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	3.(a): 3	4.: 4	5.: 4	6.(a): 2	7.: 3	8.: 4
	(b): 2	(b): 2			(b): 2		
		(c): 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 $0 \leq r < b$
- $\gcd(a, b) = \min\{as + bt \mid s, t \in \mathbb{Z}, as + bt > 0\}$
- a, b relatively prime $\Leftrightarrow \gcd(a, b) = 1$
- The Euclidean Algorithm computes $\gcd(a, b)$
- 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

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

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 $f(1) = c$ and $f(n) = af(n/b) + c$ for all $n = b^k$ $(a, b, c \in \mathbb{Z})$, then for all $n = b^k$
  1. $f(n) = c(\log_b n + 1)$ for $a = 1$
  2. $f(n) = \frac{c}{a-1}(an^{\log_b a} - 1)$ for $a \geq 2$
- If f is monotone increasing and $f(n) \in \mathrm{O}(g(n))$ for all $n = b^k$ $(b \geq 2)$, then
  1. if $g \in \mathrm{O}(n^r \log n)$ then $f \in \mathrm{O}(n^r \log n)$ $(r > 0)$
  2. if $g \in \mathrm{O}(n^r)$ then $f \in \mathrm{O}(n^r)$ $(r > 0)$
- 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 $f \in \mathrm{O}(n \log n)$

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 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 $b = a^k$ for all $b \in G$
- 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 $a^{\phi(n)} \equiv 1 (\text{mod } n)$