Kenmerk: EWI2013/TW/DMMP/020/MU

Tentamen Discrete Wiskunde II (152162/152163)

Maandag 15 april 2013, 08:45 - 11:45 uur (SC)

Alle antwoorden dienen te worden gemotiveerd. Gebruik van een rekenmachine is niet toegestaan. Er zijn in totaal 9 opgaven, dus reken gemiddeld met 20 minuten per opgave.

1. Voor $a, b \in \mathbb{Z}$, neem aan dat $as + bt = 8$ en $ax + by = 9$ voor zekere $s, t, x, y \in \mathbb{Z}$. Laat zien dat a en b relatief priem zijn.

2. Voor een gegeven alfabet $\Sigma = \{0, 1, 2, 3, 4\}$, laat a_n de aantal strings in Σ^n zijn met een *even* aantal 0-en.

   (a) Bereken a_1, en stel een recurrente betrekking op voor a_n, $n \geq 2$.

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

3. Laat $f(n) = \sum_{i=1}^{n} i^5$. Laat zien dat $f(n) \in \Theta(n^6)$, i.e., $f(n) \in \mathsf{O}(n^6)$ en $f(n) \in \Omega(n^6)$. [Hint: Om te laten zien dat $f(n) \in \Omega(n^6)$, is het voldoende te laten zien dat er in $f(n)$ $\Omega(n)$ termen staan die allemaal $\Omega(n^5)$ zijn.]

4. 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 van het soort "**if**$(a > b)$" 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 $f(n) \in \mathsf{O}(n)$, voor *alle* $n \in \mathbb{N}$ (je mag het "Master Theorem" hiervoor gebruiken).

5. Laat $G = (V, E)$ een enkelvoudige, ongerichte graaf zijn, zonder loops, met lijn lengtes $d_e \geq 0$, $e \in E$. Laat $T \subseteq E$ een minimaal opspannende boom (MST) voor G zijn. Laat $s \in V$, en laat D_s de vereniging van alle kortste (s, v)-paden zijn, voor alle $v \in V$. Laat zien dat $T \cap D_s \neq \emptyset$.

6. Laat $G = (V, E)$ een enkelvoudige, samenhangende ongerichte graaf zijn, zonder loops, met $|V| = n$. Laat zien dat, als G planair is, de gemiddelde graad van de vertices van G kleiner is dan 6, i.e., $\frac{1}{n} \sum_{v \in V} d(v) < 6$.

7. Laat $(D, +, \cdot)$ een eindig *integraal domein* zijn, dat wil zeggen, $(D, +, \cdot)$ is een ring met 1, $(D, +, \cdot)$ heeft geen nuldeler (dus $ab = 0$ impliceert dat $a = 0$ of $b = 0$), en $|D| = n < \infty$. Laat zien dat $(D, +, \cdot)$ een lichaam is. [Hint: Bekijk voor een willekeurig $0 \neq a \in D$ de coset $aD = \{ad \mid d \in D\}$, en laat zien dat $aD = D$.]

8. Laat $(G, \circ)$ een groep zijn, met één (unity) e, en $|G| = p^2$, voor een priemgetal $p > 1$. Laat zien dat G cyclisch is.

9. Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 55$ en de exponent $e = 7$ heeft gepubliceerd. Bob mailt het gecodeerde bericht $C = 2$ naar Alice. Beschrijf een manier voor afluisteraar Eve om C te decoderen, bepaal alle gegevens die Eve hiervoor nodig heeft, en bereken Bob's oorspronkelijke bericht M. Waarom wordt RSA toch als veilige methode beschouwd?

Normering:

1.: 2 2.(a): 3 (b): 3 3.: 3 4.(a): 3 (b): 3 5.: 4 6.: 3 7.: 4 8.: 3 9.: 5

Totaal: 36 + 4 = 40 punten