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, $n = p_1 \cdot p_2 \cdots p_k$ (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 $a^{\phi(n)} \equiv 1 (\text{mod } n)$