CS1231 Discrete Structures *(AY2016/2017 Semester 1)*

Definitions, Theorem and Propositions

0. Basic concept

Theorem	A theorem refers to a statement that is known to be true because it has been proved.
Corollary	A corollary is a statement whose truth can be immediately deduced from a theorem that has already been proved.

1. Number Theory

Definition 1.6.1	An integer *n* is **even** if, and only if, *n* equals twice some integer. An integer *n* is **odd** if, and only if, *n* equals twice some integer plus 1. Symbolically, if *n* is an integer, then n is even ⇔ ∃ an integer k such that $n = 2k$. n is odd ⇔ ∃ an integer k such that $n = 2k + 1$.
Theorem 4.1.1 (Epp)	The sum of any two even integers is even.
Definition 4.2.1	An integer *n* is **prime** if, and only if, $n > 1$ and for all positive integers *r* and *s*, if $n = rs$, then either *r* or *s* equals *n*. An integer *n* is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers *r* and *s* with $1 < r < n$ and $1 < s < n$. In symbols: n is prime ⇔ ∀ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$. n is composite ⇔ ∃ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.
Theorem L4.2 P8	Every integer n > 1 is either prime or composite.
Proposition 4.2.2	For any two primes p and q, if $p \mid q$ then $p = q$.
Theorem 4.2.3	If p is a prime and $x_1, x_2, \ldots, x_n$, are any integers such that: $p \mid x_1x_2 \ldots x_n$, then $p \mid x_i$ for some x_i $(1 < i < n)$.
Definition P163 (Epp)	A real number *r* is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational.** More formally, if *r* is a real number, then *r* is rational ⇔ ∃ integers *a* and *b* such that $r = a\ b$ and $b \neq 0$.
Theorem 4.2.1 (Epp)	Every integer is a rational number.
Theorem 4.2.2 (Epp)	The sum of any two rational numbers is rational.
Corollary 4.2.3 (Epp)	The double of a rational number is rational.
Definition 1.3.1	If *n* and *d* are integers and $d \neq 0$ then *n* is **divisible by** *d* if, and only if, *n* equals *d* times some integer. Instead of "*n* is divisible by *d*," we can say that *n* **is a multiple of** *d*, or *d* **is a factor of** *n*, or *d* **is a divisor of** *n*, or *d* **divides** *n*. The notation **d | n** is read "*d* divides *n*." Symbolically, if *n* and *d* are integers and $\neq 0$: $d \mid n$ ⇔ ∃ an integer k such that $n = dk$.
Theorem 4.3.1 (Epp)	For all integers *a* and *b*, if *a* and *b* are positive and *a* divides *b*, then $a \leq b$.

Theorem 4.3.2 (Epp)	The only divisors of 1 are 1 and −1.
Theorem 4.3.3 (Epp)	For all integers a, b, and c, if a divides b and b divides c, then a divides c.
Theorem 4.3.4 (Epp)	Any integer $n > 1$ is divisible by a prime number.
Theorem 4.1.1	$\forall a, b, c \in Z$, if $a \mid b$ and $a \mid c$, then $\forall x, y \in Z$, $a \mid (bx + cy)$.
Theorem 4.3.5 (Epp)	Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers p_1, p_2,..., p_k, and positive integers e_1, e_2,..., e_k such that $$\mathrm{n} = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k},$$ and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.
Definition P177 (Epp)	Given any integer $n > 1$, the **standard factored form** of n is an expression of the form $$\mathrm{n} = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k},$$ where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.
Theorem 4.4.1 (Epp)	Given any integer n and positive integer d, there exist unique integers q and r such that $n = dq + r$ and $0 \le r < d$.
Definition P181 (Epp)	Given an integer n and a positive integer d, ***n div d*** = the integer quotient obtained when n is divided by d, and ***n mod d*** = the non-negative integer remainder obtained when n is divided by d. Symbolically, if n and d are integers and $d > 0$, then $n \textit{ div } d = q$ and $n \textit{ mod } d = r \Leftrightarrow n = dq + r$ where q and r are integers and $0 \le r < d$.
Theorem 4.4.2 (Epp)	Any two consecutive integers have opposite parity.
Theorem 4.4.3 (Epp)	The square of any odd integer has the form $8m + 1$ for some integer m.
Definition P187 (Epp)	For any real number x, the **absolute value of *x***, denoted $\|x\|$, is defined as follows: $$\|x\| = \begin{cases} -x, & x < 0 \\ x, & x \ge 0 \end{cases}.$$
Lemma 4.4.4 (Epp)	For all real numbers r, $-\|r\| \le r \le \|r\|$.
Lemma 4.4.5 (Epp)	For all real numbers r, $\|-r\| = \|r\|$.
Theorem 4.4.6 (Epp)	For all real numbers x and y, $\|x + y\| \le \|x\| + \|y\|$.
Theorem 4.6.1 (Epp)	There is no greatest integer.
Theorem 4.6.2 (Epp)	There is no integer that is both even and odd.
Theorem 4.6.3 (Epp)	The sum of any rational number and any irrational number is irrational.
Proposition	For all integers n, if n^2 is even then n is even.

4.6.4 (Epp)	
Theorem 4.7.1 (Epp)	$\sqrt{2}$ is irrational.
Proposition 4.7.2 (Epp)	$1 + 3\sqrt{2}$ is irrational.
Proposition 4.7.3 (Epp)	For any integer *a* and any prime number *p*, if $p \mid a$ then $p \nmid (a+1)$.
Theorem 4.7.4 (Epp)	The set of prime numbers is infinite.
Theorem 5.2.2 (Epp)	For all integers $n \geq 1$, $$1 + 2 + \cdots + n = n(n+1)/2.$$
Theorem 5.2.3 (Epp)	For any real number *r* except 1, and any integer $n \geq 0$, $$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$
Proposition 5.3.1 (Epp)	For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.
Proposition 5.3.2 (Epp)	For all integers $n \geq 3$, $2n + 1 < 2n$.
Theorem 5.4.1 (Epp)	Given any positive integer *n*, *n* has a unique representation in the form $$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$ where *r* is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$.
Definition 4.3.1	An integer *b* is said to be a lower bound for a set $X \subseteq Z$ if $b \leq x$ for all $x \in X$.
Theorem 4.3.2 Part 1	If a non-empty set $S \subseteq Z$ has a lower bound, then *S* has a least element.
Theorem 4.3.2 Part 2	If a non-empty set $S \subseteq Z$ has an upper bound, then *S* has a greatest element.
Proposition 4.3.3	If a set *S* of integers has a least element, then the least element is unique.
Proposition 4.3.4	If a set *S* of integers has a greatest element, then the greatest element is unique.
Theorem 4.4.1	Given any integer *n* and any positive integer *d*, there exist unique integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.
Definition 4.5.1	Let *a* and *b* be integers that are not both zero. The **greatest common divisor** of *a* and *b*, denoted **gcd(*a*, *b*)**, is that integer *d* with the following properties: 1. *d* is a common divisor of both *a* and *b*. In other words, $d \mid a$ and $d \mid b$. 2. For all integers *c*, if *c* is a common divisor of both *a* and *b*, then *c* is less than or equal to *d*. In other words, for all integers *c*, if $c \mid a$ and $c \mid b$, then $c \leq d$.
Proposition 4.5.2	For any integers *a*, *b*, not both zero, their *gcd* exists and is unique.
Lemma 4.8.1 (Epp)	If *r* is a positive integer, then $\gcd(r,0) = r$.
Lemma 4.8.2 (Epp)	If *a* and *b* are any integers not both zero, and if *q* and *r* are any integers such that $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$.
Definition P486 (Epp)	An integer *d* is said to be a **linear combination of integers** *a* and *b* if, and only if, there exist integers *s* and *t* such that $as + bt = d$.

Theorem 4.5.2	Let a, b be integers, not both zero, and let $d = gcd(a, b)$. Then there exist integers x, y such that: $ax + by = d$.
Theorem L4.5 P29	There are multiple solutions x, y to the equation $ax + by = d$. Once a solution pair (x, y) is found, additional pairs may be generated by $(x + kb / d , y - ka / d)$, where k is any integer.
Definition 4.5.3, P488 (Epp)	Integers a and b are **relatively prime** if, and only if, gcd$(a, b) = 1$. Integers a_1, a_2, a_3,..., a_n are **pairwise relatively prime** if, and only if, gcd$(a_i, a_j) = 1$ for all integers i and j with $1 \leq i, j \leq n$, and $i \neq j$.
Corollary 8.4.6 (Epp)	If a and b are relatively prime integers, then there exist integers s and t such that $as + bt = 1$.
Proposition 4.5.5	For any integers a, b, not both zero, if c is a common divisor of a and b, then $c \mid gcd(a, b)$.
Definition 4.6.1	The **least common multiple** of two nonzero integers a and b, denoted **lcm*(a, b)***, is the positive integer c such that 1. $a \mid c$ and $b \mid c$; 2. for all positive integers m, if $a \mid m$ and $b \mid m$, then $c \leq m$.
Definition 4.7.1	Let m and n be integers and let d be a positive integer. We say that ***m* is congruent to *n* modulo *d*** and write $$m \equiv n \pmod{d}$$ if, and only if, $d \mid (m - n)$. Symbolically: $m \equiv n \pmod{d} \Leftrightarrow d \mid (m - n)$
Theorem 8.4.1 (Epp)	Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent: 1. $n \mid (a - b)$; 2. $a \equiv b \pmod{n}$; 3. $a = b + kn$ for some integer k; 4. a and b have the same (nonnegative) remainder when divided by n; 5. $a \bmod n = b \bmod n$.
Theorem 8.4.3 (Epp)	Let a, b, c, d, and n be integers with $n > 1$, and suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then 1. $(a + b) \equiv (c + d) \pmod{n}$ 2. $(a - b) \equiv (c - d) \pmod{n}$ 3. $ab \equiv cd \pmod{n}$ 4. $am \equiv cm \pmod{n}$ for all integers m.
Corollary 8.4.4 (Epp)	Let a, b, and n be integers with $n > 1$. Then $$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$ or, equivalently, $$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$ In particular, if m is a positive integer, then $$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$
Definition 4.7.2	For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is called the multiplicative inverse of a modulo n. We may write the inverse as a^{-1}. Because the commutative law still applies in modulo arithmetic, we also have $a^{-1}a \equiv 1 \pmod{n}$.
Theorem 4.7.3	For any integer a, its multiplicative inverse modulo n (where $n > 1$), a^{-1}, exists if, and only if, a and n are coprime.
Corollary 4.7.4	If $n = p$ is a prime number, then all integers a in the range $0 < a < p$ have multiplicative inverses modulo p.
Theorem 8.4.8 (Epp)	For all integers a, b, and c, if gcd$(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

Theorem 8.4.9 (Epp)	For all integers a, b, c, and n with $n>1$, if gcd$(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.
Theorem 8.4.10 (Epp)	If p is any prime number and a is any integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

2. Proof Strategy

Proof of existence by construction	A statement in the form $\exists x \in D$ such that $Q(x)$ is true if, and only if, $Q(x)$ is true for at least one x in D.
Proof of existence by non-construction	It shows either (a) that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem or (b) that the assumption that there is no such x leads to a contradiction.
Disproof by counter-example	To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample.**
Proof by exhaustion	To elaborate that every possible case of this statement is true.
Proof by Generalizing from Generic Particular	To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.
Method of Direct Proof	1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.) 2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.") 3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.
Proof by division into cases	To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C," prove all of the following: If A_1, then C, If A_2, then C, ... If A_n, then C. This process shows that C is true regardless of which of A_1, A_2,..., A_n happens to be the case.
Proof by Contradiction	1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true. 2. Show that this supposition leads logically to a contradiction. 3. Conclude that the statement to be proved is true.
Proof by Contraposition	1. Express the statement to be proved in the form $\forall x$ in D, if $P(x)$ then $Q(x)$. (This step may be done mentally.) 2. Rewrite this statement in the contrapositive form $\forall x$ in D, if $Q(x)$ is false then $P(x)$ is false. (This step may also be done mentally.) 3. Prove the contrapositive by a direct proof. a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false. b. Show that $P(x)$ is false.
Proof by Mathematical Induction	Consider a statement of the form, "For all integers $n \geq a$, a property $P(n)$ is true." To prove such a statement, perform the following two steps:

	Step 1 (basis step): Show that $P(a)$ is true. Step 2 (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. To perform this step, **suppose** that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$. *[This supposition is called the* ***inductive hypothesis.****]* Then **show** that $P(k+1)$ is true.
Proof by strong Mathematical Induction	Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true: 1. $P(a), P(a+1), \ldots,$ and $P(b)$ are all true. **(basis step)** 2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. **(inductive step)** Then the statement for all integers $n \geq a$, $P(n)$ is true. (The supposition that $P(i)$ is true for all integers i from a through k is called the **inductive hypothesis.** Another way to state the inductive hypothesis is to say that $P(a), P(a+1), \ldots, P(k)$ are all true.)
Universal Instantiation	If some property is true of *everything* in a set, then it is true of *any particular* thing in the set.
Existential Instantiation	If the existence of a certain kind of object is assumed or has been deduced then it can be given a name, as long as that name is not currently being used to denote something else.

3. Prime Numbers Table

Below are 168 prime numbers in the range (1, 1000).

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997

4. Set Theory

Theorem 6.2.1	1. *Inclusion of Intersection:* For all sets A and B, (a) $A \cap B \subseteq A$ and (b) $A \cap B \subseteq B$. 2. *Inclusion in Union:* For all sets A and B, (a) $A \subseteq A \cup B$ and (b) $B \subseteq A \cup B$. 3. *Transitive Property of Subsets:* For all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
Theorem 6.2.2	Let all sets referred to below be subsets of a universal set U. 1. *Commutative Laws:* For all sets A and B, (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$. 2. *Associative Laws:* For all sets A, B, and C, (a) $(A \cup B) \cup C = A \cup (B \cup C)$ and (b) $(A \cap B) \cap C = A \cap (B \cap C)$. 3. *Distributive Laws:* For all sets, A, B, and C, (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

	4. *Identity Laws:* For all sets A, (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$. 5. *Complement Laws:* (a) $A \cup A^c = U$ and (b) $A \cap A^c = \emptyset$. 6. *Double Complement Law:* For all sets A, $(A^c)^c = A$. 7. *Idempotent Laws:* For all sets A, (a) $A \cup A = A$ and (b) $A \cap A = A$. 8. *Universal Bound Laws:* For all sets A, (a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$. 9. *De Morgan's Laws:* For all sets A and B, (a) $(A \cup B)^c = A^c \cap B^c$ and (b) $(A \cap B)^c = A^c \cup B^c$. 10. *Absorption Laws:* For all sets A and B, (a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$. 11. *Complements of U and* $\emptyset$: (a) $U^c = \emptyset$ and (b) $\emptyset^c = U$. 12. *Set Difference Law:* For all sets A and B, $A - B = A \cap B^c$.
Theorem 6.2.3	For any sets A and B, if $A \subseteq B$, then (a) $A \cap B = A$ and (b) $A \cup B = B$.

5. Probability theory

6. Graph Theory