Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 1: Donderdag 19 Februarie 2004

MEMORANDUM

Tuttoets 1a.

(1) *Definieer volledig wat bedoel word met die konsep van 'n* ring $(\mathcal{R}, \star, \bullet)$.

Uit die klasnotas aangehaal:

"A non–empty set $\mathcal{R}$ together with two binary operations $\star$ and $\bullet$ form a **ring** $(\mathcal{R}, \star, \bullet)$ if:

R1: $a \star b \in \mathcal{R}$ for any $a, b \in \mathcal{R}$ (i.e. $\mathcal{R}$ is closed under $\star$).

R2: $a \star b = b \star a$ for any $a, b \in \mathcal{R}$ (i.e. $\star$ is commutative).

R3: $(a \star b) \star c = a \star (b \star c)$ for any $a, b, c \in \mathcal{R}$ (i.e. $\star$ is associative).

R4: a zero element $0 \in \mathcal{R}$ exists such that $a \star 0 = a$ for any $a \in \mathcal{R}$.

R5: an element $(-a) \in \mathcal{R}$ exists for any $a \in \mathcal{R}$ such that $a \star (-a) = 0$.

R6: $a \bullet b \in \mathcal{R}$ for any $a, b \in \mathcal{R}$ (i.e. $\mathcal{R}$ is closed under $\bullet$).

R7: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for any $a, b, c \in \mathcal{R}$ (i.e. $\bullet$ is associative).

R8: $a \bullet (b \star c) = a \bullet b \ \star \ a \bullet c$ and $(b \star c) \bullet a = b \bullet a \ \star \ c \bullet a$ for any $a, b, c \in \mathcal{R}$ (i.e. $\star$ and $\bullet$ are distributive)."

(2) *Voltooi die volgende sin deur in elke paar moontlikhede die verkeerde opsie deur te haal, en motiveer daarna u keuses. Spesifiseer ook die nul–element van die ring.*

Die drietal $(\mathcal{M}_n, +, \times)$ *is 'n voorbeeld van 'n (kommutatiewe / nie–kommutatiewe) ring (met / sonder) identiteitselement, waar* $\mathcal{M}_n$ *die versameling van alle* $n \times n$ *matrikse is, en waar '*$+$*' en '*$\times$*' die binêre operasies van onderskeidelik optelling en vermenigvuldiging tussen matrikse is.*

Die drietal $(\mathcal{M}_n, +, \times)$ is 'n voorbeeld van 'n nie–kommutatiewe ring met identiteitselement. Die redes hiervoor is dat matriksvermenigvuldiging nie kommutatief is nie, en die identiteitsmatriks ($n \times n$ matriks met ene op die hoof–diagonaal en verder nulle) is die identiteitselement vir die ring. Die nul–element is die $n \times n$ matriks wat slegs nul–inskrywings bevat.

Tuttoets 1b.

(1) *Dekripteer,* met die hand, *die kriptoteks* `NQCHJYUEM`*, wat met behulp van die additiewe substitusie–stelsel* $\Im_{26}^{20}$ *gevorm is. Wys u werking volledig.*

Kriptoteks:	N	Q	C	H	J	Y	U	E	M
$y \rightarrow$	13	16	2	7	9	24	20	4	12
$x \equiv y - 20 \pmod{26} \rightarrow$	19	22	8	13	15	4	0	10	18
Skoonteks:	t	w	i	n	p	e	a	k	s

Skoonteks is dus `twin peaks`.

(2) *Die kriptoteks* `KAEGFKTWJY` *is met behulp van die additiewe substitusie–stelsel gevorm. Ontrafel die sleutel en dekripteer dan die kriptoteks. Wys u werking.*

Met behulp van *EnDeCrypt:*

$s = 25$: `lbfhgluxkz`
$s = 24$: `mcgihmvyla`
$s = 23$: `ndhjinwzmb`
$s = 22$: `oeikjoxanc`
$s = 21$: `pfjlkpybod`
$s = 20$: `qgkmlqzcpe`
$s = 19$: `rhlnmradqf`
$s = 18$: `simonsberg`

Skoonteks is dus `Simonsberg`.

(3) *Gebruik die Gewysigde Euklidiese Algoritme om die inverse* $a \equiv (19)^{-1} \pmod{36}$ *te bepaal. Wys u werking volledig deur die onderstaande tabel in te vul. Toets die korrektheid van u antwoord deur die produk* $19a \pmod{36}$ *te evalueer.*

i	p_i	q_i	r_i	s_i	x_i	y_i
0	36	19	17	1	0	1
1	19	17	2	1	1	–1
2	17	2	1	8	–1	2
3	2	1	0	2	2	$\boxed{-17}$
4	1	0				

Dus is $(19)^{-1} \equiv -17 \equiv 19 \pmod{36}$. Toets: $19 \times 19 = 361 \equiv 1 \pmod{36}$.