Kenmerk: EWI-TW2011/DMMP/016/MU

Hertentamen Discrete Wiskunde II (152162/152163)

Dinsdag 28 juni 2011, 13:45 - 16:45 uur (CR 2K)

Alle antwoorden dienen te worden gemotiveerd

Gebruik van een rekenmachine is niet toegestaan

1. Neem aan dat voor $a, b, c \in \mathbb{Z}^+$ geldt $c|ab$.

   (a) Toon aan dat als c een priemgetal is, dat dan $c|a$ of $c|b$.

   (b) Geef een voorbeeld, waarbij wel $c|ab$, maar niet $c|a$ en ook niet $c|b$.

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 éénen 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 "$(a > b)$" zijn die maxi$(\cdot)$ 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 $f(n) \in O(n)$ (je mag het "Master Theorem" hiervoor gebruiken).

4. Laat $G = (V, E)$ een bipartiete, ongerichte graaf zijn, zonder loops. Laat $|V| = v$ en $|E| = e$, $e > 1$. Bewijs de volgende stelling.

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

5. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn, zonder loops, met lijn lengtes $d_e \geq 0$, $e \in E$. Laat T een minimaal opspannende boom zijn voor G. Voor gegeven $u \in V$, laat D_u de Dijkstra boom zijn van G, bestaande uit de vereniging van alle kortste (u, v)-paden die het Dijkstra algorithme berekent met als startpunt u.

   Laat zien dat $T \cap D_u \neq \emptyset$.

6. Zoals gebruikelijk is U_n de groep van inverteerbare elementen in $\mathbb{Z}_n$.

   (a) Laat $m \in \mathbb{Z}_n$ met $gcd(n, m) = 1$. Toon aan dat $m \in U_n$.

   (b) Is $(U_6, \cdot)$ een cyclische groep? Motiveer het antwoord.

7. We noteren met S_5 de groep van permutaties van $\{1, 2, 3, 4, 5\}$ met als groepoperatie de samenstelling $\circ$. Verder is $\sigma \in S_5$ gegeven door:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

   en $H = \langle \sigma \rangle = \{\sigma^k \mid k \in \mathbb{Z}\}$, de groep gegenereerd door σ.

   (a) Bepaal de orde van H.

   (b) Hoeveel linker cosets heeft H in S_5 ? Motiveer.

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

Totaal: 36 + 4 = 40 punten