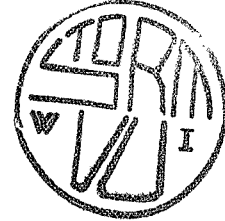


Opgelet: er is een apart multiple-choice gedeelte op de laatste bladzijde. Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!



1. De formule van Bezout en inversen

- (a) Algemene kennis
- (i) Formuleer de *stelling van Bezout* over de ggd van twee gehele getallen.
 - (ii) Leg bondig het *algoritme* uit, waarmee de onbekenden in de formule van Bezout worden berekend.
 - (iii) Gegeven een modulus $m \geq 2$ en een getal a , leg uit hoe je met Bezout aan de *inverse* komt van a modulo m , of kunt zien dat er geen inverse is.
- (b) Bepaal de inverse van 119 modulo 161 of leg uit waarom die inverse niet bestaat. Geef voldoende toelichting bij je antwoord.
- (c) Bereken (met toelichting) de inverse van de volgende matrix M , of leg uit waarom M geen inverse matrix heeft. De modulus is $m := 15$.

$$M := \begin{pmatrix} \bar{7} & \bar{6} \\ \bar{5} & \bar{4} \end{pmatrix}$$

2. Project Gehele Getallen.

- (a) Algemene kennis.
- (i) Wat bedoelt men met: een verzameling $V \subseteq \mathbb{Z}$ is *naar onder begrensd*?
 - (ii) Wat zegt het *ordeningsprincipe* over de verzameling $\mathbb{Z}$?
- Achteraan dit tentamen is een lijst opgenomen van axioma's en hun gevolgen in $\mathbb{Z}$.
- Spelregel.** In het bewijs van een formule mag je uitsluitend wetten gebruiken die één of meer regels vóór de te bewijzen formule worden genoemd.
- (b) Bewijs naar keuze één van de "schrappetten" voor optelling. Geef daarbij aan welke van de axioma's gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.
- (c) Leid af uit (b) dat bij iedere $z \in \mathbb{Z}$ een unieke tegengestelde bestaat (" $-z$ " genoteerd).
- (d) Toon aan dat $-(x+y) = (-x) + (-y)$. Geef daarbij aan welke van de axioma's gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.

3. Rekenen modulo $m \geq 2$

- (a) Algemene kennis.
- (i) Wat bedoelt men met de *reductie van een getal modulo m* ?
 - (ii) *Reduceer* de volgende uitdrukking modulo 34:
 $938 + 15 \cdot 103 \pmod{34}$.
De uitkomst moet een standaard represant zijn.
 - (iii) Zij $m \geq 2$ een gehele modulus. Leg bondig uit hoe een stelsel vergelijkingen

$$a_{11}x + a_{12}y = c_1$$

$$a_{21}x + a_{22}y = c_2$$

modulo m wordt opgelost met de *matrixmethode* ($a_{ij}, c_1, c_2 \in \mathbb{Z}$). Wanneer werkt de methode niet?

- (b) Los het volgende stelsel vergelijkingen op. $\bar{6}x + y = \bar{1}$ en $\bar{2}x + \bar{2}y = \bar{6}$ (modulus 8).
 (c) Gegeven is dat $\text{ggd}(a, m) = d$. In dit onderdeel bekijken we de volgende congruëntievergelijking in de onbekende $x \in \mathbb{Z}$:

$$a \cdot x \equiv b \pmod{m}.$$

Toon aan dat de vergelijking een oplossing heeft als $d \mid b$.

4. Diversen.

(a) Algemene kennis.

- (i) Wat is een *priemrestklasse* modulo m ?
 (ii) Wat is het verband tussen de uitdrukking $\phi(m)$ (met de *Euler functie* ϕ) enerzijds, en het aantal elementen van $\mathbb{Z}_m^*$ anderzijds?
 (iii) Zij G een groep en $g \in G$. Wat bedoelt men met: g is een *generator* van de groep G ?
 (b) Geef (zonder bewijs) de formules voor $\phi(p^e)$ en $\phi(p \cdot q)$ ($p \neq q$ priem, $e > 0$ geheel). Bereken hiermee $\phi(13^2)$ en $\phi(13 \cdot 17)$.
 (c) Bepaal, met de nodige toelichting, de orde van het element $\bar{16}$ in de groep $\mathbb{Z}_{21}^*$. Is $\bar{16}$ een generator van $\mathbb{Z}_{21}^*$?

Normering:

1a	4	2a	4	3a	4	4a	4	5	20
1b	6	2b	6	3b	6	4b	6		
1c	6	2c	6	3c	6	4c	6		
		2d	6						
	16		22		16		16		20

Cijfer = Totaal/10 + 1

Multiple choice gedeelte: -4 ptn per foute keuze.

N.B.: Na afloop van het tentamen vind je een volledig uitgewerkte versie van het tentamen op blackboard (Knop "Course materials", folder #10). De attachment bestaat in postscript en in pdf.

☞ Je hebt voor dit tentamen twee uur tijd.

5. Multiple-choice gedeelte

- Bij iedere vraag is precies één van de onderdelen juist én (meest) volledig.
- Het antwoord (aangekruist of zwartgemaakt bolletje) hoeft niet te worden toegelicht.

5.1. De Zeef van Eratosthenes is een algoritme om

- o alle positieve getallen $< m$ te vinden die relatief priem zijn met m (waar $m \geq 2$).
- o alle positieve delers van een getal m te vinden.
- o alle priemgetallen $< m$ te vinden.
- o de grootste gemene deler van twee getallen $a, b \neq 0$ te vinden.

5.2. Gegeven zijn twee vergelijkingen $x \equiv a_1 \pmod{m_1}$ en $x \equiv a_2 \pmod{m_2}$ met gehele getallen a_1, a_2 en moduli $m_1, m_2 \geq 2$. De Chinese reststelling zegt dan dat

- o er een unieke oplossing bestaat als $\text{ggd}(m_1, m_2) = 1$.
- o er een oplossing bestaat als $\text{ggd}(a_1, a_2) = 1$ en elke twee oplossingen zijn dan congruent modulo $\text{kgv}(m_1, m_2)$.
- o de oplossingsverzameling precies een congruentieklasse is modulo $m_1 \cdot m_2$ indien $\text{ggd}(m_1, m_2) = 1$.
- o het stelsel oplosbaar is enkel en alleen als de determinant niet nul is.

5.3. Het RSA Lemma (dat aan de basis ligt van de gelijknamige cryptografische methode) stelt dat

- o voor een modulus m en een geheel getal a geldt: $a^e \equiv 1 \pmod{m}$ indien $e \equiv 1 \pmod{\phi(m)}$.
- o voor een modulus m en een geheel getal a met $\text{ggd}(a, m) = 1$ geldt: $a^e \equiv 1 \pmod{m}$ indien $e \equiv 1 \pmod{\phi(m)}$.
- o voor een kwadraatvrije modulus m en een geheel getal a geldt: $a^{\phi(m)} \equiv 1 \pmod{m}$.
- o voor een kwadraatvrije modulus m en een geheel getal a geldt: $a^e \equiv a \pmod{m}$ indien $e \equiv 1 \pmod{\phi(m)}$.

5.4. De orde van een element g in een eindige groep G met neutraal element e is:

- o het kleinste getal $k > 0$ waarvoor $g^k = e$, indien zo'n getal bestaat.
- o het grootste getal $k > 0$ waarvoor $g^k \neq e$, indien zo'n getal bestaat.
- o het rangnummer van g in de opsomming van alle elementen uit G .
- o het aantal elementen in G met dezelfde inverse als g .

5.5. Zij G een eindige groep en $g \in G$. Er is een verband tussen de orde van g en de orde van G (aantal elementen), en wel het volgende.

- o De orde van g is ten hoogste de orde van G .
- o De orde van g is een deler van de orde van G .
- o De orde van g is gelijk aan de orde van G .
- o De orde van g is strict kleiner dan de orde van G , tenzij G triviaal is (orde 1).

Axioma's Gehele Getallen (zover nodig)

Gelijkheid

Gelijkheidswet: $x = x$.

Gelijkheidsregel: (Zelf formuleren)

Symmetrie van gelijkheid: $x = y \rightarrow y = x$.

Transitiviteit van gelijkheid: $x = y$ en $y = z \rightarrow x = z$.

Axioma's voor optelling

(A1) Optelling is associatief: $(x + y) + z = x + (y + z)$.

(A2) Neutraal element 0: $x + 0 = 0 + x = x$.

(A3) Tegengestelde: Bij iedere x bestaat een tegengesteld element x' zo dat $x + x' = x' + x = 0$.

(A4) Optelling is commutatief: $x + y = y + x$.

Schrapwetten voor optelling:

$x + y = x + z \rightarrow y = z$ (linker -).

$x + z = y + z \rightarrow x = y$ (rechter -).

Uniciteit van tegengestelde:

$x + y_1 = 0$ en $x + y_2 = 0 \rightarrow y_1 = y_2$.

$y_1 + x = 0$ en $y_2 + x = 0 \rightarrow y_1 = y_2$.

De unieke tegengestelde van een getal x noteert men als $-x$.

Additieve wetten voor tegengestelde:

$-(-x) = x$.

$-(x + y) = (-x) + (-y)$.

Termen overbrengen naar ander lid:

$x = y \leftrightarrow 0 = y + (-x)$.

$x + y = z \leftrightarrow x = z + (-y)$.

Axioma's voor vermenigvuldiging

(A6) Vermenigvuldiging is associatief: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(A7) Neutraal element 1: $x \cdot 1 = 1 \cdot x = x$.

(A8) Vermenigvuldiging is commutatief: $x \cdot y = y \cdot x$.

(A5) Distributieve wet: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

(A9) Wet van nuldelers: Als $x \cdot y = 0$ dan is $x = 0$ of $y = 0$.

Vermenigvuldigen met nul:

$x \cdot 0 = 0 = 0 \cdot x$.

Multipliatieve wetten voor tegengestelde:

$(-1) \cdot x = -x = x \cdot (-1)$.

$x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$.

$(-x) \cdot (-y) = x \cdot y$.

Schrapwetten voor vermenigvuldiging:

$x \cdot y = x \cdot z$ en $x \neq 0 \rightarrow y = z$.

$x \cdot z = y \cdot z$ en $z \neq 0 \rightarrow x = y$.

In plaats van $x + (-y)$ wordt ook $x - y$ geschreven.