

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.
Dit betekent dat er een k in $\mathbb{Z}$ bestaat zodanig dat $b = ka$.
- (ii) Formuleer de stelling over deling met rest voor gehele getallen a en b met $b \neq 0$.
Er bestaan unieke q en r in $\mathbb{Z}$ zodanig dat $a = qb + r$ en $0 \leq r < |b|$.

(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 $x = \overline{23}$.

De multiplicatieve inverse voor $\overline{a}$ in $\mathbb{Z}/m\mathbb{Z}$ (met $m \geq 2$) bestaat precies dan als $\text{ggd}(a, m) = 1$. Hier bestaat die inverse van $\overline{22}$ niet omdat $\text{ggd}(22, 56) = 2$. Die van $\overline{23}$ bestaat wel en kunnen we vinden met het uitgebreide algoritme van Euclides:

i	a_i	x_i	y_i	q	berekening
0	56	1	0	-	-
1	23	0	1	2	$56 = 2 \times 23 + 10$
2	10	1	-2	2	$23 = 2 \times 10 + 3$
3	3	-2	5	3	$10 = 3 \times 3 + 1$
4	1	7	-17	3	$3 = 3 \times 1 + 0$

Dus $1 = 7 \times 56 + (-17) \times 23$ en $\overline{-17} \overline{23} = \overline{1}$ in $\mathbb{Z}/56\mathbb{Z}$. De inverse is dus $\overline{-17} = \overline{39}$.

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

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

16 maal de eerste vergelijking bij de tweede optellen geeft het equivalente stelsel

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

Voor x moeten we dus de multiplicatieve inverse van $\overline{13}$ in $\mathbb{Z}/29\mathbb{Z}$ nemen, en dat is $\overline{9}$ (met behulp van het uitgebreide algoritme van Euclides, of door in te zien dat $\overline{2} \overline{13} = \overline{-3}$ en $\overline{-10} \overline{-3} = \overline{1}$ dus $(\overline{-10} \overline{2}) \overline{13} = \overline{1}$, en de inverse is $\overline{-10} \overline{2} = \overline{9}$). Dan is $y = -\overline{4}x = -\overline{4} \overline{9} = \overline{-36} = \overline{22}$.

Een andere mogelijkheid is om te zien dat we hier $M \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \overline{0} \\ \overline{1} \end{pmatrix}$ hebben met $M = \begin{pmatrix} \overline{4} & \overline{1} \\ \overline{7} & \overline{13} \end{pmatrix}$. M heeft determinant $\overline{4} \overline{13} - \overline{7} \overline{1} = \overline{16}$ met inverse $\overline{20}$, dus M heeft inverse $N = \overline{20} \begin{pmatrix} \overline{13} & -\overline{1} \\ -\overline{7} & \overline{4} \end{pmatrix} = \begin{pmatrix} \overline{28} & \overline{9} \\ \overline{5} & \overline{22} \end{pmatrix}$ en de oplossing is $\begin{pmatrix} x \\ y \end{pmatrix} = N \begin{pmatrix} \overline{0} \\ \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{9} \\ \overline{22} \end{pmatrix}$.

2. GROEPEN

(a) Algemene kennis.

- (i) Definieer wanneer een groep *cyclisch* genoemd wordt.
Wanneer er een voortbrenger g is van de groep, dus elk element is te schrijven als g^k met k in $\mathbb{Z}$.

- (ii) Gegeven is dat een groep G 10 elementen heeft. Welke mogelijkheden laat dit open voor de orde van een element in G ?

We weten dat in een eindige groep de orde van een element de orde van de groep deelt. De mogelijke ordes zijn dus de (positieve) delers van 10: 1, 2, 5 en 10.

- (b) Bereken 11^{123} modulo 41 (als $0, 1, 2, \dots, 40$) op een economische manier.

41 is een priemgetal dus $\phi(41) = 40$ en $a^{40} \equiv 1$ als $\text{ggd}(a, 41) = 1$ (dat wil zeggen omdat 41 priem is: 41 deelt a niet). Hier geeft dit $11^{123} \equiv 11^3 \equiv 121 \times 11 \equiv (-2) \times 11 \equiv 19$ modulo 41.

- (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.

Hier hebben we $m_1 = 5$, $M_1 = 42$, $m_2 = 6$, $M_2 = 35$, $m_3 = 7$ en $M_3 = 30$. We kunnen schrijven $1 = 17 \times 5 + (-2) \times 42 = 6 \times 6 + (-1) \times 35 = 13 \times 7 + (-3) \times 30$ (de tweede is makkelijk te zien, de eerste en derde volgen heel snel met het uitgebreide algoritme van Euclides). De oplossingsverzameling is dus de klasse modulo $5 \times 6 \times 7 = 210$ van $2 \times (-2) \times 42 + 3 \times (-1) \times 35 + 0 \times (-3) \times 30 = -168 - 105 = -273$, en dat is ook de klasse van 147 of -63 .

3. RINGEN

- (a) Algemene kennis.

- (i) Gegeven een ring R met een deelverzameling I , definieer (in formules) dat I een ideaal van R is.

(a) I moet niet leeg zijn. (b) Als x en y in I zijn dan moet $a - b$ ook in I zijn. (c) Als x in I is en r in R dan zijn rx en xr in I .

(a) en (b) kun je ook vervangen door (a'): I is een deelgroep van R voor de optelling.

- (ii) Geef de formule van Bezout voor twee polynomen $f(x)$ en $g(x)$ (ongelijk nul) in $K[x]$ als K een lichaam is.

Er bestaan $A(x)$ en $B(x)$ in $K[x]$ met $\text{ggd}(f(x), g(x)) = A(x)f(x) + B(x)g(x)$.

- (b) Gegeven is het lichaam $K = \mathbb{Z}/5\mathbb{Z}$ en het polynoom $f(x) = x^4 + x + \bar{2}$ in $K[x]$. Is $K[x]/(f(x))$ een lichaam? Beargumenteer je antwoord.

We weten dat $K[x]/(f(x))$ een lichaam is dan en slechts dan als $f(x)$ irreducibel is in $K[x]$. Maar $f(x)$ heeft graad $4 > 1$ en een nulpunt $\bar{2}$, dus is niet irreducibel, en $K[x]/(f(x))$ is geen lichaam. (Het is zelfs geen integriteitsgebied.)

- (c) Als $F = \mathbb{Z}/2\mathbb{Z}$, vind de grootste gemene deler van $f(x) = x^4 + \bar{1}$ en $g(x) = x^2 + x$ in $F[x]$ met behulp van het algoritme van Euclides.

Herhaaldelijke deling met rest geeft:

$$\begin{aligned} x^4 + \bar{1} &= (x^2 + x + \bar{1})(x^2 + x) + (x + \bar{1}) \\ x^2 + x &= x(x + \bar{1}) + \bar{0} \end{aligned}$$

dus de grootste gemene deler is $x + \bar{1}$ (die al monisch is).

4. VECTORRUIMTEN

- (a) Algemene kennis.

- (i) Gegeven een vectorruimte V over een lichaam F , wanneer is een deelverzameling W van V een lineaire deelruimte?

- (a) Als w_1 en w_2 in W zijn dan is $w_1 + w_2$ in W . (b) Als λ in F is en W in W , dan is λw in W . W moet ook niet leeg zijn maar dat ontbreekt helaas in het dictaat.
- (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 . w is te schrijven in de vorm $\lambda_1 v_1 + \dots + \lambda_n v_n$ voor unieke $\lambda_1, \dots, \lambda_n$ in F , en $\lambda_1, \dots, \lambda_n$ zijn de gevraagde coördinaten.
- (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.

AB bestaat niet omdat het aantal kolommen van A niet gelijk is aan het aantal rijen van B is. Voor BA zijn deze afmetingen wel gelijk en vinden we

$$BA = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{2} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} \times \bar{2} + \bar{1} \times \bar{0} & \bar{1} \times \bar{2} + \bar{1} \times \bar{1} & \bar{1} \times \bar{1} + \bar{1} \times \bar{2} \\ \bar{0} \times \bar{2} + \bar{1} \times \bar{0} & \bar{0} \times \bar{2} + \bar{1} \times \bar{1} & \bar{0} \times \bar{1} + \bar{1} \times \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{2} \end{pmatrix}$$

(b) Laat zien dat de vectoren $u = \begin{pmatrix} \bar{2} \\ \bar{3} \end{pmatrix}$ en $v = \begin{pmatrix} \bar{1} \\ \bar{4} \end{pmatrix}$ 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 $K = \mathbb{Z}/5\mathbb{Z}$.

We moeten zien dat elke vector $\begin{pmatrix} x \\ y \end{pmatrix}$ in K^2 te schrijven is als $\lambda u + \mu v$ voor unieke λ en μ in K . Dat geeft het stelsel

$$\begin{cases} \bar{2}\lambda + \mu = x \\ \bar{3}\lambda + \bar{4}\mu = y \end{cases} \iff \begin{cases} \bar{2}\lambda + \mu = x \\ \bar{6}\mu = \bar{2}x + y \end{cases} \iff \begin{cases} \lambda + \bar{4}\mu = \bar{4}x \\ \mu = \bar{5}x + \bar{6}y \end{cases} \iff \begin{cases} \lambda = \bar{4}x - \bar{4}\mu = \bar{5}x + \bar{4}y \\ \mu = \bar{5}x + \bar{6}y \end{cases}$$

dus voor gegeven x en y bestaan unieke λ en μ , zoals we wilden.

Als $K = \mathbb{Z}/5\mathbb{Z}$ dan geldt $u + \bar{3}v = \begin{pmatrix} \bar{0} \\ \bar{0} \end{pmatrix}$ dus u en v zijn niet eens lineair onafhankelijk.

(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).)

We weten van (b) dat de eerste twee kolommen een basis vormen van K^2 dus de kolomruimte van M moet K^2 zijn en heeft dimensie 2. Omdat het domein van M K^5 is, met dimensie 5, moet de dimensie van de nulruimte $5 - 2 = 3$ zijn.

5. EINDIGE LICHAMEN

(a) Algemene kennis.

(i) Definieer de karakteristiek van een lichaam K .

Dit is de orde van de identiteit (neutrale element voor de vermenigvuldiging) met betrekking tot de optelling als die orde eindig is, anders is de karakteristiek 0. Met andere woorden, het is de kleinste k in $\mathbb{N}$ zodanig dat $k \cdot 1 = 0$ als zo'n k bestaat, anders is de karakteristiek 0.

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

Alle getallen van de vorm p^k met p een priemgetal en k een positief geheel getal.

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 ?

$3^2 = 9$ omdat F als elementen de klassen $\overline{ax+b}$ met a en b in K heeft en dit alle elementen van F precies één keer geeft. (Merk op dat dit alleen van de graad van $f(x)$ afhangt en niet van het feit dat $f(x)$ irreducibel is in $K[x]$.)

(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 .

Merk op dat $\overline{x^2} = -\overline{2x+2} = \overline{x+1}$ waarbij we in K gewoon a schrijven in plaats van $\bar{a}$. Als we dat in de tabel ook doen dan vinden we

α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7
$\overline{1}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{2}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{x+2}$

Dan is dus $\alpha^4 + \alpha^6 = \overline{2} + \overline{2x+2} = \overline{2+2x+2} = \overline{2x+1} = \alpha^3$.

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 $\text{ggd}(a, m) = 1$;

De eerste keuze werkt wel als m een priemgetal is maar niet voor bijvoorbeeld $m = 4$ (je krijgt ook $\bar{2}$). De tweede keuze gaat ook mis voor $m = 4$ en $a = 2$. De derde keuze gaat altijd mis omdat je $\overline{m} = \bar{0}$ krijgt. De vierde keuze is een van de karakterizeringen van $(\mathbb{Z}/m\mathbb{Z})^*$.

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 $\mathbb{Z}$.

De derde keuze is precies wat het RSA lemma zegt. De overige keuzes zijn vrij duidelijk fout. De eerste twee gelden al niet als $k=1$ (dus m is priem) omdat dan $\phi(m) = m-1$ en $a^{m-1} \equiv 1$ modulo m als $\text{ggd}(m, a) = 1$ volgens de stelling van Euler, en dit is niet congruent a modulo m voor $a=2$. De laatste keuze kan duidelijk niet voor $a > 0$ en voldoende groot omdat $m \geq 2$, of voor $a=0$.

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.

Dit is de definitie. De eerste keuze is fout voor bijvoorbeeld $R = \mathbb{Q}$, waar $R^* = \mathbb{Q} \setminus \{0\}$, de derde voor bijvoorbeeld $R = \mathbb{Z}$ (met $\mathbb{Z}^* = \{1, -1\}$) of $R = \mathbb{Z}/4\mathbb{Z}$ (met $(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\}$). De laatste mogelijkheid is gewoon onzin, R^* is ook gedefinieerd voor een niet-commutatieve ring met identiteit.

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.

F^3 heeft dimensie 3 en dus moet de lineaire deelruimte W dimensie 0, 1, 2 of 3 hebben. Omdat een vectorruimte van dimensie k over een eindig lichaam met q elementen q^k elementen bevat is hier (waar $q=5$) de derde keuze de juiste.

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.

De eerste keuze is wel waar maar dit geldt dan ook voor $f(x)^2$, die duidelijk reducibel is. De tweede keuze voldoet niet, want x^3 heeft graad drie maar is reducibel. De derde keuze voldoet ook niet want $f(x)^2$ voldoet hier ook aan en is reducibel. De vierde keuze is de juiste: voor een polynoom van graad 2 of 3 met coëfficiënten in een lichaam is het niet hebben van een nulpunt in dat lichaam equivalent met irreducibiliteit.

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