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., $f(n) \in O(n^6)$ 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($\cdot$)

```
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 $f(n) \in O(n)$, 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	3.: 3	4.(a): 3	5.: 4	6.: 3	7.: 4	8.: 3	9.: 5
	(b): 3		(b): 3					

Totaal: 36 + 4 = 40 punten

Kenmerk: TW09/DWMP/MU/09-05

Cheat Sheet Discrete Mathematics II (152162/152163)

Chapters 4.3, 4.4, and 4.5

- If $a, b \in \mathbb{Z}$, $b > 0$, there exist unique $k, r \in \mathbb{Z}$ with $a = kb + r$ and $0 \leq r < b$
- $\text{gcd}(a, b) = \min\{as + bt \mid s, t \in \mathbb{Z}, as + bt > 0\}$
- a, b relatively prime $\Leftrightarrow$ $\text{gcd}(a, b) = 1$
- The Euclidean Algorithm computes $\text{gcd}(a, b)$
- Every integer $n > 1$ has a unique prime factorization, $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$ (where $p_1 \leq \cdots \leq p_k$ are primes, not necessarily all p_i different)

Chapters 5.7 and 5.8

- $f : \mathbb{N} \to \mathbb{R}$, $f \in \text{O}(g) \Leftrightarrow \exists m, n_0$ with $f(n) \leq m \cdot g(n)\ \forall\ n \geq n_0$
- $f : \mathbb{N} \to \mathbb{R}$, $f \in \Omega(g) \Leftrightarrow \exists m, n_0$ with $f(n) \geq m \cdot g(n)\ \forall\ n \geq n_0$
- $\log(n!) \in \text{O}(n \log n)$

Chapters 10.1, 10.2, and 10.3

- If $a_{n+1} = da_n\ \forall n \geq 0$ and $a_0 = A$ then $a_n = Ad^n$
- If $a_{n+2} = a_{n+1} + a_n\ \forall n \geq 0$ and $a_0 = 0, a_1 = 1$, then $a_n = F_n$ (Fibonacci numbers)

Chapters 10.6 and 12.3

- Master Theorem: if $f(1) = d$ and $f(n) = af(n/b) + c$ for all $n = b^k$ $(a, b, c, d \in \mathbb{Z}_+)$, $b \geq 2$, then for all $n = b^k$
  1. $f(n) = d + c \log_b n$ for $a = 1$
  2. $f(n) = dn^{log_b a} + \frac{c}{a-1}(n^{\log_b a} - 1)$ for $a \geq 2$
- If f is monotone increasing and $f(n) \in \text{O}(g(n))$ for all $n = b^k$ $(b \geq 2)$, then
  1. if $g \in \text{O}(n^r \log n)$ then $f \in \text{O}(n^r \log n)$ $(r > 0)$
  2. if $g \in \text{O}(n^r)$ then $f \in \text{O}(n^r)$ $(r > 0)$
- For $b, c \in \mathbb{N}$, $b \geq 2$, if $f(1) \leq c$ and $f(n) \leq b \cdot f(n/b) + c \cdot n$, for all $n = b, b^2, b^3 \ldots$, and f is monotone increasing, then $f \in \text{O}(n \log n)$

Chapters 13.1 and 13.2

- If $P = (v_0, v_1, \ldots, v_k)$ is a shortest path from v_0 to v_k, then $P_i = (v_0, v_1, \ldots, v_i)$ is a shortest path from v_0 to v_i for any $i = 0, \ldots, k$
- A spanning tree for a connected graph $G = (V, E)$ is a subgraph of G with $|V| - 1$ edges and without cycles
- In a tree $T = (V, E)$, there is a unique path $P_T(v, w)$ between any two nodes v and w
- In an edge weighted graph $G = (V, E, c)$, T is a minimum spanning tree if and only if for any edge $f = \{v, w\} \notin T$, $c_e \leq c_f\ \forall$ edges $e \in P_T(v, w)$

- In an edge weighted graph $G = (V, E, c)$, T is a minimum spanning tree if and only if for any edge $e \in T$, $c_e \leq c_f$ $\forall$ edges $f \in C(e)$, where $C(e)$ is the set of edges in the cut induced by removing edge e from T

Chapter 11.4

- A graph $G = (V, E)$ is planar if it can be drawn (embedded) in the plane without edge crossings
- A graph $G = (V, E)$ is bipartite if the nodes V can be partitioned into two sets V_1 and V_2 such that $V_1 \cap e \neq \emptyset$ and $V_2 \cap e \neq \emptyset$ $\forall e \in E$
- K_n is a complete graph on n nodes, and $K_{n,m}$ is a complete bipartite graph with $|V_1| = n$ and $|V_2| = m$
- K_5 and $K_{3,3}$ are not planar
- A graph is planar if and only if it contains no subgraph homeomorphic to K_5 and $K_{3,3}$
- For planar graph $G = (V, E)$ with $|V| = v$ and $|E| = e$, $v - e + r = 2$, where r is the number of regions of a planar embedding of G
- The dual of a planar graph $G = (V, E)$ with $|V| = v$ and $|E| = e$ has $e - v + 2$ nodes and e edges

Chapters 14.1 and 14.3

- $(R, +, \cdot)$ is a ring if R is closed for "$+$" and "$\cdot$", "$+$" is associative, commutative, has an identity for "$+$" (0), and each element has a "$+$"-inverse $(-a)$, "$\cdot$" is associative, and the distributive law for "$\cdot$" over "$+$" holds
- $(R, +, \cdot)$ is a commutative ring if in addition "$\cdot$" is commutative
- A commutative ring is a field if every element ($\neq 0$) is a unit (has an inverse for "$\cdot$")
- In $\mathbb{Z}_n$, a is a unit if and only if $\gcd(a, n) = 1$
- $\mathbb{Z}_n$ is a field if and only if n is prime
- $\mathbb{Z}_n$ has $\phi(n)$ units, with $\phi(n) = |\{k \mid 1 \leq k < n, \gcd(k, n) = 1\}|$

Chapters 16.1, 16.2, and 16.3

- $(G, \circ)$ is a group if G is closed for "$\circ$" and "$\circ$" is associative, has an identity for "$\circ$" (e), and each element a has an inverse for "$\circ$" (a^{-1})
- If $(G, \circ)$ is a finite group and $H \subseteq G$, then H is a subgroup if and only if H is closed for "$\circ$"
- A group G is cyclic if there is an $a \in G$ with $G = < a > = \{a^k \mid k \in \mathbb{Z}\}$.
- If G is a finite group and $a \in G$ then $< a >$ is a subgroup of G, and $< a > = \{a^k \mid k \in \mathbb{Z}\} = \{a, a^2, \ldots, a^m = e\}$ for some $m \in \mathbb{N}$
- Lagrange's Theorem: If G is a group with $|G| = n$ and $H \subseteq G$ is a subgroup with $|H| = m$, then $m|n$

RSA

- If G is a group and $|G| = n$ then $a^n = e$ $\forall a \in G$
- Euler's Theorem: If $n > 1$ and $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (\text{mod } n)$