

Opgelet

- (1) Dit tentamen bestaat uit vijf vraagstukken (inclusief meerkeuzegedeelte).
 - (2) Zakrekenmachines, etc., mogen niet gebruikt worden.
 - (3) Goede toelichting scoort!
 - (4) Op de achterkant van deze bladzijde staat een apart gedeelte met meerkeuzevragen.
- Schrijf je naam daar** en lever dit blad mee in met je oplossingen van de overige opgaven.
- (5) Het tentamen en een uitwerking verschijnen later vandaag op blackboard.

1. DE FORMULE VAN BEZOUT EN VERWANTE RESULTATEN

- (a) Algemene kennis.
 - (i) Formuleer de hoofdstelling van de rekenkunde voor een geheel getal $n \geq 2$.
 - (ii) Geef de “formule van Bezout” voor gehele getallen a en b , beide ongelijk nul.
- (b) Vind met het uitgebreide algoritme van Euclides $\text{ggd}(85, 221)$ en gehele getallen x en y met $x \cdot 85 + y \cdot 221 = \text{ggd}(85, 221)$.
- (c) Gegeven is de modulus $m := 20$. Bepaal methodisch de inverse van de matrix

$$M := \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{5} & \bar{1} \end{pmatrix}$$

of leg uit waarom die inverse niet bestaat.

2. REKENEN MODULO $m \geq 2$

- (a) Algemene kennis.
 - (i) Geef de formule voor $\phi(n)$ als $n \geq 2$, in termen van de priemfactorisatie van n .
 - (ii) Formuleer het RSA lemma voor verschillende priemgetallen $p_1, \dots, p_k$.
- (b) Los op met x en y in $\mathbb{Z}/8\mathbb{Z}$:

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

- (c) Gebruik de methode van de Chinese reststelling om het kleinste positieve gehele getal x te vinden zodanig dat $x \equiv 4$ modulo 5, $x \equiv 1$ modulo 6 en $x \equiv 3$ modulo 7.

3. PROJECT GEHELE GETALLEN

- (a) Formuleer het resultaat over deling met rest voor a en b in $\mathbb{Z}$ met $b \neq 0$.

Achteraan dit tentamen is een lijst opgenomen van axioma's van $\mathbb{Z}$ voor de optelling en vermenigvuldiging, alsmede een aantal gevolgen hiervan. In de onderdelen (b) en (c) van deze opgave wordt gevraagd om enkele van deze gevolgen aan te tonen.

Spelregel: bij het bewijzen van een formule mag je uitsluitend wetten gebruiken die vóór de gevraagde formule staan in de lijst.

- (b) Laat zien dat $x = y \Leftrightarrow 0 = y + (-x)$ (je moet dus beide richtingen bewijzen). Geef bij iedere stap aan welk axioma of afgeleide wet wordt gebruikt en geef bij tenminste één stap aan hoe de gelijkheidsregel wordt gehanteerd.
- (c) Toon aan dat $x \cdot 0 = 0$. Geef bij iedere stap aan welk axioma of afgeleide wet wordt gebruikt (de gelijkheidsregel hoeft je hier niet te noemen).

4. DIVERSEN

- (a) Schrijf het decimale getal 4321 in het zeventallig stelsel.
 (b) Wat zijn de laatste twee cijfers in het tientallig stelsel van 11^{2008} ?
 (c) Schrijf $(123)(13)(24)(132)$ in S_4 als een product van onderling disjuncte cycli.
 (d) Op $\mathbb{R}$ is de relatie R gegeven via aRb dan en slechts dan als q in $\mathbb{Q}$ bestaat met $a = qb$.
 Is R een equivalentierelatie?

5. 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.

5.1 Gegeven zijn een injectieve functie $f : \mathbb{N} \rightarrow \mathbb{N}$ en een surjectieve functie $g : \mathbb{N} \rightarrow \mathbb{N}$. Dan

- ☐ is $f \circ g$ injectief;
☐ is $g \circ f$ surjectief;
☐ is $f \circ g$ injectief en $g \circ f$ surjectief;
☐ geldt in het algemeen geen van de drie alternatieven hierboven.

5.2 Voor $n \geq 2$ is $(\mathbb{Z}/n\mathbb{Z})^*$, de verzameling priemrestklassen modulo n , gelijk aan

- ☐ $\{1, \dots, n-1\}$;
☐ $\{\bar{a} \text{ voor die } a \text{ in } \mathbb{Z} \text{ waarvoor } \text{ggd}(a, n) = 1\}$;
☐ $\{\bar{a} \text{ voor die } a \text{ in } \{1, \dots, n\} \text{ die een priemgetal zijn}\}$;
☐ $\{\bar{a} \text{ voor die } a \text{ in } \{1, \dots, n\} \text{ die géén priemgetal zijn}\}$.

5.3 In de groep S_5 heeft $\sigma = (1234)$ orde 4 omdat

- ☐ $\sigma(4) \neq 4$;
☐ $\sigma^4 = e$, het neutrale element van S_5 ;
☐ $\sigma(i) \neq i$ voor $i = 1, 2, 3$ en 4 , maar $\sigma(5) = 5$;
☐ $\sigma^4 = e$ en $\sigma^2 \neq e$, waar e het neutrale element van S_5 is.

5.4 Op $\mathbb{N} = \{1, 2, 3, \dots\}$ is de relatie R gegeven via aRb dan en slechts dan als $a|b$. Dan is R

- ☐ een partiële ordening;
☐ een equivalentierelatie;
☐ zowel een partiële ordening als een equivalentierelatie;
☐ geen partiële ordening omdat $2R3$ en $3R2$ allebei niet gelden.

5.5 Gegeven is de verzameling G van positieve reële getallen. Dan is G

- ☐ een groep onder vermenigvuldiging;
☐ geen groep onder vermenigvuldiging omdat 0 niet in G is;
☐ geen groep onder vermenigvuldiging omdat als x in G is $-x$ niet in G is;
☐ geen groep onder vermenigvuldiging omdat die vermenigvuldiging niet commutatief is.

Naam:

Normering:

1a	4	2a	4	3a	4	4a	4	5.1	4
1b	6	2b	6	3b	7	4b	6	5.2	4
1c	6	2c	6	3c	7	4c	4	5.3	4
						4d	6	5.4	4
								5.5	4
16		16		18		20		20	

Maximum totaal = 90

Cijfer = 1 + Totaal/10