
- ☐ geen van de eerste drie keuzes.

6.2 Een groep G heet *cyclisch* als

- ☐ G maar één element heeft;
- ☐ G eindig veel elementen heeft;
- ☐ er een g in G bestaat met $G = \{g^m \text{ met } m \text{ in } \mathbb{Z}\}$;
- ☐ voor elke g in G geldt dat $G = \{g^m \text{ met } m \text{ in } \mathbb{Z}\}$.

6.3 Een *nuldeler* van een commutatieve ring R is

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

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

- ☐ zijn 3^3 elementen;
- ☐ zijn $3 + 3 = 6$ elementen;
- ☐ zijn $3 \cdot 3 = 9$ elementen;
- ☐ zijn 1, 3, 3^2 of 3^3 elementen.

6.5 Zij $R = \mathbb{Q}[x]/(x^2 - 2)$. In R is het product $\overline{x-1} \cdot \overline{x+1}$

- ☐ gelijk aan $\overline{0}$;
- ☐ gelijk aan $\overline{1}$;
- ☐ gelijk aan $\overline{-1}$;
- ☐ gelijk aan $\overline{2x}$.

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