ENIGE (SAK)REKENAARS TOEGELAAT

University of Stellenbosch
Toegepaste Wiskunde 314
Semestertoets 1a
24 Maart 2004 om 19:30

***Time*: 90 min** ***Full marks*: 60**

Vul asseblief in / *Please complete*:

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

Vir kantoorgebruik / *For official use*

Vraag *Question*	Punte *Marks*	Nasiener *Marker*
1	/10	H Botha
2	/25	H Botha
3	/11	JH van Vuuren
4	/14	JH van Vuuren
Totaal		

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

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

'n Binêre operasie • en 'n nie-leë versameling $\mathcal{G}$ vorm 'n groep indien

i) $a \bullet b \in \mathcal{G} \quad \forall\, a, b \in \mathcal{G}$

ii) $a \bullet (b \bullet c) = (a \bullet b) \bullet c \quad \forall\, a, b, c \in \mathcal{G}$

iii) daar 'n element $\varepsilon \in \mathcal{G}$ bestaan sodat $a \bullet \varepsilon = \varepsilon \bullet a \quad \forall\, a \in \mathcal{G}$

iv) daar vir elke $a \in \mathcal{G}$ 'n $a^{-1} \in \mathcal{G}$ bestaan sodat
$a \bullet a^{-1} = a^{-1} \bullet a = \varepsilon$

(b) Vorm $(\mathbb{Z}_m, +)$ 'n groep (waar '+' m–modulêre optelling aandui)? Motiveer. / *Does* $(\mathbb{Z}_m, +)$ *form a group (where '+' denotes* m*–modular addition)? Motivate.* [1]

Ja, dit voldoen aan die voorwaardes in (a).
'+' is beslis assosiatief en $\mathbb{Z}_m$ is geslote onder m-modulêre optelling.

$\varepsilon = 0$

$a^{-1} = m - a \quad \forall\, a \in \mathbb{Z}_m,\ a \neq 0$ en $0^{-1} = 0$

(c) Vorm $(\mathbb{Z}_m, \times)$ 'n groep (waar '×' m–modulêre vermenigvuldiging aandui) indien m priem is? Motiveer. / *Does* $(\mathbb{Z}_m, \times)$ *form a group (where '×' denotes* m*–modular multiplication) if* m *is prime? Motivate.* [1]

Nee, $0 \in \mathbb{Z}_m$ en 0^{-1} bestaan nie, al is m priem

(d) Bevestig dat $(\{1,3,5,7\},\times)$ 'n groep vorm (waar '$\times$' 8–modulêre vermenigvuldiging aandui), deur 'n vermenigvuldigingstabel op te stel. Skryf die inverse van elke groep-element direk vanuit die tabel neer. / *Verify that* $(\{1,3,5,7\},\times)$ *forms a group (where '$\times$' denotes 8–modular multiplication), by constructing a multiplication table. Write down the inverse of each group element directly from the table.* [4]

'x' is beslis assosiatief

$\varepsilon = 1$

x	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Uit bostaande tabel volg dit dat $\{1,3,5,7\}$ geslote is onder 'x'.

Elke element in $\{1,3,5,7\}$ is self-invoterend.

(2) (a) Gee 'n nodige en voldoende voorwaarde vir die bestaan van 'n multiplikatiewe inverse van 'n element a in die ring $(\mathbb{Z}_m, \times, +)$. / *Give a necessary and sufficient condition for the existence of a multiplicative inverse to an element A in the ring* $(\mathbb{Z}_m, \times, +)$. [2]

ggd$(a, m) = 1$

(b) 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.* [4]

i. $4^{-1} \pmod{15}$

i	p_i	q_i	r_i	s_i	x_i	y_i
0	15	4	3	3	0	1
1	4	3	1	1	1	−3
2	3	1	0	3	−3	4
3	1	0				
4						
5						
6						

$4^{-1} \equiv 4 \pmod{15}$

ii. $4^{-1} \pmod{60}$

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

$4^{-1} \pmod{60} \nexists$, want ggd$(4, 60) = 4 \neq 1$

(c) Bewys die volgende stelling: / *Prove the following theorem:* [7]

Die lineêre kongruensie / *The linear congruence*

$$ax \equiv y \pmod{m}$$

besit oplossings $x \in \mathbb{Z}_m$ as en slegs as $d = \mathrm{ggd}(a, m)$ 'n deler is van y. As d wel 'n deler is van y, dan besit die kongruensie presies d oplossings, en hulle is: / *possesses solutions $x \in \mathbb{Z}_m$ if and only if $d = \mathrm{ggd}(a, m)$ is a divisor of y. If d is indeed a divisor of y, then the congruence possesses exactly d solutions, and they are:*

$$x = \left(\frac{a}{d}\right)^{-1}\left(\frac{y}{d}\right) + k\left(\frac{m}{d}\right), \quad 0 \leq k \leq d-1.$$

Sien bladsy 31 van die klasnotas

(d) Vind alle oplossings $x \in \mathbb{Z}_{60}$ tot die lineêre kongruensie / *Find all solutions $x \in \mathbb{Z}_{60}$ to the linear congruence*

$$16x \equiv 24 \pmod{60}$$

Wys u werking volledig. / *Show all your working.* [4]

ggd(16,60) = 4 wat 'n deler is van 24

Dus besit die kongruensie 4 verskillende oplossings in $\mathbb{Z}_{60}$

Die oplossings is — moet mod 15 bereken word – sien 2(b)(i)

$$x = \left(\frac{16}{4}\right)^{-1}\left(\frac{24}{4}\right) + k\left(\frac{60}{4}\right), \quad k = 0,1,2,3$$

$$= 4 \times 6 + 15k, \quad k = 0,1,2,3$$

$$= 24, 39, 54, 69$$

$$\equiv 9, 24, 39, 54 \pmod{60}$$

(e) Bewys, vanuit eerste beginsels, dat / *Prove, from first principles, that*

$$|\mathbb{Z}_m^*| = \prod_{i=1}^{k} \left(p_i^{e_i} - p_i^{e_i-1}\right)$$

indien m se priemfaktorisering gegee word deur / *if the prime factorisation of m is given by*

$$m = \prod_{i=1}^{k} p_i^{e_i}, \quad e_i > 0,\ i = 1, \ldots, k.$$

U mag, sonder bewys aanvaar dat $\phi(ab) = \phi(a)\phi(b)$ indien a en b relatief priem is (waar ϕ die beroemde Euler–funksie is), maar alle ander resultate wat u gebruik, moet ook bewys word. / *You may use, without proof, the result that $\phi(ab) = \phi(a)\phi(b)$ if a and b are relatively prime (where ϕ is the famous Euler function), but all other results that you use, must also be proved.* [5]

<u>Lemma:</u> $\phi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i-1}$ vir enige priem p_i

<u>Bewys:</u> Omdat p_i priem is, is die enigste getalle in die interval $[1, \ldots, p_i^{e_i}]$ wat <u>nie</u> relatief priem t.o.v. $p_i^{e_i}$ is nie, die veelvoude van p_i

$$\therefore \phi(p_i^{e_i}) = p_i^{e_i} - |\{m, 2m, 3m, \ldots, p_i^{e_i-1}p_i\}|$$
$$= p_i^{e_i} - p_i^{e_i-1}$$

Nou is
$$|\mathbb{Z}_m^*| = \phi(m)$$
$$= \phi\left(\prod_{i=1}^{k} p_i^{e_i}\right)$$
$$= \prod_{i=1}^{k} \phi(p_i^{e_i}) \quad [\text{want } p_i^{e_i}, p_j^{e_j} \text{ is relatief priem vir } i \neq j]$$
$$= \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i-1}) \quad [\text{uit die Lemma}]$$

(f) Bereken $\phi(120)$. / *Compute* $\phi(120)$. [2]

$$120 = 2^3 \times 3^1 \times 5^1$$
$$\Rightarrow \phi(120) = (2^3 - 2^2)(3^1 - 3^0)(5^1 - 5^0)$$
$$= (8-4)(3-1)(5-1)$$
$$= 32$$

(3) (a) Laat $\mathcal{Z}_m^n$ die versameling van alle $n \times n$ matrikse wees met inskrywings in $\mathbb{Z}_m$. Gee 'n nodige en voldoende voorwaarde vir die bestaan van 'n inverse tot 'n matriks $\mathbf{X} \in \mathcal{Z}_m^n$, wat self weer 'n element van $\mathcal{Z}_m^n$ is. / *Let $\mathcal{Z}_m^n$ be the set of all $n \times n$ matrices with entries in the set $\mathbb{Z}_m$. Give a necessary and sufficient condition for the existence of a multiplicative inverse to a matrix $\mathbf{X} \in \mathcal{Z}_m^n$, which is itself again an element of $\mathcal{Z}_m^n$.* [2]

$\text{ggd}(|X|, m) = 1$

(b) Laat $\mathcal{Z}_m^{n,*}$ die versameling van alle $n \times n$ matrikse met inskrywings in $\mathbb{Z}_m$ wees, wat multiplikatiewe inverses in dieselfde versameling besit. Vorm $(\mathcal{Z}_m^{n,*}, \times, +)$ 'n ring? Motiveer. / *Let $\mathcal{Z}_m^{n,*}$ be the set of all $n \times n$ matrices with entries in $\mathbb{Z}_m$ that have multipilcative inverses in the same set. Does $(\mathcal{Z}_m^{n,*}, \times, +)$ form a ring? Motivate.* [3]

Nee, die versameling $\mathcal{Z}_m^{n,*}$ is nie geslote onder '+' nie (wel onder '$\times$').

(c) Bereken die 26–modulêre inverse van die matriks / *Compute the 26–modular inverse of the matrix*

$$X = \begin{bmatrix} 8 & 13 & 8 \\ 18 & 8 & 13 \\ 25 & 20 & 17 \end{bmatrix}.$$

Wys u werking volledig. / *Show all your working.* [6]

$|X| = 535 \equiv 15 \pmod{26}$, sodat $X^{-1} \pmod{26}$ bestaan.

Die toegevoegde van X word gegee deur

$$X^* = \begin{bmatrix} \begin{vmatrix} 8 & 13 \\ 20 & 17 \end{vmatrix} & -\begin{vmatrix} 13 & 8 \\ 20 & 17 \end{vmatrix} & \begin{vmatrix} 13 & 8 \\ 8 & 13 \end{vmatrix} \\ -\begin{vmatrix} 18 & 13 \\ 25 & 17 \end{vmatrix} & \begin{vmatrix} 8 & 8 \\ 25 & 17 \end{vmatrix} & -\begin{vmatrix} 8 & 8 \\ 18 & 13 \end{vmatrix} \\ \begin{vmatrix} 18 & 8 \\ 25 & 20 \end{vmatrix} & -\begin{vmatrix} 8 & 13 \\ 25 & 20 \end{vmatrix} & \begin{vmatrix} 8 & 13 \\ 18 & 8 \end{vmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} -124 & -61 & 105 \\ 19 & -64 & 40 \\ 160 & 165 & -170 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 6 & 17 & 1 \\ 19 & 14 & 14 \\ 4 & 9 & 12 \end{bmatrix} \pmod{26}$$

Dus is $X^{-1} = (15)^{-1} \begin{bmatrix} 6 & 17 & 1 \\ 19 & 14 & 14 \\ 4 & 9 & 12 \end{bmatrix}$

$$= \begin{bmatrix} 42 & 119 & 7 \\ 133 & 98 & 98 \\ 28 & 63 & 84 \end{bmatrix} \equiv \begin{bmatrix} 16 & 15 & 7 \\ 3 & 20 & 20 \\ 2 & 11 & 6 \end{bmatrix} \pmod{26}$$

(4) (a) Bereken die inverse van die permutasie $\pi^* = [4,1,5,3,2,6]$. / *Compute the inverse of the permutation* $\pi^* = [4,1,5,3,2,6]$. [2]

$$\begin{array}{c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 4 & 1 & 5 & 3 & 2 & 6 \end{array} \Rightarrow \begin{array}{c|c|c|c|c|c} 4 & 1 & 5 & 3 & 2 & 6 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 \end{array} \Rightarrow \begin{array}{c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 2 & 5 & 4 & 1 & 3 & 6 \end{array}$$

$$\therefore (\pi^*)^{-1} = [2,5,4,1,3,6]$$

(b) Die kriptoteks **NWSEHHWAELLTEHMEREGEAATI** is met behulp van die kolomtransposisie stelsel $\mathcal{C}_{26}^{6,\pi^*}$ gevorm. Wat is die ooreenstemmende skoonteks? / *The ciphertext* **NWSEHHWAELLTEHMEREGEAATI** *was formed by means of the columnar transposition* $\mathcal{C}_{26}^{6,\pi^*}$. *What is the corresponding plaintext?* [3]

1	2	3	4	5	6
N	W	S	E	H	H
W	A	E	L	L	T
E	H	M	E	R	E
G	E	A	A	T	I

$\Rightarrow$

2	5	4	1	3	6
w	h	e	n	s	h
a	l	l	w	e	t
h	r	e	e	m	e
e	t	a	g	a	i

Skoonteks is dus "whenshallwethreemeetagai" oftewel "when shall we three meet agai(n)".

(c) Definieer wat bedoel word met 'n permutasiematriks. / *Define what is meant by a permutation matrix.* [1]

'n Matriks met presies een 1 in elke ry en in elke kolom; die ander inskrywings is almal 0

(d) Skryf neer die permutasiematriks wat met die permutasie π^* in (a) ooreenstem. / *Write down the permutation matrix corresponding to the permutation π^* in (a).* [1]

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(e) Bewys dat die inverse $\mathbf{P}^{-1}$ van elke permutasiematriks $\mathbf{P}$ weer 'n permutasiematriks is. [Wenk: Ondersoek die transponent $\mathbf{P}^T$.] / *Prove that the inverse* $\mathbf{P}^{-1}$ *of any permutation matrix* $\mathbf{P}$ *is again a permutation matrix. [Hint: Investigate the transposed matrix* $\mathbf{P}^T$*.]* [7]

Laat $P = [p_{ij}]$ 'n $n \times n$ permutasiematriks wees met $p_{i,k_i} = 1$ die nie-nul element in ry i. Dan is die (enigste) nie-nul element in die i-te kolom van P^T die element $p^T_{k_i,i} = p_{i,k_i} = 1$. Dus word die (i,j)-te inskrywing van PP^T gegee deur

$$\sum_{\ell=1}^{n} p_{i,\ell}\, p^T_{\ell,j} = \sum_{\ell=1}^{n} p_{i,\ell}\, p_{j,\ell} = p_{i,k_i} p_{j,k_i}$$

(aangesien $p_{i,\ell} = 0$, tensy $\ell = k_i$). Maar nou is $p_{j,k_i} = 0$, tensy $j = i$, sodat die (i,j)-te inskrywing van PP^T gegee word deur

$$\begin{cases} 1, & \text{as } j = i \\ 0, & \text{as } j \neq i \end{cases}$$

wat impliseer dat $PP^T = I$. Dit volg soortgelyk dat $P^T P = I$, sodat $P^T = P^{-1}$.