Kenmerk: EWI2012/TW/DMMP/059/MU

Hertentamen Discrete Wiskunde II (152162/152163)

Dinsdag 03 juli 2012, 13:45 - 16:45 uur

Alle antwoorden dienen te worden gemotiveerd

Gebruik van een rekenmachine is niet toegestaan

Er zijn 8 opgaven, dus reken ca. 22 minuten per opgave

1. (a) Laat zien dat de Diophantische vergelijking $924s + 36t = 10$ geen oplossing heeft voor $s, t \in \mathbb{Z}$.

   (b) Als a en b relatief priem zijn, en $a > b$, laat zien dat $\gcd(a - b, a + b) = 1$ of $\gcd(a - b, a + b) = 2$.

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

$$a_n - 10a_{n-1} + 21a_{n-2} = 60 \cdot 3^n \quad (n \geq 2) \quad \text{met} \quad a_0 = 2 \text{ en } a_1 = -5\,.$$

   (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 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 $f(n) \in \mathsf{O}(n)$, voor *alle* $n \in \mathbb{N}$ (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 of geef een tegenvoorbeeld voor de volgende stellingen.

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

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

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 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 samenstelling $\circ$. Laat $\sigma \in S_4$ gegeven zijn door

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

   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.

7. Laat $(G, \circ)$ een groep zijn met $|G| = 59$, 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, maar dat ontvangt ook luisteraar Eve. Beschrijf de procedure die Eve gebruikt om C te decoderen, bepaal alle gegevens die Eve hiervoor nodig heeft, en bereken Bob's oorspronkelijke bericht M. Beantwoord in één zinnetje: Waarom wordt RSA toch als veilige methode beschouwd?

Normering:

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

Totaal: 36 + 4 = 40 punten