



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! Tentamenduur: 2 uur.

1. Elementair modulorekenen en cryptografie

De onderdelen van deze opgave moeten worden opgelost met modulorekenen.

- (a) In het zeventallig stelsel is een getal deelbaar door 4 precies dan als de alternerende som van de cijfers deelbaar is door 4. (Bijvoorbeeld: $(4, 3, 6, 5)_7$ is niet deelbaar door 4 want $4 - 3 + 6 - 5 = 2$ is niet deelbaar door 4.)
- (b) Een vlo bevindt zich op de wijzerplaat van een klok en springt heen en weer over de minuten-streepjes of -getallen met sprongen van alleen maar 7 minuten. Als de vlo nu op XII zit, hoeveel sprongen moet ze dan minimaal maken om op I te komen?
- (c) Neem het volgende stelsel vergelijkingen met modulus 8:

$$x + \bar{2} \cdot y = \bar{2} \quad (\text{i})$$

$$\bar{3} \cdot x + \bar{4} \cdot y = \bar{0} \quad (\text{ii})$$

Los het stelsel op met de eliminatiemethode voor de aangegeven modulus. Let op: je moet alle oplossingen hebben.

2. De Euler functie, hoge exponenten, en RSA

- (a) Algemene kennis.
 - (i) Wat is de Euler functie $\phi(m)$?
 - (ii) Met welke formules kun je (in principe) de Euler functie $\phi(m)$ uitrekenen?
 - (iii) Bereken met de formules uit (ii): $\phi(300)$.
- (b) Formuleer:
 - (i) De Euler stelling aangaande $\phi(m)$.
 - (ii) Het RSA Lemma.
- (c) Los op met behulp van de Euler stelling: wat is de rest bij deling van 3^{119} door 22?
- (d) Neem als modulus 1147 en encryptiesleutel $e := 23$ voor een RSA code. Breek (met voldoende toelichting) de code.

3. Project Gehele Getallen

Voor deze opgave kan je de aparte pagina (na het multiple choice deel) gebruiken met axioma's over $\mathbb{Z}$ en gevolgtrekkingen hieruit.

Spelregel. In het bewijs van een formule mag je uitsluitend wetten gebruiken die één of meer regels vóór de te bewijzen formule worden genoemd.

- (a) Formuleer de gelijkheidsregel.
- (b) Toon aan dat $z \cdot 0 = 0$. Geef daarbij aan welke van de axioma's of afgeleide wetten gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.
- (c) Toon aan dat $x \cdot y = x \cdot z$ en $x \neq 0 \rightarrow y = z$ (schrappwet voor vermenigvuldiging). Geef daarbij aan welke van de axioma's of afgeleide wetten gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.

4. Cyclische groepen

- (a) Algemene kennis.
- (i) Wat bedoelt men met: de orde van een element in een groep? Geef de orde van $\bar{2}$ in de groep $\mathbb{Z}/3\mathbb{Z}$ (met optelling) en in de groep $(\mathbb{Z}/3\mathbb{Z})^*$ (met vermenigvuldiging).
 - (ii) Zij G een eindige groep met n elementen, en zij $d \in G$ een element van orde d . Welk verband bestaat er tussen d en n ?
 - (iii) Wat bedoelt men met een cyclische groep?
 - (iv) Stel: van een eindige groep G ken je de orde van ieder element. Hoe kun je hieruit opmaken dat de groep al dan niet cyclisch is?
- (b) De Viergroep van Klein V_4 is gegeven via de volgende vermenigvuldigingstabel.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a
Viergroep van Klein				

Laat zien dat V_4 niet cyclisch is.

- (c) Bepaal $\phi(30)$ en geef een opsomming van alle elementen van $(\mathbb{Z}/(30))^*$.
- (d) Bepaal van elk element van $(\mathbb{Z}/(30))^*$ de orde. Werk efficiënt en geef voldoende toelichting.
- (e) Is $(\mathbb{Z}/(30))^*$ een cyclische groep?

Normering:

1a	6	2a	3	3a	2	4a	5	MC	20
1b	6	2b	3	3b	6	4b	3		
1c	6	2c	6	3c	6	4c	3		
		2d	6			4d	5		
						4e	4		
18		18		14		20		20	

Voor het multiple choice gedeelte geldt: -4 ptn per foute keuze.

Totaal = 90

Cijfer = Behaald Totaal / 10 + 1

N.B.: Na afloop van het tentamen vind je een volledig uitgewerkte versie van het tentamen op blackboard (Knop "Course materials", folder #9, laatste item). De attachment bestaat in postscript en in pdf.

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. Gegeven is dat $a = b \cdot q + r$ met $0 \leq r < |b|$ (delingsalgoritme voor a, b). Dan is de $\text{ggd}(a, b)$ in het algemeen gelijk aan:

- ☐ $\text{ggd}(a, r)$.
- ☐ $\text{ggd}(b, r)$.
- ☐ $\text{ggd}(a, q)$.
- ☐ $\text{ggd}(b, q)$.

5.2. De stelling van Bezout in $\mathbb{Z}$ stelt dat voor iedere $a, b \neq 0$

- ☐ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
- ☐ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$.
- ☐ een unieke oplossing x bestaat van het stelsel vergelijkingen

$$x \equiv \begin{cases} a \bmod m, \\ b \bmod n, \end{cases}$$

waar de moduli m, n relatief priem zijn.

- ☐ geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .

5.3. Gegeven is de modulus $m = 9$ en de matrix

$$M := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad (\text{modulo } 9, \text{ standaard representanten}).$$

- ☐ De inverse matrix van M modulo m is

$$\begin{pmatrix} 7 & 1 \\ 6 & 4 \end{pmatrix} \quad (\text{standaard representanten}).$$

- ☐ De inverse matrix van M modulo m is

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \quad (\text{standaard representanten}).$$

- ☐ M heeft weliswaar een inverse modulo m , maar het is niet een van de voorgaande.
- ☐ De matrix M heeft geen inverse modulo m .

5.4. De axioma's (O1-3) in $\mathbb{Z}$ stellen dat de natuurlijke ordening een *partiële* ordening is. Het axioma (O4) in $\mathbb{Z}$ stelt dat deze ordening *totaal* is. Dat laatste betekent:

- ☐ Voor alle x bestaat een y met $x \leq y$.
- ☐ Voor alle x bestaat een y met $x \leq y$ of $y \leq x$.
- ☐ Er bestaat een y zodat voor alle x geldt: $x \leq y$ of $y \leq x$.
- ☐ Voor alle x en voor alle y is $x \leq y$ of $y \leq x$.

5.5. Een verzameling $A \subseteq V$ is stabiel onder een binaire operatie f in V wanneer aan de volgende voorwaarde is voldaan.

- ☐ Voor alle $x, y \in V$: als $f(x, y) \in A$ dan $x, y \in A$.
- ☐ Voor alle $x, y \in V$: $f(x, y) \in A$.
- ☐ Voor alle $x, y \in V$: als $x, y \in A$ dan $f(x, y) \in A$.
- ☐ Voor alle $x, y \in V$: als $y \in A$ dan $f(x, y) \in A$.

5.6. In de vermenigvuldigingstabel van een bepaalde groep met 6 elementen e (neutraal), p, q, r, s, t , lezen we onder het hoofdje de volgende onvolledige regel:

*	e	p	q	r	s	t
p	p	q	e	.	t	.

- o** Je kan deze gegevens met zekerheid vervolledigen tot

*	e	p	q	r	s	t
p	p	q	e	s	t	r

- o** Je kan deze gegevens met zekerheid vervolledigen tot

*	e	p	q	r	s	t
p	p	q	e	r	t	s

- o** Je kan deze gegevens met zekerheid vervolledigen tot

*	e	p	q	r	s	t
p	p	q	e	p	t	r

- o** De informatie is onvoldoende, er kunnen meerdere mogelijkheden zijn.

Axioma's Gehele Getallen (zover nodig)

Gelijkheid

Gelijkheidswet: $x = x$.

Gelijkheidsregel: ...

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:

$$x + y = x + z \rightarrow y = z \quad (\text{linker } -).$$

$$x + z = y + z \rightarrow x = y \quad (\text{rechter } -).$$

Uniciteit van tegengestelde:

$$x + y_1 = 0 \text{ en } x + y_2 = 0 \rightarrow y_1 = y_2.$$

$$y_1 + x = 0 \text{ en } y_2 + x = 0 \rightarrow y_1 = y_2.$$

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:

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

Multiplicatieve 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:

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

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

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