Kenmerk: TW10/DWMP/MU/0704

Tentamen Discrete Wiskunde II (152162/152163)

Maandag 12 april 2010, 08:45 - 11:45 uur (SC 0)

Alle antwoorden dienen te worden gemotiveerd

Gebruik van een rekenmachine is niet toegestaan

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

$$888a + 108b = c\,.$$

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

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

   (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 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 machten a^n.

Algorithm 1: `Power`

```
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 $n = 2^k$. Je mag het "master theorem" gebruiken.

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

   (c) Laat per mathematische inductie zien dat $f(n) \leq 2 + \log_2 n$ voor alle $n \geq 1$ (en dus $f(n) \in \mathrm{O}(\log n)$ voor alle $n \geq 0$).

4. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn, zonder loops, 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 $e = \{v, w\}$, dan zijn v en w buren in iedere minimaal opspannende boom T van G.

5. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn, zonder loops. Laat $|V| = v$ en $|E| = e \geq 2$. Bewijs de volgende stelling:

   Als G planair en bipartiet is, dan $e \leq 2v - 4$

6. Bekijk de ring $\mathbb{Z}_{10}$.

   (a) Bepaal alle eenheiden (units) in $\mathbb{Z}_{10}$, en voor iedere eenheid de (multiplicatieve) inverse. Is $\mathbb{Z}_{10}$ een lichaam? Hoezo (niet)?

   (b) Bereken $7^{65} \pmod{10}$.

7. Laat $(G, \circ)$ een groep zijn met 13 elementen, 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 $n = 55$ en de exponent $e = 7$ heeft gepubliceerd. Alice ontvangt het gecodeerde bericht $C = 2$ 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 (b): 2 ? 3.(a): 3 (b): 2 ? (c): 3 ← 4.: 4 5.: 4 6.(a): 2 (b): 2 7.: 3 8.: 4

Totaal: 36 + 4 = 40 punten