Kenmerk: EWI2011/TW/DMMP/012/MU

Tentamen Discrete Wiskunde II (152162/152163)

Maandag 11 april 2011, 08:45 - 11:45 uur (SC)

Alle antwoorden dienen te worden gemotiveerd

Gebruik van een rekenmachine is niet toegestaan

1. Voor welke waarden van c heeft de volgende diophantische vergelijking een oplossing met $a, b, c \in \mathbb{Z}$? (Gebruik het algoritme van Euclides.)

$$922a + 34b = c\,.$$

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

$$a_n + 4a_{n-1} + 4a_{n-2} = 6(-2)^n + 9 \quad (n \geq 2) \quad \text{met } a_0 = 10 \text{ en } a_1 = 5\,.$$

   (b) We bekijken strings uit $\{0,1,2\}^*$. Noem a_n het aantal strings uit $\{0,1,2\}^*$ van lengte n die niet de substring 01 en ook niet de substring 02 bevatten. Bepaal a_1, a_2, a_3 en een recurrente betrekking voor a_n, $n \geq 4$. (Je hoeft deze betrekking niet op te lossen.)

3. Het volgende, recursieve algoritme berekent a^n.

Algorithm 1: `Power`(a, n)

```
input  : a, n with n ∈ ℤ, n ≥ 0
output: a^n
if (n == 0) then return 1;
else
    if (n even) then
        return Power(a · a, n/2);                    // a^n = (a^2)^{n/2}
    else
        if (n == 1) then
            return a;
        else
            return a·Power(a · a, (n − 1)/2); // a^n = a · (a^2)^{(n−1)/2}
```

Laat $f(n)$ het aantal vermenigvuldigingen zijn van algorithme `Power`, voor $n \geq 0$.

(a) Geef een recurrente betrekking aan voor $f(n)$, voor $n = 2^k$, en laat zien dat $f(n) \in \mathrm{O}(\log n)$ voor alle $n = 2^k$. Je mag het "master theorem" gebruiken.

(b) Laat zien dat $f(n)$ *niet* monotoon stijgend is.

(c) Laat met volledige inductie zien dat $f(n) \leq 2\log_2 n + 2$ voor alle $n \geq 1$.

4. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn, zonder loops, met lijn lengtes $d_e \geq 0$, $e \in E$. Laat $v_0 \in V$. Noem een lijn $e \in E$ *vitaal* als er een $v \in V$ bestaat en een kortste pad $P(v_0, v)$ vanuit v_0 naar v zodat $e \in P(v_0, v)$. Bewijs of geef een tegenvoorbeeld voor de volgende stelling.

   Als $d_e \neq d_{e'}$ voor alle lijnen $e \neq e'$, dan is $\{e \in E \mid e \text{ is } \textit{vitaal}\}$ een boom.

5. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn met $|V| \geq 11$, en laat $\bar{G} = (V, \bar{E})$ de complement graaf van G zijn, waarbij $\bar{E} = \{\{v, w\} \mid v \neq w,\ \{v, w\} \notin E\}$. Laat zien dat G en $\bar{G}$ niet beide planair kunnen zijn.

6. Bekijk de vergelijking $x^2 + x = 2$ in $\mathbb{Z}_p$, $p \geq 2$.

   (a) Bewijs dat er precies 2 oplossingen zijn als p een priemgetal is.

   (b) Toon aan, door geven van een voorbeeld, dat er meer dan 2 oplossingen kunnen zijn als p geen priemgetal is.

7. Laat $(G, \circ)$ een groep zijn met $|G| = 29$, en laat e de één (unity) van G zijn. Laat zien dat voor alle $a, b \in G$ met $b \neq e$, een $k \in \mathbb{Z}$ bestaat met

$$a = b^k .$$

8. Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 91$ en de exponent $e = 31$ heeft gepubliceerd. Alice ontvangt het gecodeerde bericht $C = 10$ van Bob. Beschrijf de procedure die Alice gebruikt om C te decoderen, bepaal alle gegevens die Alice hiervoor nodig heeft, en bereken Bob's oorspronkelijke bericht M.

Normering:

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

Totaal: 36 + 4 = 40 punten