GEEN SAKREKENAARS TOEGELAAT

Universiteit van Stellenbosch
Toegepaste Wiskunde 314
Semestertoets 1a
25 Maart 2003 om 19:30
Tyd: 90 min Punte: 80

.

Vul asseblief in / *Please complete*:

Van (blokletters) / *Surname (capitals)*
Volle Voorname / *Full First Names*
US–nommer / *US Number*

Vir kantoorgebruik / *For official use*

Vraag *Question*	Punte *Marks*	Nasiener *Examiner*
1–2	/11	L Terblanche
3–4	/11	L Terblanche
5–7	/9	L Terblanche
8	/5	L Terblanche
9	/7	L Terblanche
10	/9	L Terblanche
11	/9	L Terblanche
12	/6	L Terblanche
13	/3	L Terblanche
14	/10	L Terblanche
Totaal		

Eksaminatore / Examiners: Dr PJP Grobler & Prof JH van Vuuren

Lees asseblief die volgende reëls en voorskrifte, en teken dan die onderstaande verklaring:

(1) Kommunikasie tussen kandidate word nie in die eksamenlokaal toegelaat nie.

(2) Hulpmiddels (insluitende blankopapier, boeke, geskrifte en elektroniese apparaat) word nie in die eksamenlokaal toegelaat nie, tensy die gebruik van spesifieke items uitdruklik toegelaat of voorgeskryf is.

(3) Geen dele van hierdie vraestel/antwoordstel mag verwyder word nie.

(4) Ekstra tyd word nie toegestaan aan kandidate wat laat kom nie.

(5) Kandidate word nie toegelaat om die eksamenlokaal binne die eerste 45 minute van die eksamensessie te verlaat nie.

(6) Antwoorde moet in ink direk op hierdie vraestel/antwoordstel ingevul word.

(7) Hierdie vraestel/antwoordstel moet aan 'n opsiener oorhandig word voordat u die eksamenlokaal verlaat.

Please read the following rules and instructions, and then sign the declaration below:

(1) Communication between candidates is not allowed.

(2) Supporting material (including blank paper, books, notes and electronic equipment) is not allowed in the examination room, unless the use of particular items is expressly allowed or prescribed.

(3) No parts of this question/answer paper may be removed.

(4) Latecomers are not allowed extra time.

(5) Candidates are not allowed to leave the examination room within the first 45 minutes of the examination session.

(6) Answers must be supplied in ink directly on this question/answer paper.

(7) Before leaving the examination room candidates must hand this question/answer paper to an invigilator.

VERKLARING / *DECLARATION*	HANDTEKENING / *SIGNATURE*
Hiermee verklaar ek dat ek die bogenoemde eksamenreëls sal gehoorsaam en dat die inligting op hierdie bladsy verstrek, korrek is. / *I hereby declare that I will abide by the above examination rules and that the particulars supplied on this front cover are correct.*	

(1) Definieer wat bedoel word met die konsep van 'n ring $(\mathcal{R}, \bullet, \star)$ met identiteitselement. /
Define what is meant by the notion of a ring $(\mathcal{R}, \bullet, \star)$ *with identity element.* [9]

(2) $(\mathbb{Z}_m, +, \times)$ is 'n voorbeeld van 'n ring met identiteitselement, waar $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, en waar "+" en "×" geneem word as m–modulêre optelling en vermenigvuldiging onderskeidelik. As $m = \infty$, dan word die ring verkry waarin u op laerskool leer tel het. Gee nog 'n (verskillende) voorbeeld van 'n ring met identiteitselement. / *$(\mathbb{Z}_m, +, \times)$ is an example of a ring with identity element, where $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, and where "+" and "×" are taken as m–modular addition and multiplication respectively. If $m = \infty$, then the ring is obtained in which you learned to count at primary school. Give another (different) example of a ring with identity element.* [2]

(3) Definieer wat bedoel word met die konsep van 'n groep $(\mathcal{G}, \bullet)$. / *Define what is meant by the notion of a group $(\mathcal{G}, \bullet)$.* [4]

(4) Watter van die volgende tweetalle is groepe en watter is nie? Motiveer indien u sê dat 'n tweetal nie 'n groep is nie. / *Which of the following pairs represent groups. Motivate if you answer that a pair is not a group.* [7]

(a) $(\mathbb{Z}_m[x], +)$, waar $\mathbb{Z}_m[x]$ die ruimte van alle polinome met koëffisiënte in $\mathbb{Z}_m$ is, en waar "+" geneem word as gewone polinoomoptelling, gevolg deur 'n reduksie van koëffisiënte na hul ooreenstemmende ekwivalensieklasse modulo m. / *where $\mathbb{Z}_m[x]$ denotes the space of all polynomials with coefficients in $\mathbb{Z}_m$ and where "+" is taken as the usual addition of polynomials, followed by a reduction of coefficients to their corresponding equivalence classes modulo m.*

(b) $(\mathbb{Z}[x], \times)$, waar $\mathbb{Z}[x]$ die ruimte van alle polinome met heeltallige koëffisiënte is, en waar "$\times$" geneem word as gewone polinoomvermenigvuldiging. / *where $\mathbb{Z}[x]$ denotes the space of all polynomials with integral coefficients and where "$\times$" is taken as the usual multiplication operation for polynomials.*

(c) $(\mathbb{Z}\backslash\{0\}, /)$, waar $\mathbb{Z}\backslash\{0\}$ alle heelgetalle uitgesonderd nul aandui, en waar a/b gedefineer word as $\lfloor a \div b \rfloor$ vir enige $a, b \in \mathbb{Z}\backslash\{0\}$. / *where* $\mathbb{Z}\backslash\{0\}$ *denotes the set of all integers except zero, and where* a/b *is defined as* $\lfloor a \div b \rfloor$ *for any* $a, b \in \mathbb{Z}\backslash\{0\}$.

(d) $(\mathbb{Z}^+, \backslash)$, waar $\mathbb{Z}^+$ alle positiewe heelgetalle aandui, en waar $a\backslash b$ gedefineer word as $\lceil a \div b \rceil$ vir enige $a, b \in \mathbb{Z}^+$. / *where* $\mathbb{Z}^+$ *denotes the set of all positive integers, and where* $a\backslash b$ *is defined as* $\lceil a \div b \rceil$ *for any* $a, b \in \mathbb{Z}^+$.

(5) Definieer wat bedoel word met die konsep van 'n Abelse groep $(\mathcal{A}, \bullet)$. / *Define what is meant by the notion of an Abelean group* $(\mathcal{A}, \bullet)$. [2]

(6) Watter van die volgende tweetalle is Abelse groepe en watter is nie? Motiveer indien u sê dat 'n tweetal nie 'n Abelse groep is nie. / *Which of the following pairs represent Abelean groups? Motivate if you answer that a pair is not an Abelean group.* [4]

(a) $(\mathcal{Z}^n, \bullet)$, waar $\mathcal{Z}^n$ die versameling van alle n–ryvektore met heeltallige inskrywings voorstel, en waar "$\bullet$" as die dotproduk tussen vektore geneem word. / *where* $\mathcal{Z}^n$ *denotes the set of all* n*–row vectors with integral entries, and where "*$\bullet$*" is taken as the dot product between vectors.*

(b) $(\mathcal{Z}_m^{n*}, \times)$, waar $\mathcal{Z}_m^{n*}$ die versameling van alle $n \times n$ matrikse met inskrywings in $\mathbb{Z}_m^*$ voorstel, en waar "$\times$" as die m–modulêre produk tussen matrikse geneem word. / *where $\mathcal{Z}_m^{n*}$ denotes the set of all $n \times n$ matrices with entries in $\mathbb{Z}_m^*$, and where "$\times$" is taken as the m–modular product between matrices.*

(7) Is $(\mathcal{Z}_m^{n*}, +, \times)$ 'n ring? Hier is $\mathcal{Z}_m^{n*}$ die versameling van alle $n \times n$ matrikse met inskrywings in $\mathbb{Z}_m^*$, "+" is die modulêre som tussen matrikse, en "$\times$" is die m–modulêre produk tussen matrikse. Motiveer. / *Is $(\mathcal{Z}_m^{n*}, +, \times)$ a ring? Here $\mathcal{Z}_m^{n*}$ denotes the set of all $n \times n$ matrices with entries in $\mathbb{Z}_m^*$, "+" is the m–modular sum of two matrices, and "$\times$" is the m–modular product of two matrices. Motivate.* [3]

(8) Bewys dat elke element $a \in \mathcal{A}$ in 'n Abelse groep $(\mathcal{A}, \bullet)$ 'n *unieke* inverse met betrekking tot die operasie "$\bullet$" besit. [Wenk: Neem die teendeel aan, en soek 'n teenspraak.] / *Prove that every element $a \in \mathcal{A}$ in an Abelean group $(\mathcal{A}, \bullet)$ possesses a* unique *inverse with respect to the operation "$\bullet$". [Hint: Assume the opposite and seek a contradiction.]*
. [5]

(9) (a) Verskaf 'n **nodige en voldoende voorwaarde** vir die **bestaan** van 'n inverse tot 'n heelgetal modulo m. / *Provide a* **necessary and sufficient condition** *for the* **existence** *of an inverse to an integer modulo m.* [1]

(b) Verskaf 'n **nodige en voldoende voorwaarde** vir die **uniekheid** van 'n inverse tot 'n heelgetal modulo m. / *Provide a* **necessary and sufficient condition** *for the* **uniqueness** *of an inverse to an integer modulo m.* [1]

(c) Gebruik die **Gewysigde Euklidiese Algoritme** om elk van die volgende modulêre inverses te bereken. Vul u antwoorde in die onderstaande tabelle in. / *Use the* **Revised Euclidean Algorithm** *to calculate each of the following modular inverses. Fill in your answers in the tables below.* [5]

i. $23^{-1} \pmod{40}$

i	p_i	q_i	r_i	s_i	x_i	y_i
0						
1						
2						
3						
4						
5						
6						
7						

ii. $25^{-1} \pmod{40}$

i	p_i	q_i	r_i	s_i	x_i	y_i
0						
1						
2						
3						
4						
5						
6						
7						

(10) (a) Gee 'n **nodige en voldoende voorwaarde** vir die bestaan van oplossings $x \in \mathbb{Z}_m$ tot die lineêre kongruensie $ax \equiv y \pmod{m}$. Indien daar aan hierdie voorwaarde voldoen word, hoeveel verskillende oplossings $x \in \mathbb{Z}_m$ bestaan daar tot die kongruensie? / *Provide a* **necessary and sufficient condition** *for the existence of solutions $x \in \mathbb{Z}_m$ to the linear congruence $ax \equiv y \pmod{m}$. If this condition is satisfied, how many different solutions $x \in \mathbb{Z}_m$ does the congruence admit?* [3]

(b) Bepaal alle oplossings $(x, y) \in \mathbb{Z}_{40} \times \mathbb{Z}_{40}$ tot die onderstaande sisteem van lineêre kongruensies. Wys volledige werking.

$$\begin{cases} 2x - 3y & \equiv & 16 \pmod{40} \\ 2x + 5y & \equiv & 32 \pmod{40} \end{cases}$$

Determine all solutions $(x, y) \in \mathbb{Z}_{40} \times \mathbb{Z}_{40}$ to the above system of linear congruences. Show your complete working. [6]

(11) (a) Die onderstaande indeks kan gebruik word om die onderliggende natuurlike taal tot 'n kriptoteks wat met behulp van mono–alfabetiese substitusie gevorm is, te bepaal. Verduidelik die betekenis en rol van elk van die simbole η, κ, T, k, $\underline{\alpha}$, ρ en 26 in hierdie indeks.

$$\eta^T(k) = \underbrace{\sum_{\underline{\alpha}} \left(\rho^T_{\underline{\alpha}}\right)^2}_{\kappa^T(k)} - \frac{1}{(26)^k}$$

The above index may be used to the determine the underlying natural language of a ciphertext formed by a mono–alphabetic substitution. Describe the meaning and role of each of the symbols η, κ, T, k, $\underline{\alpha}$, ρ and 26 in this index. [4]

(b) Verskaf 'n volledige afleiding en motivering vir die struktuur van die indeks in (a). / *Provide a complete derivation and motivation for the structure of the index in (a).*
. [5]

(12) Aanvaar dat $\phi(ab) = \phi(a)\phi(b)$ vir enige paar relatiewe priem getalle a en b, waar ϕ die bekende Euler–funksie is, en bewys dat / *Assume that $\phi(ab) = \phi(a)\phi(b)$ for any pair of relatively prime numbers a en b, waar ϕ is the well–known Euler function, and prove that*

$$\phi(m) = \prod_{i=1}^{k} \left(p_i^{e_i} - p_i^{e_i-1}\right),$$

waar / *where*

$$m = \prod_{i=1}^{k} p_i^{e_i}$$

die priemfaktorisering van m voorstel, met $e_i > 0$ vir alle $i = 1, \ldots, k$ / *denotes the prime factorisation of m, with $e_i > 0$ for all $i = 1, \ldots, k$.* [6]

(13) Bereken die inverse van die onderstaande matriks $\mathbf{S}$ in die versameling $\mathcal{Z}_{26}^{2*}$. Toets die korrektheid van u antwoord deur te toets dat die identiteit $\mathbf{S}\mathbf{S}^{-1} = \mathbf{I}$ bevredig word.

$$\mathbf{S} = \begin{bmatrix} 3 & 7 \\ 21 & 4 \end{bmatrix}$$

Calculate the inverse of the above matrix $\mathbf{S}$ *in the set* $\mathcal{Z}_{26}^{2*}$. *Test the validity of your answer by verifying that the identity* $\mathbf{S}\mathbf{S}^{-1} = \mathbf{I}$ *is satisfied.* [3]

(14) Gebruik 'n boom–struktuur om 'n breë klassifikasie van die verskillende soorte kripto–sisteme wat vandag in gebruik is, te gee, en omskryf kortliks die hoof–verskille tussen die verskillende soorte sisteme. / *Use a tree–structure to give a broad classification of the different types of cryptographic ciphers that are in use today, and briefly describe the chief differences between each of these types of ciphers.* [10]