Divisie Wiskunde en Informatika	**Algebra en Discrete Wiskunde I**
Vrije Universiteit	**Tentamen 20-12-06**

Opgelet: Er is een apart multiple-choice gedeelte op de laatste bladzijde (vraag 6). Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!

1. Modulorekenen

(a) Algemene kennis:

- **(i)** Zij $m \geq 2$ een geheel getal. Geef het relatievoorschrift voor de relatie *x is congruent met y modulo m*.
- **(ii)** Laat a, b gehele getallen ongelijk nul zijn. Wat zegt de *Bezout formule* over deze getallen?
- **(iii)** De *ISBN code* bestaat uit een aantal symbolen (cijfers 0-9 of 'x' voor '10'). Het laatste symbool is een "check" symbool. Wat is de check voorwaarde?

(b) In $\mathbb{Z}/(65)$ met vermenigvuldiging zoeken we naar de inverse van een klasse x. Completeer de volgende tabel. Antwoorden volstaan; een kopie van de tabel is beschikbaar achterop het multiple-choice blad.

x is:	inverse ja/nee:	(zo ja) inverse is:
$\overline{25}$		
$\overline{26}$		
$\overline{27}$		

(c) Los het volgende stelsel vergelijkingen op (modulus 31):

$$\begin{cases} \bar{6} \cdot x + \overline{11} \cdot y = \bar{0} \\ \bar{5} \cdot x + \bar{3} \cdot y = \bar{3} \end{cases}$$

2. Groepen

(a) Algemene kennis:

- **(i)** Je heb een groep van orde 29 en een element x dat niet het neutrale element is. Wat weet je van de *orde van x?*
- **(ii)** Laat $m \geq 2$ geheel zijn. Welke informatie wordt er weergegeven met de *Euler functie* $\phi(m)$*?*
- **(iii)** Formuleer de *Chinese reststelling* in een situatie waar je precies twee moduli m_1, m_2 hebt.

(b) Zoek een geheel getal x dat tegelijk voldoet aan $x \equiv 11 \,(mod\ 14)$ en $x \equiv 8 \,(mod\ 15)$ (goede toelichting scoort).

(c) Bereken $10^{74} \,(mod\ 51)$ op een economische manier (goede toelichting scoort).

3. Veeltermringen

(a) Algemene kennis:

- **(i)** In sommige veeltermringen $R[X]$ geldt de *gradenformule.* Wat zegt deze formule en voor welk type van ringen R is ze geldig?
- **(ii)** Gegeven zijn: een lichaam K en twee veeltermen $A, B \in K[X]$ ongelijk nul. Het *Delingsalgoritme* zegt iets over een formule van de vorm $A = B \cdot Q + R$. Wat wordt er precies gezegd?
- **(iii)** Leg bondig uit hoe de *CRC* (*Cyclic Redundancy Check*) functioneert: sleutel, codering, decodering. Je hoeft niets aan te tonen.

(b) Zij K een lichaam. Laat zien dat een veelterm $P \in K[X]$ van graad ≥ 1 geen (multiplicatieve) inverse kan hebben in $K[X]$ (goede toelichting scoort).

(c) Zij $K := \mathbb{Z}/(2)$. Het is bekend dat $X^2 + X + \bar{1}$ de enige tweedegraadse irreducibele veelterm is in

$K[X]$ (niet aantonen). Gebruik dit resultaat om aan te tonen dat $M := X^4 + X^3 + \bar{1}$ irreducibel is in $K[X]$.

4. Vector ruimten

(a) Algemene kennis:

(i) Wat bedoelt men met een *lineair onafhankelijk stel vectoren* $\{v_1,..,v_n\}$ in een vector ruimte V over een lichaam $\mathbb{F}$?
(ii) Wat bedoelt men met een *voortbrengend stel vectoren* $\{v_1,..,v_n\}$ in een vector ruimte V over een lichaam $\mathbb{F}$?
(iii) Wat bedoelt men met *een basis* in een vector ruimte V over een lichaam $\mathbb{F}$?

(b) We bekijken de volgende drie vectoren achtereenvolgens over $\mathbb{Z}/(3)$ en $\mathbb{Z}/(5)$:

$$u := \begin{pmatrix} \bar{0} \\ \bar{1} \\ \bar{2} \end{pmatrix}, \quad v := \begin{pmatrix} \bar{1} \\ \bar{2} \\ \bar{0} \end{pmatrix}, \quad w := \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix}.$$

Laat zien dat $\{u, v, w\}$ lineair afhankelijk is in $(\mathbb{Z}/(3))^3$, maar lineair onafhankelijk in $(\mathbb{Z}/(5))^3$. Beredeneer dat het in dit geval zelfs om een basis gaat.

(c) Neem nu de volgende 3 bij 5 matrix over $\mathbb{Z}/(5)$.

$$M := \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{1} & \bar{2} \\ \bar{1} & \bar{2} & \bar{0} & \bar{1} & \bar{1} \\ \bar{2} & \bar{0} & \bar{1} & \bar{1} & \bar{2} \end{pmatrix}.$$

Bepaal de dimensie van de nulruimte van M (goede toelichting scoort).
N.B.: de eerste drie kolommen zijn precies de vectoren uit deel (b); je mag de resultaten uit dat onderdeel indien nodig hier gebruiken.

5. Eindige lichamen

(a) Algemene kennis.

(i) Wat is een *primitief element* van een eindig lichaam?
(ii) Welke getallen $m \geq 2$ komen in aanmerking als het *aantal elementen* van een eindig lichaam, en welke niet?
(iii) Leg bondig uit: het *Diffie-Hellman protocol* voor sleuteluitwisseling.

Voor de rest van deze opgave bekijken we de veelterm $M := X^3 + X + \bar{1} \in \mathbb{Z}_2[X]$ en de quotiëntring $\mathbb{F} := \mathbb{Z}_2[X])/(M)$.

(b) Laat zien dat M irreducibel is. Volgens de theorie is de quotiëntring $\mathbb{F}$ dus een lichaam (niet aantonen). Controleer nu dat $\alpha := \bar{X}$ een *primitief element* is van het lichaam $\mathbb{F}$. Goede toelichting scoort.
(c) Maak een *tabel* waarin de elementen van $\mathbb{F}^*$ weergegeven zijn als (i) macht van α, (ii) een veelterm, (iii) een 3-bit code. Geef voldoende toelichting; je hoeft je berekeningen niet te tonen.
(d) Bereken efficiënt met behulp van je tabel:

(i) `110 * 101`
(ii) de inverse van `110`

Normering:

1a:	4	2a:	4	3a:	4	4a:	4	5a:	4	6:	15
1b:	5	2b:	6	3b:	5	4b:	5	5b:	3		
1c:	6	2c:	5	3c:	6	4c:	5	5c:	5		
								5d:	4		
	15		15		15		14		16		15

Voor het multiple-choice deel geldt: –3 punten per fout.

Totaal = 90; Cijfer = Behaald totaal/10 + 1

Na afloop van dit tentamen vind je een volledig uitgewerkte versie van het tentamen op blackboard (Knop "Course information", folder #9 bij week 51). De attachment bestaat in postscript en in pdf.

Leeg blad ten behoeve van apart multiple-choice gedeelte.

naam, studierichting & jaar: 18-12-02

6. 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.

6.1. Welke bewering over *priemrestklassen* is waar?
o $\overline{13}$ is een priemrestklasse modulo 26.
o De som van twee priemrestklassen modulo 26 is weer een priemrestklasse modulo 26.
o Het product van twee priemrestklassen modulo 26 is weer een priemrestklasse modulo 26.
o Er zijn geen priemrestklassen modulo 26 want 26 is niet priem.

6.2. Een *deelgroep* H van een groep $(G,*)$ is
o Een deelverzameling H van G met een operatie $x\#y$, zó dat $(H,\#)$ een groep is.
o Een deelverzameling H van G die stabiel is onder de operatie $x*y$ van G.
o Een deelverzameling H van G die stabiel is onder de operatie y^{-1} (inverse) van G.
o Een deelverzameling H van G die stabiel is onder de operatie $x*y^{-1}$ van G.

6.3. De sleutel voor de cryptografische methode van *RSA* bestaat uit 5 getallen $m=p\cdot q$ (met p,q priem) en d,e, waarbij m,e publiek zijn en p,q,d privé. Aan welke voorwaarde moeten d,e voldoen:
o $ggd(m,d)=1=ggd(m,e)$.
o $d\cdot e\equiv 1\,(mod\ m)$.
o $d\cdot e\equiv 1\,(mod\ \phi(m))$.
o $\phi(d)\cdot\phi(e)\equiv 1\,(mod\ m)$.

6.4. Een *ideaal* van een commutatieve unitaire ring R is een deelverzameling van R die
o stabiel is onder de optelling $x+y$ en de vermenigvuldiging $x\cdot y$ van R.
o stabiel is onder de optelling $x+y$ en de vermenigvuldiging $x\cdot y$ van R, en die het eenheidselement van R bevat.
o stabiel is onder de optelling $x+y$ van R en sterk stabiel is onder de vermenigvuldiging $x\cdot y$ van R.
o sterk stabiel is onder de optelling $x+y$ van R en stabiel is onder de vermenigvuldiging $x\cdot y$ van R.
N.B.: Een verzameling $A\subseteq V$ is *sterk stabiel* onder een bewerking $x\#y$ in V wanneer geldt: als $x\in V$ en $y\in A$ dan $x\#y\in A$.

6.5. Zij V een *vectorruimte* van *dimensie* 3 over een lichaam $\mathbb{F}$ met 4 elementen. Dan is
o $\#V=64\ (=4^3)$.
o $\#V=81\ (=3^4)$.
o $\#V=12\ (=3\cdot 4)$.
o $\#V$ onbepaald want er zijn onvoldoende gegevens.

6.6. De *karakteristiek* van een eindig lichaam K is
o de additieve orde van het eenheidselement van K.
o de multiplicatieve orde van het nulelement van K.
o de orde van de additieve groep K.
o de orde van de multiplicatieve groep K *.

x is:	inverse ja/nee:	(zo ja) inverse is:
$\overline{25}$		
$\overline{26}$		
$\overline{27}$		

Tabel bij Opgave 1(b): $\mathbb{Z}/(65)$