Kenmerk: EWI2012/TW/DMMP/052/MU

Tentamen Discrete Wiskunde II (152162/152163)

Maandag 16 april 2012, 08:45 - 11:45 uur (SC)

Alle antwoorden dienen te worden gemotiveerd

Gebruik van een rekenmachine is niet toegestaan

Er zijn 9 opgaven, dus reken ca. 20 minuten per opgave

2 1. (a) Laat zien dat de Diophantische vergelijking $1000s + 444t = 2$ geen oplossing heeft voor $s, t \in \mathbb{Z}$.

2 (b) Voor $a, b \in \mathbb{Z}$, neem aan dat $as+bt = c$ en $ax+by = c+1$ voor zekere $s, t, x, y, c \in \mathbb{Z}$. Laat zien dat a en b relatief priem zijn.

3 2. (a) Bereken de oplossing van de recurrente betrekking

$$a_n - 10a_{n-1} + 25a_{n-2} = 16n + 8 \quad (n \geq 2) \quad \text{met } a_0 = 3 \text{ en } a_1 = 12\,.$$

3 (b) Noem a_n het aantal strings uit $\{0, 1, 2\}^*$ van lengte n die geen oneven aantal 1-en bevatten. Bepaal a_1, a_2, en een recurrente betrekking voor a_n, $n \geq 3$. (Je hoeft deze betrekking niet op te lossen.)

2 3. Voor gegeven $c \in \mathbb{Z}, c \geq 1$, laat zien dat $c^n \in \mathrm{O}(\, n!\,)$. [Hint: Voor n groot genoeg geldt $c^n \leq n!$]

4. Geef een *recursieve* beschrijving van een algoritme $\mathtt{Max}(a_1, \ldots, a_n)$ die als input $n = 2^k$ getallen $\{a_1, \ldots, a_n\}$ krijgt, en als output $\max_{i=1,\ldots,n} a_i$ geeft. Analyseer ook de looptijd van jouw algoritme in termen van het aantal vergelijkingen. Gebruik hiervoor eenvoudig leesbare pseudocode zoals "For $k = 1, \ldots, n$ do", "If $(\ldots)$ then $(\ldots)$;", etc. Je mag het master theorem gebruiken, en ook O( )-notatie.

4

5. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn, zonder loops, met lijn lengtes $d_e \geq 0$, $e \in E$. Laat $T \subseteq E$ een minimaal opspannende boom (MST) voor G zijn. Laat $s \in V$, en laat D_s de vereniging van alle kortste (s, v)-paden zijn, voor alle $v \in V$. Laat zien dat $T \cap D_s \neq \emptyset$.

4

6. Laat $G = (V, E)$ een enkelvoudige ongerichte graaf zijn, zonder loops, en $|V| \geq 7$. Bewijs dat, als $d(v) \geq 6$ voor alle $v \in V$, dan is G niet planair. [Hier is $d(v)$ de graad van v, dus de aantal buren van v.]

4

7. Laat zoals gebruikelijk S_4 de symmetrische groep zijn, i.e., de elementen van S_4 zijn de permutaties van $\{1,2,3,4\}$ en de operatie is de concatenatie $\circ$. Laat $\sigma \in S_4$ gegeven zijn door

3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

dus $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4$, en $\sigma(4) = 1$. Bekijk de deelgroep H gegenereerd door σ, $H := < \sigma > = \{\sigma^k \mid k \in \mathbb{Z}\}$. Hoeveel linker of rechter cosets heeft H in S_4? Motiveer het antwoord.

4

8. Laat $(G, \circ)$ een groep zijn, met één (unity) e, en $a \in G$ met $|< a >| = n$. Als $a^k = e$, laat zien dat dan $n|k$.

9. Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 55$ en de exponent $e = 7$ heeft gepubliceerd. Bob mailt het gecodeerde bericht $C = 2$ naar Alice. Beschrijf een manier voor afluisteraar Eve om C te decoderen, bepaal alle gegevens die Eve hiervoor nodig heeft, en bereken Bob's oorspronkelijke bericht M. Waarom wordt RSA toch als veilige methode beschouwd?

5

$C^d = m$

Normering:

1.(a): 2 2.(a): 3 3.: 2 4.: 4 5.: 4 6.: 4 7.: 3 8.: 4 9.: 5
(b): 2 (b): 3

Totaal: 36 + 4 = 40 punten