Kenmerk: TW10/DWMP/MU/0704

Hertentamen Discrete Wiskunde II (152162/152163)

Dinsdag 29 juni 2010, 13:45 - 16:45 uur (SP 1)

Alle antwoorden dienen te worden gemotiveerd

Gebruik van een rekenmachine is niet toegestaan

1. (a) Bepaal met behulp van het algoritme van Euclides de grootste gemene deler van 1000 en 444.

   (b) Voor welke $k \in \mathbb{Z}$ bestaan er $s, t \in \mathbb{Z}$ met

$$1000s + 444t = k\,?$$

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

$$a_{n+2} - 6a_{n+1} + 9a_n = 3 \cdot 2^n + 7 \cdot 3^n \ (n \geq 0) \quad \text{met } a_0 = 1 \text{ en } a_1 = 4\,.$$

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

3. Het volgende, recursieve algoritme berekent het maximum van n getallen $x_1, \ldots, x_n$.

Algorithm 1: maxi(·)

```
input  : x_1, ..., x_n
output: max{x_1, ..., x_n}
if (n == 1) then return x_1;
else
    k = ⌊n/2⌋;
    a = maxi(x_1, ..., x_k);
    b = maxi(x_{k+1}, ..., x_n);
    if (a > b) then
        return a;
    else
        return b;
```

Laat $f(n)$ het maximale aantal vergelijkingen zijn die maxi(·) op een input van lengte n doet.

   (a) Bewijs met behulp van volledige inductie dat f monotoon stijgend is.

   (b) Bepaal een recurrente betrekking voor $f(n)$ als $n = 2^k$. Laat zien dat $f(n) \in \mathrm{O}(n)$ (je mag het "Master Theorem" hiervoor gebruiken).

4. Bewijs de volgende stelling
$$\log(n!) \in \Omega(n \log n)\,.$$

5. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn met lijn gewichten $w_e \geq 0$, $e \in E$. Bewijs of geef een tegenvoorbeeld voor de volgende stelling.

   Als e een lijn is met $w_e < w_{e'}$ voor alle $e' \neq e$, en $e = \{i, j\}$, dan zijn i en j buren in iedere minimaal opspannende boom T van G.

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

7. 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.

8. Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 91$ en de exponent $e = 29$ heeft gepubliceerd. Alice ontvangt het gecodeerde bericht $C = 4$ 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.: 2	2.(a): 4	3.(a): 4	4.: 3	5.: 4	6. 4	7.(a): 2	8.: 4
2	(b): 2	(b): 3				(b): 2	

Totaal: 36 + 4 = 40 punten