Kenmerk: EWI2015/TW/DMMP/MU/00X

Oefen Tentamen 2, Module 7, Vakcode 201400433
Discrete Structuren & Efficiënte Algoritmes

Alle antwoorden dienen te worden gemotiveerd. Gebruik van een rekenmachine is niet toegestaan. Gebruik van zelfgeschreven formulebladen, één dubbelzijdig A4 (deze keer 1 A4 in totaal), is wel toegestaan. Indien u een onderdeel niet kunt oplossen dan kunt het resultaat van dat onderdeel in latere onderdelen toch gebruiken.

Dit tentamen bestaat uit drie onderdelen, en is gebaseerd op de volgende, geschatte tijdsbesteding per onderdeel (slechts als indicatie):

Languages & Machines (L&M)	1h	(30 punten)
Algebra (ALG)	1h40min	(50 punten)
Discrete Mathematics (DW)	20 min	(10 punten)

Dus in totaal 30+10+50=90 punten. Incl. de 10 gratis punten zijn het 100 punten. Het tentamencijfer is het totaal aantal punten gedeeld door 10.

Gebruik aub per onderdeel (L&M/ALG/DW) een nieuw vel!

Algebra

1. Zij $(G, \cdot)$ de groep

   $$G = \{M \mid M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad a, b, c, d \in \mathbb{Z}_{11} \quad \det M \neq 0\}$$ met matrixvermenigvuldiging.

   (a) Laat zien dat G een groep is.

   (b) Bepaal
   $$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1}$$

   (c) Bepaal het aantal elementen van G. Hint: bereken eerst het aantal 2×2 matrices M in $\mathbb{Z}_{11}^{2\times 2}$, de verzameling 2×2 matrices over $\mathbb{Z}_{11}$, met $\det M = 0$.

2. (a) Schrijf de unitaire groep $U(165)$ op vier verschillende manieren als directe som van unitaire groepen.

   (b) Is $U(165)$ cyclisch?

3. Is de verzameling $S = \{a \mid a \in \mathbb{Z} \quad 2 \text{ deelt } a \text{ of } 3 \text{ deelt } a\}$ een deelring van $\mathbb{Z}$?

4. Gegeven is het polynoom $p(x) = 1 + x + x^3 + x^4 + x^5 \in \mathbb{Z}_2[x]$.

   (a) Laat zien dat er geen polynomen $a(x), b(x) \in \mathbb{Z}_2[x]$ bestaan zodanig dat $a(x)b(x) = p(x)$ en $\operatorname{gr} a(x) = 2$ en $\operatorname{gr} b(x) = 3$.

   (b) Beredeneer dat $p(x)$ irreducibel is.

   Definieer $\mathbb{F} = \mathbb{Z}_2[x]/(p(x))$.

   (c) Is $\mathbb{F}$ een lichaam?

   (d) Hoeveel elementen heeft $\mathbb{F}$?

   (e) Wat is de dimensie van $\mathbb{F}$ als vectorruimte over $\mathbb{Z}_2$?

   (f) (extra, niet verplicht). Laat $\mathbb{K}$ een lichaam zijn van dimensie d als vectorruimte over $\mathbb{Z}_2$ en $\mathbb{Z}_2 \subset \mathbb{K} \subset \mathbb{F}$.

   Hoeveel elementen heeft $\mathbb{K}$? Wat is de dimensie van $\mathbb{F}$ opgevat als vectorruimte over $\mathbb{K}$?

   (g) (extra, niet verplicht). Beredeneer dat er geen lichamen strikt tussen $\mathbb{Z}_2$ en $\mathbb{F}$ zitten.

Languages & Machines

5. Breng de volgende contextvrije grammatica G stapsgewijs naar Chomsky Normaalvorm. Geef duidelijk aan welke stappen je neemt, en wat de tussenresultaten zijn:

$$G = \begin{cases} S & \to & A\,B \mid B\,C\,S \\ A & \to & a\,A \mid C \\ B & \to & b\,B \mid \lambda \\ C & \to & c\,C \mid \lambda \end{cases}$$

6. Beschouw de volgende contextvrije taal $L = \{a^i\, b^*\, c^j \mid j \geq i \geq 0\}$.
   Geef een *deterministische* PDA (stapelautomaat) voor deze taal.

7. Een two-tape Turing Machine (TM) heeft twee tapes. Bij de start staat het woord op tape 1 en is tape 2 blanco. Voor het woord $aabcbaa$ is de startconfiguratie bijvoorbeeld

$$[q_0; *Baabcbaa B; *BBBBB]$$

   waarbij B een blanco symbool is, en * de positie van de kop in de tapes aangeeft.

   (a) Schrijf een two-tape Turing Machine (TM) die de volgende taal *herkent*: $\{w\,c\,w^R \mid w \in \{a,b\}^*\}$.

   (b) Leg kort de werking van uw machine uit, aan de hand van een berekening voor het woord $aabcbaa$ vanaf de startconfiguratie

(c) Kan uw TM deze taal ook *beslissen*?

(d) Is uw TM deterministisch?

Discrete Mathematics

8. (3 punten) Bereken 3^{20} (mod 5).

9. (7 punten) De RSA methode met modulus $n = 55$ en exponent $e = 7$ is gebruikt om bericht M te coderen tot $C = M^e = 2$. Bereken M.