CS 201: Discrete Math for Computer Science
2017 Fall Semester
Written Assignments # 1 – # 5 Solutions

P14, Ex. 14. Let p, q and r be the propositions
p: You get an A on the final exam.
q: You do every exercise in this book.
r: You get an A in this class.
Write these propositions using p, q, and r and logical connectives (including negations).

a) You get an A in this class, but you do not do every exercise in this book.

b) You get an A on the final, you do every exercise in this book, and you get an A in this class.

c) To get an A in this class, it is necessary for you to get an A on the final.

d) You get an A on the final, but you don't do every exercise in this book; nevertheless, you get an A in this class.

e) Getting an A on the final and doing every exercise in this book is suffcient for getting an A in this class.

f) You will get an A in this class if and only if you either do every exercise in this book or you get an A on the final.

Solution:

a) $r \wedge \neg q$

b) $p \wedge q \wedge r$

c) $r \rightarrow p$

d) $p \wedge \neg q \wedge r$

e) $(p \wedge q) \rightarrow r$

f) $r \leftrightarrow (q \vee p)$

□

P15, Ex. 34 **b) d) f).** Construct a truth table for each of these compound propositions.

b) $p \oplus \neg p$

d) $\neg p \oplus \neg q$

f) $(p \oplus q) \wedge (p \oplus \neg q)$

Solution:

b)

p	$\neg p$	$(p \oplus \neg p)$
T	F	T
F	T	T

d)

p	q	$\neg p$	$\neg q$	$\neg p \oplus \neg q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	F

f)

p	q	$p \oplus q$	$p \oplus \neg q$	$(p \oplus q) \wedge (p \oplus \neg q)$
T	T	F	T	F
T	F	T	F	F
F	T	T	F	F
F	F	F	T	F

□

P16, Ex. 40 Explain, without using a truth table, why $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ is true, when p, q, and r have the same truth value and it is false otherwise.

Solution: The statement is true if and only if all the three clauses, $p \vee \neg q$, $q \vee \neg r$, and $r \vee \neg p$ are true. Suppose that p, q and r are all true, or all false, it is checked that each clause is true, and the statement is true. On the other hand, if one of the variables is true, and the other two false, then the clause containing the negation of that variable will be false, making the

entire conjunction false. Similarly, if one of the variable is false and the other two true, then the clause containing that variable unnegated will be false, again making the entire statement false.

□

P35, Ex. 26 Show that $\neg p \to (q \to r)$ and $q \to (p \vee r)$ are logically equivalent.
Solution: The second statement is false only when q is true and $p \vee r$ is false, which means both p and r are false.

The first statement if false only when $\neg p$ is true, and $q \to r$ is false. This only happens when p is false, and q is true, r is false.

Thus, these two statements are logically equivalent.

□

P35, Ex. 30 Show that $(p \vee q) \wedge (\neg p \vee r) \to (q \vee r)$ is a tautology.
Solution: The conclusion $q \vee r$ is true except when both q and r are false. But if q and r are both false, then one of $p \vee q$ or $\neg p \vee r$ is false, because one of p or $\neg p$ is false. Thus in this case the hypothesis $(p \vee q) \wedge (\neg p \vee r)$ is false. An conditional statement in which the conclusion is true or the hypothesis is false is true, and this completes the proof.

□

P35, Ex. 32 Show that $(p \wedge q) \to r$ and $(p \to r) \wedge (q \to r)$ are not logically equivalent.
Solution: What we need only is to find an assignment of truth values such that one of these propositions is true and the other false. Let p be true, and the other two be false. Then the first statement will be $F \to F$, which is true. But, the other will be $F \wedge T$, which is false.

□

P53, Ex. 9 Let $P(x)$ be the statement "x can speak Russian" and let $Q(x)$ be the statement "x knows the computer language C++". Express each of these sentences in terms of $P(x)$, $Q(x)$, quantifiers, and logical connectives. The domain for quantifiers consists of all students at your school.

a) There is a student at your school who can speak Russian and who knows C++.

b) There is a student at your school who can speak Russian but who doesn't know C++.

c) Every student at your school either can speak Russian or knows C++.

d) No student at your school can speak Russian or knows C++.

Solution:

a) $\exists x(P(x) \wedge Q(x))$

b) $\exists x(P(x) \wedge \neg Q(x))$

c) $\forall x(P(x) \vee Q(x))$

d) $\forall x \neg (P(x) \vee Q(x))$

□

P65, Ex. 10 Let $F(x, y)$ be the statement "x can fool y", where the domain consists of all people in the world. Use quantifiers to express each of these statement.

a) Everybody can fool Fred.

b) Evelyn can fool everybody.

c) Everybody can fool somebody.

d) There is no one who can fool everybody.

e) Everyone can be fooled by somebody.

f) No one can fool both Fred and Jerry.

g) Nancy can fool exactly two people.

h) There is exactly one person whom everybody can fool.

i) No one can fool himself or herself.

j) There is someone who can fool exactly one person besides himself or herself.

Solution:

a) $\forall x F(x, \text{Fred})$

b) $\forall y F(\text{Evelyn}, y)$

c) $\forall x \exists y F(x, y)$

d) $\neg \exists x \forall y F(x, y)$

e) $\forall y \exists x F(x, y)$

f) $\neg \exists x (F(x, \text{Fred}) \wedge F(x, \text{Jerry}))$

g) $\exists y_1 \exists y_2 (F(\text{Nancy}, y_1) \wedge F(\text{Nancy}, y_2) \wedge y_1 \neq y_2 \wedge \forall y (F(\text{Nancy}, y) \rightarrow (y = y_1 \vee y = y_2)))$

h) $\exists y (\forall x F(x, y) \wedge \forall z (\forall x F(x, z) \rightarrow z = y))$

i) $\neg \exists x F(x, x)$

j) $\exists x \exists y (x \neq y \wedge F(x, y) \wedge \forall z ((F(x, z) \wedge z \neq x) \rightarrow z = y))$

□

P67, Ex. 30 Rewrite each of these statements so that negations appear only within predicates (that is, so that no negation is outside a quantifier or an expression involving logical connectives).

a) $\neg \exists y \exists x P(x, y)$

c) $\neg \exists y (Q(y) \wedge \forall x \neg R(x, y))$

e) $\neg \exists y (\forall x \exists z T(x, y, z) \vee \exists x \forall z U(x, y, z))$

Solution:

a) $\forall y \forall x \neg P(x, y)$

c) $\forall y (\neg Q(y) \vee \exists x R(x, y))$

d) $\forall y(\exists x \forall z \neg T(x, y, z) \wedge \forall x \exists z \neg U(z, y, z)$

□

P79, Ex. 13 For each of these arguments, explain which rules of inference are used for each step.

a) "Doug, a student in this class, knows how to write programs in JAVA. Everyone who knows how to write programs in JAVA can get a high-paying job. Therefore, someone in this class can get a high-paying job."

c) "Each of the 93 students in this class owns a personal computer. Everyone who owns a personal computer can use a word processing program. Therefore, Zeke, a student in this class, can use a word processing program."

Solution:

a) Let $c(x)$ be "x is in this class", $j(x)$ denote "x knows how to wirte programs in JAVA", and $h(x)$ be "x can get a high-paying job". The premises are $c(Doug)$, $j(Doug)$, $\forall x(j(x) \rightarrow h(x))$. Using universal instantiation and the last premise, $j(Doug) \rightarrow h(Doug)$ follows. Applying modus ponens to this conclusion and the second premise, $h(Doug)$ follows. Using conjunction and the first premise, $c(Doug) \wedge h(Doug)$ follows. Finaly, using existential generalization, the desired conclusion, $\exists x(c(x) \wedge h(x))$ follows.

c) Let $c(x)$ be "x is in this class," $p(x)$ be "x owns a PC", and $w(x)$ be "x can use a word-processing program". The premises are $c(Zeke)$, $\forall x(c(x) \rightarrow p(x))$, and $\forall x(p(x) \rightarrow w(x))$. Using the second premise and universal instantiation and modus ponens, $c(Zeke) \rightarrow p(Zeke)$ follows. Using the first premise and modus ponens, $p(Zeke)$ follows. Using the third premise and universal instantiation, $p(Zeke) \rightarrow w(Zeke)$ follows. Finally, using modus ponens, $w(Zeke)$, the desired conclusion follows.

□

P79, Ex. 14 For each of these arguments, explain which rules of inference are used for each step.

b) "Each of five roommates, Melissa, Aaron, Ralph, Veneesha, and Keeshawn, has taken a course in discrete mathematics. Every student who has taken a course in discrete mathematics can take a course in algorithms. Therefore, all five roommates can take a course in algorithms next year."

d) "There is someone in this class who has been to France. Everyone who goes to France visits the Louvre. Therefore, someone in this class has visited the Louvre."

Solution:

b) Let $r(x)$ be "r is one of the five roommates listed", let $d(x)$ be "x has taken a course in discrete mathematics", and let $a(x)$ be "x can take a course in algorithms". We are given premises $\forall x(r(x) \rightarrow d(x)$, $\forall x(d(x) \rightarrow a(x)$, and we want to conclude $\forall x(r(x) \wedge a(x))$.

Step	**Reason**
1. $\forall x(r(x) \rightarrow d(x))$	Hypothesis
2. $r(y) \rightarrow d(y)$	Universal Instantiation using 1.
3. $\forall x(d(x) \rightarrow a(x))$	Hypothesis
4. $d(y) \rightarrow a(y)$	Universal instantiation using 3.
5. $r(y) \rightarrow a(y)$	Hypothetical syllogism using 2. and 4.
6. $\forall x(r(x) \rightarrow a(x))$	Universal generalization using 5.

d) Let $c(x)$ be "x is in this class," let $f(x)$ be "x has been to France", and let $l(x)$ be "x has visited the Louvre". We are given premises $\exists x(c(x) \wedge f(x))$, $\forall x(f(x) \wedge l(x))$, and we want to conclude $\exists x(c(x) \wedge l(x))$.

Step	**Reason**
1. $\exists x(c(x) \wedge f(x))$	Hypothesis
2. $c(y) \wedge f(y)$	Existential Instantiation using 1.
3. $f(y)$	Simplification using 2.
4. $c(y)$	Simplification using 2.
5. $\forall x(f(x) \rightarrow l(x))$	Hypothesis
6. $f(y) \rightarrow l(y)$	Universal instantiation using 5.
7. $l(y)$	Modus ponens using 3. and 6.
8. $c(y) \wedge l(y)$	Conjunction using 4. and 7.
9. $\exists x(c(x) \wedge l(x))$	Existential generalization using 8.

□

P91**, Ex.** 26 Prove that if n is a positive integer, then n is even if and only if $7n + 4$ is even.
Solution: First, we directly prove that if n is even then $7n + 4$ is even. Since n is even, it can be written as $2k$ for some integer k. Then $7n + 4 = 14k + 4 = 2(7k + 2)$, which is even. Conversely, we prove by contrapositive that if $7n + 4$ is even then n is even. Suppose that n is odd, i.e., $n = 2k + 1$ for some integer k. Then $7n + 4 = 14k + 11 = 2(7k + 5) + 1$, which is odd.

□

P108**, Ex.** 7 Prove the **triangle inequality**, which states that if x and y are real numbers, then $|x| + |y| \geq |x + y|$ (where $|x|$ represents the absolute value of x, which equals x if $x \geq 0$ and equals $-x$ if $x < 0$.
Solution: We prove by four cases.

Case 1: $x \geq 0$ and $y \geq 0$. Then $|x| + |y| = x + y = |x + y|$.

Case 2: $x < 0$ and $y < 0$. Then $|x| + |y| = -x + (-y) = -(x + y) = |x + y|$.

Case 3: $x \geq 0$ and $y < 0$. Then $|x| + |y| = x + (-y)$. If $x \geq -y$, then $|x + y| = x + y$. But because $y < 0$, $-y > y$, so $|x| + |y| = x + (-y) > x + y = |x + y|$. If $x < -y$, then $|x + y| = -(x + y)$. But because $x < 0$, $x \geq -x$, so $|x| + |y| = x + (-y) \geq -x + (-y) = |x + y|$.

Case 4: $x < 0$ and $y \geq 0$. Similar to Case 3.

□

P108**, Ex.** 14 Prove or disprove that if a and b are rational numbers, then a^b is also rational. .
Solution: Take $a = 2$ and $b = 1/2$. Then $a^b = 2^{1/2} = \sqrt{2}$, and this number is not rational.

□

P109**, Ex.** 34 Prove that $\sqrt[3]{2}$ is irrational.
Solution: Suppose that $\sqrt[3]{2}$ is the rational number p/q, where p and q are positive integers with no common factors. Cubing both sides, we have

$2 = p^3/q^3$, or $p^3 = 2q^3$. Thus p^3 is even. Since the product of odd number is odd, this means that p is even, so we can write $p = 2k$ for some integer k. We then have $q^3 = 4k^3$. Since q^3 is even, q must be even. We have now seen that both p and q are even, a contradiction.

□

P109**, Ex.** 36 Prove that between every rational number and every irrational number there is an irrational number.
Solution: The average of two different numbers is certainly always between the two numbers. Furthermore, the average a of rational number x and irrational number y must be irrational, because the equation $a = (x + y)/2$ leads to $y = 2a - x$, which would be rational if a were rational.

□

P126**, Ex.** 45**.** The defining property of an ordered pair is that two ordered pairs are equal if and only if their first elements are equal and their second elements are equal. Surprisingly, instead of taking the ordered pair as a primitive concept, we can construct ordered pairs using basic notions from set theory. Show that if we define the ordered pair (a, b) to be $\{\{a\}, \{a, b\}\}$, then $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.
Solution: This is an if and only if condition. The "if" part is immediate. For the "only if" part, assume these two sets $\{\{a\}, \{a, b\}\}$ and $\{\{c\}, \{c, d\}\}$ are equal. First, consider the case when $a \neq b$. Then $\{\{a\}, \{a, b\}\}$ contains exactly two elements, one of which contains one elements. Thus, the set $\{\{c\}, \{c, d\}\}$ must have the same property, so $c \neq d$ and $\{c\}$ is the element containing exactly one element. Hence, $\{a\} = \{c\}$, which implies that $a = c$. Moreover, the two-element sets $\{a, b\}$ and $\{c, d\}$ must be equal. Because $a = c$ and $a \neq b$, it follows that $b = d$.

Second, suppose that $a = b$. Then $\{\{a\}, \{a, b\}\} = \{\{a\}\}$, a set with one element. Hence $\{\{c\}, \{c, d\}\}$ has only one element, which can happen only when $c = d$, and the set if $\{\{c\}\}$. It then follows that $a = c$ and $b = d$.

□

P137**, Ex.** 40**.** Determine whether the symmetric difference is associative; that is, if A, B and C are sets, does it follow that $A \oplus (B \oplus C) = (A \oplus B) \oplus C$?

Solution:

Using membership table, one can show that each side consists of the elements that are in an odd number of the sets A, B and C. Thus, it follows.

□

P137**, Ex.** 41**.** Suppose that A, B and C are sets such that $A \oplus C = B \oplus C$. Must it be the case that $A = B$?

Solution:

Yes. We prove that for every element $x \in A$, we have $x \in B$ and vice versa.

First, for elements $x \in A$ and $x \notin C$, since $A \oplus C = B \oplus C$, we know that $x \in A \oplus C$ and thus $x \in B \oplus C$. Since $x \notin C$, we must have $x \in B$. For elements $x \in A$ and $x \in C$, we have $x \notin A \oplus C$. Thus, $x \notin B \oplus C$. Since $x \in C$, we must have $x \in B$.

The proof of the other way around is similar.

□

P137**, Ex.** 46**.**

Show that if A, B and C are sets, then

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| \\ &- |A \cap C| - |B \cap C| + |A \cap B \cap C|. \end{aligned}$$

Solution:

To count the number of $A \cup B \cup C$ we proceed as follows. First we count the elements in each of the sets and add. This certainly gives us all the elements in the union, but we have overcounted. Each element in $A \cap B$, $A \cap C$, and $B \cap C$ has been counted twice. Therefore we subtract the cardinalities of these intersections to make up for the overcount. Finally, we have compensated a bit too much, since the elements of $A \cap B \cap C$ have now been counted three times and subtracted three times. We adjust by adding back the cardinality of $A \cap B \cap C$.

□

P155, Ex. 70 Suppose that f is an invertible function from Y to Z and g is an invertible function from X to Y. Show that the inverse of the composition $f \circ g$ is given by $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Solution:

This follows directly from the definition. We want to show that

$$\begin{aligned}
&((f \circ g) \circ (g^{-1} \circ f^{-1}))(z) \\
&= (f \circ g)((g^{-1} \circ f^{-1})(z)) \\
&= (f \circ g)(g^{-1}(f^{-1}(z))) \\
&= f(g(g^{-1}(f^{-1}(z)))) \\
&= f(f^{-1}(z)) \\
&= z.
\end{aligned}$$

The second equality is similar.

□

P155, Ex. 76 Let x be a real number. Show that $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$.

Solution:

Certainly every real number x lies in an interval $[n, n+1)$ for some integer n; indeed $n = \lfloor x \rfloor$.

- if $x \in [n, n + \frac{1}{3})$, then $3x$ lies in the interval $[3n, 3n + 1)$, so $\lfloor 3x \rfloor = 3n$. Moreover in this case $x + \frac{1}{3}$ is still less than $n + 1$, and $x + \frac{2}{3}$ is still less than $n + 1$. So, $\lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor = n + n + n = 3n$ as well.
- if $x \in [n + \frac{1}{3}, n + \frac{2}{3})$, then $3x \in [3n + 1, 3n + 2)$, so $\lfloor 3x \rfloor = 3n + 1$. Moreover in this case $x + \frac{1}{3}$ is in $[n + \frac{2}{3}, n + 1)$, and $x + \frac{2}{3}$ is in $[n + 1, n + \frac{4}{3})$, so $\lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor = n + n + (n + 1) = 3n + 1$ as well.
- if $x \in [n + \frac{2}{3}, n + 1)$, similar and both sides equal $3n + 2$.

□

P155, Ex. 80 Show that a set S is infinite if and only if there is a proper subset A of S such that there is a one-to-one correspondence between A and S.

Solution:

- "only if" part: Let S be the given infinite set. Clearly S is not empty, because by definition, the empty set has cardinality 0, a nonnegative integer. Let a_0 be one element of S, and let $A = S - \{a_0\}$. Clearly, A is also infinite (because if it were finite, then we would have $|S| = |A| + 1$, making S finite). We will now construct a one-to-one correspondence between S and A; think of this as a one-to-one and onto function f from S to A. In order to define $f(a_0)$, we choose an arbitrary element a_1 in A (which is possible because A is infinite) and set $f(a_0) = a_1$. Next we define f at a_1. To do so, we choose an arbitrary element a_2 in $A - \{a_1\}$ (which is possible because $A - \{a_1\}$ is necessarily infinite) and set $f(a_1) = a_2$. Next we define f at a_2. To do so, we choose an arbitrary element a_3 in $A - \{a_1, a_2\}$ (which is possible because $A - \{a_1, a_2\}$ is necessarily infinite) and set $f(a_2) = a_3$. We continue this process forever. Finally, we let f be the identity function on $S - \{a_0, a_1, a_2, \ldots\}$. The function thus defined has $f(a_i) = a_{i+1}$ for all natural numbers i and $f(x) = x$ for all $x \in S - \{a_0, a_1, a_2, \ldots\}$. Our construction forced f to be one-to-one and onto.

- "if" part: If S is a finite set, with cardinality m, then every proper subset of S has cardinality strictly smaller than m. Thus, there is no possible one-to-one correspondence between the elements of S and the elements of the proper subsets.

□

P169, Ex. 35 Show that $\sum_{j=1}^{n}(a_j - a_{j-1}) = a_n - a_0$, where $a_0, a_1, \ldots, a_n$ is a sequence of real numbers. This type of sum is called **telescoping**.
Solution: Straightforward.

□

P169, Ex. 38

Use the technique given in Ex. 35, together with the result of Ex. 37*b*, to derive the formula for $\sum_{k=1}^{n} k^2$ given in Table 2.
Solution:

First we note that $k^3 - (k-1)^3 = 3k^2 - 3k + 1$. Then we sum this equation for all values of k from 1 to n. On the left, because of telescoping, we have

just n^3; on the right we have

$$3\sum_{k=1}^{n} k^2 - 3\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1 = 3\sum_{k=1}^{n} k^2 - \frac{3n(n+1)}{2} + n.$$

Equating the two sides and solving for $\sum_{k=1}^{n} k^2$, we obtain

$$\begin{aligned}
\sum_{k=1}^{n} k^2 &= \frac{1}{3}\left(n^3 + \frac{3n(n+1)}{2} - n\right) \\
&= \frac{n}{3}\left(\frac{2n^2+3n+3-2}{2}\right) \\
&= \frac{n}{3}\left(\frac{2n^2+3n+1}{2}\right) \\
&= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

□

P169, Ex. 41 Find a formula for $\sum_{k=0}^{m} \lfloor \sqrt{k} \rfloor$, when m is a positive integer.
Solution:

By the definition of the floor function, there are $2n+1$ n's in the summation. Let $n = \lfloor \sqrt{m} \rfloor - 1$. Then

$$\begin{aligned}
&\sum_{k=0}^{m} \lfloor \sqrt{k} \rfloor \\
&= \sum_{i=1}^{n} (2i^2 + i) + (n+1)(m - (n+1)^2 + 1) \\
&= 2\sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i + (n+1)(m - (n+1)^2 + 1) \\
&= \frac{n(n+1)(2n+1)}{3} + \frac{n(n+1)}{2} + (n+1)(m - (n+1)^2 + 1)
\end{aligned}$$

□

P176, Ex. 16 Show that a subset of a countable set is also countable.

Solution:

If a set A is countable, then we can list its elements, $a_1, a_2, a_3, \ldots, a_n, \ldots$ (possibly ending after a finite number of terms). Every subset of A consists of some (or none or all) of the items in this sequence, and we can list them in the same order in which they appear in the sequence. This gives us a sequence (again, infinite or finite) listing all the elements of the subset. Thus the subset is also countable.

□

P176**, Ex.** 17

If A is an uncountable set and B is a countable set, must $A - B$ be uncountable?

Solution:

Since $A = (A - B) \cup (A \cap B)$, if $A - B$ is countable, the elements of A can be listed in a sequence by alternating elements of $A - B$ and elements of $A \cap B$. This contradicts the uncountability of A.

□

P203**, Ex.** 49

Express the binary insertion sort in pseudocode.

Solution:

□

P217**, Ex.** 44

Suppose that $f(x), g(x)$ and $h(x)$ are functions such that $f(x)$ is $\Theta(g(x))$ and $g(x)$ is $\Theta(h(x))$. Show that $f(x)$ is $\Theta(h(x))$.

Solution:

The definition of "$f(x)$ is $\Theta(g(x))$" is that $f(x)$ if both $O(g(x))$ and $\Omega(g(x))$. This means that there are positive constants C_1, k_1, C_2, and k_2 such that $|f(x)| \leq C_2|g(x)|$ for all $x > k_2$ and $|f(x) \geq C_1|g(x)|$ for all $x > k_1$. Similarly, we have that there are positive constants C_1', k_1', C_2', and k_2' such that $|g(x)| \leq C_2'|h(x)|$ for all $x > k_2'$ and $|g(x)| \geq C_1'|h(x)|$ for all $x > k_1'$. We can combine these inequalities to obtain $|f(x)| \leq C_2C_2'|h(x)|$ for all $x > \max(k_2, k_2')$ and $|f(x)| \geq C_1C_1'|h(x)|$ for all $x > \max(k_1, k_1')$. This means that $f(x)$ is $\Theta(h(x))$.

Algorithm 1 binary insertion sort ($a_1, a_2, \ldots, a_n$: real numbers with $n \geq 2$)

```
for j := 2 to n do
  left := 1
  right := j − 1
  while left < right do
      middle := ⌊(left + right)/2⌋
    if a_j > a_middle then
      left := middle + 1
    else
      right := middle
    end if
  end while
  if a_j < a_left then
    {insert a_j in location i by moving a_i through a_{j−1} towards back of
    list}
    i := left
  else
    i := left + 1
  end if
  m := a_j
  for k := 0 to j − i − 1 do
    a_{j−k} := a_{j−k−1}
  end for
  a_i := m
end for
```

□

P217, Ex. 45

If $f_1(x)$ and $f_1(x)$ are functions from the set of positive integers to the set of positive real numbers and $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$, is $(f_1 - f_2)(x)$ also $\Theta(g(x))$? Either prove that it is or give a counter example.

Solution:

This is false. Let $f_1 = 2x^2 + 3x$, $f_2 = 2x^2 + 2x$ and $g(x) = x^2$.

□

P217, Ex. 50

Show that if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_{n-1}$, and a_n are real numbers and $a_n \neq 0$, then $f(x)$ is $\Theta(x^n)$.

Solution:

We need to show inequalities in both ways. First, we show that $|f(x)| \leq Cx^n$ for all $x \geq 1$ in the following. Noting that $x^i \leq x^n$ for such values of x whenever $i < n$. We have the following inequalities, where M is the largest of the absolute values of the coefficients and $C = (n+1)M$:

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\ &\leq |a_n|x^n + |a_{n-1}|x^{n-1} + \cdots + |a_1|x + |a_0| \\ &\leq |a_n|x^n + |a_{n-1}|x^n + \cdots + |a_1|x^n + |a_0|x^n \\ &\leq Mx^n + Mx^n + \cdots + Mx^n \\ &= Cx^n. \end{aligned}$$

For the other direction, let k be chosen larger than 1 and larger than $2nm/|a_n|$, where m is the largest of the absolute values of the a_i's for $i < n$. Then each a_{n-i}/x^i will be smaller than $|a_n|/2n$ in absolute value for all $x > k$. Now we have for all $x > k$,

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\ &= x^n \left| a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n} \right| \\ &\geq x^n |a_n/2|. \end{aligned}$$

□

P218**, Ex.** 71

Show that $n \log n$ is $O(\log n!)$.

Solution:

Note that $(n-i)(i+1) \geq n$ for $i = 0, 1, \ldots, n-1$. Hence, we have

$$(n!)^2 = (n \cdot 1) \cdot ((n-1) \cdot 2) \cdot ((n-1) \cdot 3) \cdot \cdots \cdot (2 \cdot (n-1)) \cdot (1 \cdot n) \geq n^n.$$

Therefore, $2 \log n! \geq n \log n$.

□

P229**, Ex.** 10

a) Show that this algorithm determines the number of 1 bits in the bit string S:

Algorithm 2 bit count (S: bit string)

count := 1
while $S \neq 0$ **do**
  count := *count* + 1
  $S := S \wedge (S-1)$
end while
return *count* {*count* is the number of 1's in S}

Here $S-1$ is the bit string obtained by changing the rightmost 1 bit of S to a 0 and all the 0 bits to the right of this to 1's. [Recall that $S \wedge (S-1)$ is the bitwise AND of S and $S-1$.]

b) How many bitwise AND operations are needed to find the number of 1 bits in a string S using the algorithm in part a)?

Solution:

a) By the way that $S-1$ is defined, it is clear that $S \wedge (S-1)$ is the same as S except that the rightmost 1 bit has been changed to a 0. Thus, we add 1 to *count* for every one bit (since we stop as soon as $S = 0$, i.e., as soon as S consists of just 0 bits.)

b) Obviously, the number of bitwise AND operations is equal to the final value of *count*, i.e., the number of one bits in S.

□

P230, Ex. 13 The conventional algorithm for evaluating a polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ at $x = c$ can be expressed in pseudocode by where

Algorithm 3 polynomial ($c, a_0, a_1, \ldots, a_n$: real numbers)

```
power := 1
y := a_0
for i := 1 to n do
   power := power * c
   y := y + a_i * power
end for
return y {y = a_n c^n + a_{n-1} c^{n-1} + ··· + a_1 c + a_0}
```

the final value of y is the value of the polynomial at $x = c$.

b) Exactly how many multiplications and additions are used to evaluate a polynomial of degree n at $x = c$? (Do not count additions used to increment the loop variable).

Solution:

b) $2n$ multiplications and n additions.

□

P230, Ex. 14 There is a more efficient algorithm (in terms of the number of multiplications and additions used) for evaluating polynomials than the conventional algorithm described in the previous exercise. It is called **Horner's method**. This pseudocode shows how to use this method to find the value of $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ at $x = c$.

b) Exactly how many multiplications and additions are used by this algorithm to evaluate a polynomial of degree n at $x = c$? (Do not count additions used to increment the loop variable.)

Algorithm 4 Horner ($c, a_0, a_1, \ldots, a_n$: real numbers)

```
y := a_n
for i := 1 to n do
   y := y * c + a_{n-i}
end for
return y {y = a_n c^n + a_{n-1} c^{n-1} + ··· + a_1 c + a_0}
```

Solution:

b) n multiplications and n additions.

□

P245, Ex. 37. Find counterexamples to each of these statements about congruences.

a) If $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

Solution:

a) Let $m = c = 2$, $a = 0$ and $b = 1$. Then $0 = ac \equiv bc = 2 \pmod{2}$, but $0 = a \not\equiv b = 1 \pmod{2}$.

b) Let $m = 5$, $a = b = 3$, $c = 1$, and $d = 6$. Then $3 \equiv 3 \pmod{5}$ and $1 \equiv 6 \pmod{5}$, but $3^1 = 3 \not\equiv 4 \equiv 729 = 3^6 \pmod{5}$.

□

P245, Ex. 38. Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod{4}$.
Solution: There are two cases. If n is even, then $n = 2k$ for some integer k, so $n^2 = 4k^2$, which means that $n^2 \equiv 0 \pmod{4}$. If n is odd, then $n = 2k + 1$ for some integer k, so $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, which means that $n^2 \equiv 1 \pmod{4}$.

□

P245, Ex. 39. Use Exercise 38 to show that if m is a positive integer of the form $4k + 3$ for some nonnegative integer k, then m is not the sum of the squares of two integers.

Solution:

BY Exercise 38, the sum of two squares must be either $0+0 = 0$, $0+1 = 1$, or $1 + 1 = 2$, modulo 4, never 3, and therefore not of the form $4k + 3$.

□

P255, Ex. 2.

Convert the decimal expansion of each of these integers to a binary expansion. a) 321 b) 1023 c) 100632

Solution:

a) 101000001

b) 1111111111

c) 11000100100011000

□

P255, Ex. 26.

Use Algorithm 5 to find $11^{644} \bmod 645$.

Solution:

The algorithm computes $11 \bmod 645$, $11^2 \bmod 645$, $11^4 \bmod 645$, $11^8 \bmod 645$, $11^{16} \bmod 645$, ..., and then multiplies (mod645) the required values. Since $644 = (1010000100)_2$, we need to multiply together $11^4 \bmod 645$, $11^{128} \bmod 645$, and $11^{512} \bmod 645$, reducing modulo 645 at each step. We compute by repeatedly squaring: $11^2 \bmod 645 = 121$, $11^4 \bmod 645 = 121^2 \bmod 645 = 451$, $11^8 \bmod 645 = 451^2 \bmod 645 = 226$, $11^{16} \bmod 645 = 226^2 \bmod 645 = 121$. At this point we notice that 121 appeared earlier in our calculation, so we have $11^{32} \bmod 645 = 121^2 \bmod 645 = 451$, $11^{64} \bmod 645 = 451^2 \bmod 645 = 226$, $11^{128} \bmod 645 = 226^2 \bmod 645 = 121$, $11^{256} \bmod 645 = 451$, $11^{512} \bmod 645 = 226$. Thus, our final answer will be the product of $451, 121$, and 226, reduced modulo 645. We compute these one at a time: $451 \cdot 121 \bmod 645 = 54571 \bmod 645 = 391$, and $391 \cdot 226 \bmod 645 = 88366 \bmod 645 = 1$. So, $11^{644} \bmod 645 = 1$.

□

P272, Ex. 11

Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number x cannot be written as the ratio of two integers.

Solution:

Suppose that $\log_2 3 = a/b$ where $a, b \in \mathbf{Z}^+$ and $b \neq 0$. Then $2^{a/b} = 3$, so $2^a = 3^b$. This violates the fundamental theorem of arithmetic. Hence $\log_2 3$ is irrational.

□

P272, Ex. 12

Prove that for every positive integer n, there are n consecutive composite integers.

Solution: We follow the hint. There are n numbers in the sequences $(n+1)! + 2$, $(n+1)! + 3$, $\cdots$, $(n+1)! + (n+1)$. The first of these is composite because it is divisible by 2; the second is composite because it is divisible by 3; $\cdots$; the last is composite because it is divisible by $n+1$. This gives us the desired n consecutive composite integers.

□

P273, Ex. 42

Use the extended Euclidean algorithm to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

Solution:

$$4 = \gcd(144, 89) = 17 \cdot 356 + (-24) \cdot 252.$$

□

P274, Ex. 50

Show that if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \bmod m$, then $\gcd(a, m) = \gcd(b, m)$.

Solution:

From $a \equiv b \bmod m$, we know that $b = a + sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a = b - sm$,

and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a, m) = \gcd(b, m)$.

□

P274**, Ex.** 55

Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form $4k + 3$, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes $q_1, q_2, \ldots, q_n$, and consider the number $4q_1q_2 \cdots q_n - 1$.

Solution: Suppose that there are only finitely many primes of the form $4k + 3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on.

Let $Q = 4q_1q_2 \cdots q_n - 1$. Note that Q is of the form $4k + 3$ (where $k = q_1q_2 \cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed.

If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k + 1$ or of the form $4k + 3$, and the product of primes of the form $4k + 1$ is also of this form (because $(4k + 1)(4m + 1) = 4(4km + k + m) + 1$), there must be a factor of Q of the form $4k + 3$ different from the primes we listed.

□

P284**, Ex.** 7

Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m. [Hint: Assume that there two solutions b and c of the congruence $ax \equiv 1 \pmod{m}$. Use Theorem 7 of Section 4.3 to show that $b \equiv c \pmod{m}$.]

Solution:

Suppose that b and c are both the inversed of a modulo m. Then $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Hence, $ba \equiv ca \pmod{m}$. Because $\gcd(a, m) = 1$ it follows by Theorem 7 in Section 4.3 that $b \equiv c \pmod{m}$.

□

P285**, Ex.** 22

Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of back substitution.

Solution:

By definition, the first congruence can be written as $x = 6t + 3$ where t is an integer. Substituting this expression for x into the second congruence tells us that $6t + 3 \equiv 4 \pmod 7$, which can be easily be solved to show that $t \equiv 6 \pmod 7$. From this we can write $t = 7u + 6$ for some integer u. Thus, $x = 6t + 3 = 6 \cdot (7u + 6) + 3 = 42u + 39$. Thus, our answer is all numbers congruent to 39 modulo 42.

□

P286**, Ex.** 39

a) Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

b) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Solution:

a) By Fermat's little theorem we know that $5^6 \equiv 1 \pmod 7$; therefore $5^{1998} = (5^6)^{333} \equiv 1^{75} \equiv 1 \pmod 7$, and so $5^{2003} = 5^5 \cdot 5^{1998} \equiv 3 \cdot 1 = 3 \pmod 7$, so $5^{2003} \bmod 7 = 3$. Similarly, $5^{10} \equiv 1 \bmod 11$; therefore $5^{2000} = (5^{10})^{200} \equiv 1 \pmod{11}$, and so $5^{2003} = 5^3 \cdot 5^{2000} \equiv 4 \pmod{11}$, so $5^{2003} \bmod 11 = 4$. Finally, $5^{12} \equiv 1 \pmod{13}$; therefore $5^{1992} = (5^{12})^{166} \equiv 1 \pmod{13}$, and so $5^{2003} = 5^{11} \cdot 5^{1992} \equiv 8 \pmod{13}$, so $5^{2003} \bmod 13 = 8$.

b) 983

□

P305**, Ex.** 23

Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p - 1)(q - 1)$.

Solution:

Suppose that we know both $n = pq$ and $(p-1)(q-1)$. To find p and q, first note that $(p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. From this we can find $s = p + q$. Then with $n = pq$, we can use the quadratic formula to find p and q.

□

P305**, Ex.** 28

Suppose that (n, e) is an RSA encryption key, with $n = pq$ where p and q are large primes and $\gcd(e, (p-1)(q-1)) = 1$. Furthermore, suppose that d is an inverse of e modulo $(p-1)(q-1)$. Suppose that $C \equiv M^e \pmod{pq}$. In the text we showed that RSA decryption, that is, the congruence $C^d \equiv M \pmod{pq}$ holds when $\gcd(M, pq) = 1$. Show that this decryption congruence also holds when $\gcd(M, pq) > 1$. [Hint: Use congruences modulo p and modulo q and apply the Chinese remainder theorem.]

Solution:

If $M \equiv 0 \pmod{n}$, then $C \equiv M^e \equiv 0 \pmod{n}$ and so $C^d \equiv 0 \equiv M \pmod{n}$. Otherwise, $\gcd(M, p) = p$ and $\gcd(M, q) = 1$, or $\gcd(M, p) = 1$ and $\gcd(M, q) = q$. By symmetry it suffices to consider the first case, where $M \equiv 0 \pmod{p}$. We have $C^d \equiv (M^e)^d \equiv (0^e)^d \equiv 0 \equiv M \pmod{p}$. As in the case considered in the text, $de = 1 + k(p-1)(q-1)$ for some integer k, so

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M \pmod{q}$$

by Fermat's little theorem. Thus by the Chinese remainder theorem, $C^d \equiv M \pmod{pq}$.

□

P305**, Ex.** 30

Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime $p = 101$ and take $a = 2$, which is a primitive root of 101, and that Alice selects $k_1 = 7$ and Bob selects $k_2 = 9$. (You may want to use some computational aid).

Solution:

Alice sends $2^7 \bmod 101 = 27$ to Bob. Bob sends $2^9 \bmod 101 = 7$ to Alice. Alice computes $7^7 \bmod 101 = 90$ and Bob computes $27^9 \bmod 101 = 90$. The shared key is 90.

□

P330, Ex. 25.

Prove that if $h > -1$, then $1 + nh \leq (1 + h)^n$ for all nonnegative integers n. This is called **Bernoulli's inequality**.

Solution:

Let $P(n)$ be "$1 + nh \leq (1 + h)^n$, $h > -1$."

Basic step: $P(0)$ is true because $1 + 0 \cdot h = 1 \leq 1 = (1 + h)^0$.

Inductive step: Assume that $1+kh \leq (1+h)^k$. *Then because* $(1+h) > 0$, $(1+h)^{k+1} = (1+h)(1+h)^k \geq (1+h)(1+kh) = 1+(k+1)h+kh^2 \geq 1+(k+1)h$.

Inductive conclusion: By mathematical induction, we have $P(n)$ is true for all nonnegative integers n.

□

P330, Ex. 26. Suppose that a and b are real numbers with $0 < b < a$. Prove that if n is a positive integer, then $a^n - b^n \leq na^{n-1}(a - b)$.

Solution:

It turns out to be easier to think about the given statement as $na^{n-1}(a - b) \geq a^n - b^n$. The basic step ($n = 1$) is true since $a - b \geq a - b$. Assume that the inductive hypothesis, that $ka^{k-1}(a - b) \geq a^k - b^k$; we must show that $(k + 1)a^k(a - b) \geq a^{k+1} - b^{k+1}$. We have

$$\begin{aligned}(k+1)a^k(a-b) &= k \cdot a \cdot a^{k-1}(a-b) + a^k(a-b) \\ &\geq a(a^k - b^k) + a^k(a-b) \\ &= a^{k+1} - ab^k + a^{k+1} - ba^k.\end{aligned}$$

To complete the proof we want to show that $a^{k+1} - ab^k + a^{k+1} - ba^k \geq a^{k+1} - b^{k+1}$. This inequality is equivalent to $a^{k+1} - ab^k - ba^k + b^{k+1} \geq 0$, which factors into $(a^k - b^k)(a - b) \geq 0$, and this is true, because we are given that $a > b$.

□

P331, Ex. 44.

Prove that if $A_1, A_2, \ldots, A_n$ and B are sets, then

$$\begin{aligned}(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) \\ = \quad (A_1 \cup A_2 \cup \cdots \cup A_n) - B.\end{aligned}$$

Solution:

If $n = 1$, there is nothing to prove, and then $n = 2$, this says that $(A_1 \cap \bar{B}) \cup (A_2 \cap \bar{B}) = (A_1 \cup A_2) \cap \bar{B})$, which is the distributive law. For the inductive step, assume that

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) = (A_1 \cup A_2 \cup \cdots \cup A_n) - B;$$

we must show that

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) \cup (A_{n+1} - B) = (A_1 \cup A_2 \cup \cdots A_n \cup A_{n+1}) - B.$$

We have

$$\begin{aligned}&(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) \cup (A_{n+1} - B) \\ &= \quad ((A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B)) \cup (A_{n+1} - B) \\ &= \quad ((A_1 \cup A_2 \cup \cdots \cup A_n) - B) \cup (A_{n+1} - B) \\ &= \quad (A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}) - B.\end{aligned}$$

The third line follows from the inductive hypothesis, and the fourth line follows from the $n = 2$ case.

□

P341**, Ex.** 4

Let $P(n)$ be the statement that a postage of n cents can be formed using just 4-cent stamps and 7-cent stamps. The parts of this exercise outline a strong induction proof that $P(n)$ is true for $n \geq 18$.

a) Show statements $P(18)$, $P(19)$, $P(20)$ and $P(21)$ are true, completing the basis step of the proof.

b) What is the inductive hypothesis of the proof?

c) What do you need to prove in the inductive step?

d) Complete the inductive step for $k \geq 21$.

e) Explain why these steps show that this statement is true whenever $n \geq 18$.

Solution:

a) $P(18)$ is true, because we can form 18 cents of postage with one 4-cent stamp and two 7-cent stamps. $P(19)$ is true, because we can form 19 cents of postage with three 4-cent stamps and one 7-cent stamp. $P(20)$ is true, because we can form 20 cents of postage with five 4-cent stamps. $P(21)$ is true, because we can form 20 cents of postage with three 7-cent stamps.

b) The inductive hypothesis is the statement that using just 4-cent and 7-cent stamps we can form j cents postage for all j with $18 \leq j \leq k$, where we assume that $k \geq 21$.

c) In the inductive step we must show, assuming the inductive hypothesis, that we can form $k+1$ cents postage using just 4-cent and 7-cent stamps.

d) We want to form $k + 1$ cents of postage. Since $k \geq 21$, we know that $P(k - 3)$ is true, that is, we can form $k - 3$ cents of postage. Put one more 4-cent stamp on the envelope, and we have formed $k + 1$ cents of postage, as desired.

e) We have completed both the basis step and the inductive step, so by the principle of strong induction, the statement is true for every integer n greater than or equal to 18.

□

P344**, Ex.** 37

Let a be an integer and d be a positive integer. Show that the integers q and r with $a = dq + r$ and $0 \leq r < d$, are unique.

Solution:

Assume that $a = dq + r = dq' + r'$ with $0 \leq r < d$ and $0 \leq r' < d$. Then $d(q - q') = r' - r$. It follows that d divides $r - r'$. Because $-d < r' - r < d$, we have $r' - r = 0$. Hence, $r' = r$. It then follows that $q = q'$.

□

P344**, Ex.** 42

Show that the principle of mathematical induction and strong induction are equivalent; that is, each can be shown to be valid from the other.

Solution: The strong induction principle clearly implies ordinary induction, for if one has shown that $P(k) \rightarrow P(k+1)$, then it automatically follows that $[P(1) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$; in other words, strong induction can always be invoked whenever ordinary induction is used.

Conversely, suppose that $P(n)$ is a statement that one can prove using strong induction. Let $Q(n)$ be $P(1) \wedge \cdots \wedge P(n)$. Clearly $\forall n P(n)$ is logically equivalent to $\forall n Q(n)$. We show how $\forall n Q(n)$ can be proved using ordinary induction. First, $Q(1)$ is true because $Q(1) = P(1)$ and $P(1)$ is true by the basis step for the proof of $\forall n P(n)$ by strong induction. Now suppose that $Q(k)$ is true, i.e., $P(1) \wedge \cdots \wedge P(k)$ is true. By the proof of $\forall n P(n)$ by strong induction, it follows that $P(k+1)$ is true. But $Q(k) \wedge P(k+1)$ is just $Q(k+1)$. Thus, we have proved $\forall n Q(n)$ by ordinary induction.

□

P371**, Ex.** 24

Devise a recursive algorithm to find a^{2^n}, where a is a real number and n is a positive integer.

Solution:

We use the hint.

Algorithm 5 twopower (n: positive integer, a: real number)

```
if n = 1 then
  return a^2
else
  return twopower(n − 1, a)^2
end if
```

□

P371, Ex. 26

Use the algorithm in Exercise 24 to devise an algorithm for evaluating a^n when n is a nonnegative integer.

Solution:

We use the idea in Exercise 24, together with the fact that $a^n = (a^{n/2})^2$ if n is even, and $a^n = a \cdot (a^{(n-1)/2})^2$ is n is odd, to obtain the following algorithm.

Algorithm 6 fastpower (n: positive integer, a: real number)

---

if $n = 1$ **then**
  return a
else if n is even **then**
  return $fastpower(n/2, a)^2$
else
  return $a \cdot fastpower((n-1)/2, a)^2$
end if

□

P535, Ex. 12

Find $f(n)$ when $n = 3^k$, where f satisfies the recurrence relation $f(n) = 2f(n/3) + 4$ with $f(1) = 1$.

Solution:

$f(n) = 5n^{\log_3 2} - 4$.

□

P535, Ex. 22

Suppose that the function f satisfies the recurrence relation $f(n) = 2f(\sqrt{n}) + \log n$ whenever n is a perfect square greater than 1 and $f(2) = 1$.

a) Find $f(16)$

b) Find a big-O estimate for $f(n)$. [Hint: make the substitution $m = \log n$.]

Solution:

a) $f(16) = 2f(4) + 4 = 2(2f(2) + 2) + 4 = 2(2 \cdot 1 + 2) + 4 = 12$.

b) Let $m = \log n$, so that $n = 2^m$. Also, let $g(m) = f(2^m)$. Then our recurrence becomes $f(2^m) = 2f(2^{m/2}) + m$, since $\sqrt{2^m} = (2^m)^{1/2} = 2^{m/2}$. Rewriting this in terms of g we have $g(m) = 2g(m/2) + m$. Theorem 2 (with $a = 2, b = 2, c = 1$, and $d = 1$ now tells us that $g(m)$ is $O(m \log m)$. Since $m = \log n$, this means that our function is $O(\log n \cdot \log \log n)$.

□

P536, Ex. 34

Find $f(n)$ when $n = 4^k$, where f satisfies the recurrence relation $f(n) = 5f(n/4) + 6n$, with $f(1) = 1$.

Solution:

$f(n) = 25n^{\log_4 5} - 24n$.

□

P536, Ex. 36

Find $f(n)$ when $n = 2^k$, where f satisfies the recurrence relation $f(n) = 8f(n/2) + n^2$ with $f(1) = 1$.

Solution:

$f(n) = 2n^3 - n^2$.

□

P397, Ex. 37.

How many functions are there from the set $\{1, 2, \ldots, n\}$, where n is a positive integer, to the set $\{0, 1\}$

a) that are one-to-one?

b) that assign 0 to both 1 and n?

c) that assign 1 to exactly one of the positive integers less than n?

Solution:

a) 2 if $n = 1$, 2 if $n = 2$, and 0 if $n \geq 3$.

b) 2^{n-2} for $n > 1$; 1 if $n = 1$.

c) $2(n - 1)$.

□

P398**, Ex.** 50**.**

How many bit strings of length 10 contain either five consecutive 0s or five consecutive 1s?

Solution: First we count the number of bit strings of length 10 that contain five consecutive 0s. We will count based on where the string of five or more consecutive 0s starts. If it starts in the first bit, then the first five bits are all 0s, but there is free choice for the last five bits, therefore there are $2^5 = 32$ such strings. If it starts in the second bit, then the first bit must be a 1, the next five bits are all 0s, but there is free choice for the last four bits; therefore there are $2^4 = 16$ such strings. If it starts in the third bit, then the second bit must be a 1 but the first bit and the last three bits are arbitrary; therefore there are $2^4 = 16$ such strings. Similarly, there are 16 such strings that have the consecutive 0s starting in each of positions four, five, and six. This gives us a total of $32 + 5 \cdot 16 = 112$ strings that contain five consecutive 0s. Symmetrically there are 112 strings that contain five consecutive 1s. Clearly there are exactly two strings that contain both (0000011111 and 1111100000). Therefore by the inclusion-exclusion principle, the answer is $112 + 112 - 2 = 222$.

□

P398**, Ex.** 62

Suppose that p and q are prime numbers and that $n = pq$. Use the principle of inclusion-exclusion to find the number of positive integers not exceeding n that are relatively prime to n.

Solution:

Let P be the set of numbers in $\{1, 2, 3, \ldots, n\}$ that are divisible by p, and similarly define the set Q. We want to count the numbers not divisible by either p or q, so we want $n - |P \cup Q|$. By the principle of inclusion-exclusion, $|P \cup Q| = |P| + |Q| - |P \cap Q|$. Every pth number is divisible by p, so

$|P| = \lfloor n/p \rfloor = q$. Similarly $|Q| = \lfloor n/q \rfloor = q$. Clearly, n is the only positive integer not exceeding n that is divisible by both p and q, so $|P \cap Q| = 1$. Therefore, the number of positive integers not exceeding n that are relatively prime to n is $n - p - q + 1$.

□

P398**, Ex.** 64

Use a tree diagram to find the number of bit strings of length four with no three consecutive 0s.

Solution:

There are 13 leaves. So the answer is 13.

□

P405**, Ex.** 10

Let (x_i, y_i), $i = 1, 2, 3, 4, 5$, be a set of five distinct points with integer coordinates in the xy plane. Show that the midpoint of the line joining at least one pair of these points has integers coordinates.

Solution:

The midpoint of the segment whose endpoints are (a, b) and (c, d) is $((a+c)/2, (b+d)/2)$. We are concerned only with integer values of the original coordinates. Clearly the coordinates of these fractions will be integers as well if and only if a and c have the same parity (both odd or both even) and b and d have the same parity. There are four possible pairs of parities: (odd, odd), $(odd, even)$, $(even, odd)$, $(even, even)$. Since we are given five points, the pigeonhole principle guarantees that at least two of them will have the same pair of parities. The midpoint of the segment joining these two points will therefore have integer coordinates.

□

P406**, Ex.** 40 Prove that at a party where there are at least two people, there are two people who know the same number of other people there.

Solution:

Let $K(x)$ be the number of other people at the party that person x knows. The possible values for $K(x)$ are $0, 1, \ldots, n-1$, where $n \geq 2$ is the number of

people at the party. We cannot apply the pigeonhole principle directly, since there are n pigeons and n pigeonholes. However, it is impossible for both 0 and $n-1$ to be in the range of K, since if one person knows everybody else, then nobody can know no one else (we assume that "knowing" is symmetric). Therefore, the range of K has at most $n-1$ elements, whereas the domain has n elements, so K is not one-to-one, precisely what we wanted to prove.

□

P413**, Ex.** 13

A group contains n men and n women. How many ways are there to arrange these people in a row if the men and women alternate?

Solution:

$2(n!)^2$

□

P422**, Ex.** 24

Show that if p is a prime and k is an integer such that $1 \leq k \leq p-1$, then p divides $\binom{p}{k}$.

Solution: We know that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Clearly p divides the numerator. On the other hand, p cannot divide the denominator, since the prime factorizations of these factorials contains only numbers less than p. Therefore the factor p does not cancel when this fraction is reduced to lowest terms (i.e., to a whole number), so p divides $\binom{p}{k}$.

□

P422**, Ex.** 27

Prove the hockeystick identity

$$\sum_{k=0}^{r} \binom{n+k}{k} = \binom{n+r+1}{r}$$

whenever n and r are positive integers,

a) using a combinatorial argument

b) using Pascal's identity.

Solution:

a) $\binom{n+r+1}{r}$ counts the number of ways to choose a sequence of r 0s and $n+1$ 1s by choosing the positions of the 0s. Alternatively, suppose that the $(j+1)$st term is the last term equal to 1, so that $n \leq j \leq n+r$. Once we have determined where the last 1 is, we decide where the 0s are to be placed in the j spaces before the last 1. There are n 1s and $j-n$ 0s in this range. By the sum rule it follows that there are $\sum_{j=n}^{n+r} \binom{j}{j-n} = \sum_{k=0}^{r} \binom{n+k}{k}$ ways to this.

b) Let $P(r)$ be the statement to be proved. The basis step is the equation $\binom{n}{0} = \binom{n+1}{0}$, which is just $1 = 1$. Assume that $P(r)$ is true. Then

$$\begin{aligned}
&\sum_{k=0}^{r+1} \binom{n+k}{k} \\
&= \sum_{k=0}^{r} \binom{n+k}{k} + \binom{n+r+1}{r+1} \\
&= \binom{n+r+1}{r} + \binom{n+r+1}{r+1} \\
&= \binom{n+r+2}{r+1},
\end{aligned}$$

using the inductive hypothesis and Pascal's identity.

□

P525, Ex. 12

Find the solution to $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ for $n = 3, 4, 5, \ldots$, with $a_0 = 3$, $a_1 = 6$, and $a_2 = 0$.

Solution:

The characteristic equation is $r^3 - 2r^2 - r + 2 = 0$. This factors as $(r-1)(r+1)(r-2) = 0$, so the roots are $1, -1$, and 2. Therefore the general solution is $a_n = \alpha_1 + \alpha_2(-1)^n + \alpha_3 2^n$. Plugging in initial conditions gives

$3 = \alpha_1 + \alpha_2 + \alpha_3$, $6 = \alpha_1 - \alpha_2 + 2\alpha_3$, and $0 = \alpha_1 + \alpha_2 + 4\alpha_3$. The solution to this system of equations is $\alpha_1 = 6$, $\alpha_2 = -1$ and $\alpha_3 = -1$. Therefore, the answer is $a_n = 6 - 2(-1)^n - 2^n$.

□

P525**, Ex.** 28

a) Find all solutions of the recurrence relation $a_n = 2a_{n-1} + 2n^2$.

b) Find the solution of the recurrence relation in part (a) with initial condition $a_1 = 4$.

Solution:

a) The associated homogeneous recurrence relation is $a_n = 2a_{n-1}$. We easily solve it to obtain $a_n^{(h)} = \alpha 2^n$. Next we need a particular solution to the given recurrence relation. By Theorem 6 we want to look for a function of the form $a_n = p_2 n^2 + p_1 n + p_0$. (Note that $s = 1$ here, and 1 is not a root of the characteristic polynomial.) We plug this into our recurrence relation and obtain $p_2 n^2 + p_1 n + p_0 = 2(p_2(n-1)^2 + p_1(n-1) + p_0) + 2n^2$. We rewrite this by grouping terms with equal powers of n, obtaining $(-p_2 - 2)n^2 + (4p_2 - p_1)n + (-2p_2 + 2p_1 - p_0) = 0$. In order for this equation to be true for all n, we must have $p_2 = -2$, $4p_2 = p_1$, and $-2p_2 + 2p_1 - p_0 = 0$. This tells us that $p_1 = -8$ and $p_0 = -12$. Therefore the particular solution we seek is $a_n^{(p)} = -2n^2 - 8n - 12$. So the general solution is the sum of the homogeneous solution and this particular solution, namely $a_n = \alpha 2^n - 2n^2 - 8n - 12$.

b) We plug the initial condition into our solution from part (a) to obtain $4 = a_1 = 2\alpha - 2 - 8 - 12$. This tells us that $\alpha = 13$. So the solution is $a_n = 13 \cdot 2^n - 2n^2 - 8n - 12$.

□

P526**, Ex.** 44

Let $\mathbf{A}_n$ be the $n \times n$ matrix with 2's on its main diagonal, 1's in all positions next to a diagonal element, and 0's everywhere else. Find a recurrence

relation for d_n, the determinant of $\mathbf{A}_n$. Solve this recurrence relation to find a formula for d_n.

Solution:

We can compute the first few terms by hand. For $n = 1$, the matrix is just the number 2, so $d_1 = 2$. For $n = 2$, the matrix is $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, and its determinant is clearly $d_2 = 4 - 1 = 3$. For $n = 3$, the matrix is

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix},$$

and we get $d_3 = 4$. For the general case, our matrix is

$$\mathbf{A}_n = \begin{bmatrix} 2 & 1 & 0 & 0 & \dots & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 \\ 0 & 1 & 2 & 1 & \dots & 0 \\ 0 & 0 & 1 & 2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 \end{bmatrix}.$$

To compute the determinant, we expand along the top row. This gives us a value of 2 times the determinant of the matrix obtained by deleting the first row and first column minus the determinant of the matrix obtained by deleting the first row and second column. The first of these smaller matrices is just $\mathbf{A}_{n-1}$, with determinant d_{n-1}. The second of these smaller matrices has just one nonzero entry in its first column, so we expand its determinant along the first column and see that it equals d_{n-2}. Therefore our recurrence relation is $d_n = 2d_{n-1} - d_{n-2}$, with initial conditions as computed at the start of this solution. If we compute a few more terms we are led to the conjecture that $d_n = n + 1$. If we show that this satisfies the recurrence, then we have proved that it is indeed the solution. And sure enough, $n + 1 = 2n - (n - 1)$.

□

P550**, Ex.** 22

Give a combinatorial interpretation of the coefficient of x^6 in the expansion $(1 + x + x^2 + x^3 + \cdots)^n$. Use this interpretation to find this number.

Solution:

Let e_i, for $i = 1, 2, \ldots, n$, be the exponent of x taken from the ith factor in forming a term x^6 in the expansion. Thus $e_1 + e_2 + \cdots + e_n = 6$. The coefficient of x^6 is therefore the number of ways to solve this equation with nonnegative integers, which is $C(n + 6 - 1, 6) = C(n + 5, 6)$.

□

P551**, Ex.** 42

Use generating functions to prove Pascal's identity: $C(n, r) = C(n - 1, r) + C(n - 1, r - 1)$ when n and r are positive integers with $r < n$. [Hint: Use the identity $(1 + x)^n = (1 + x)^{n-1} + x(1 + x)^{n-1}$.]

Solution:

First we note, as the hint suggests, that $(1 + x)^n = (1 + x)(1 + x)^{n-1} = (1 + x)^{n-1} + x(1 + x)^{n-1}$. Expanding both sides of this equality using the binomial theorem, we have

$$\begin{aligned}\sum_{r=0}^{n} C(n, r)x^r &= \sum_{r=1}^{n-1} C(n-1, r)x^r + \sum_{r=0}^{n-1} C(n-1, r)x^{r+1} \\ &= \sum_{r=0}^{n-1} C(n-1, r)x^r + \sum_{r=1}^{n} C(n-1, r-1)x^r.\end{aligned}$$

Thus,

$$1 + \left(\sum_{r=1}^{n-1} C(n, r)x^r\right) + x^n = 1 + \left(\sum_{r=1}^{n-1} (C(n-1, r) + C(n-1, r-1))x^r\right) + x^n.$$

Comparing these two expressions, coefficient by coefficient, we see that $C(n, r)$ must equal $C(n - 1, r) + C(n - 1, r - 1)$ for $1 \leq r \leq n - 1$, as desired.

□

P583**, Ex.** 47

How many relations are there on a set with n elements that are

a) symmetric?

b) antisymmetric?

d) irreflexive?

e) reflexive and symmetric?

Solution:

a) $2^{n(n+1)/2}$

b) $2^n 3^{n(n-1)/2}$

d) $2^{n(n-1)}$

e) $2^{n(n-1)/2}$

□

P607**, Ex.** 20

Let R be the relation that contains the pair (a, b) if a and b are cities such that there is a direct non-stop airline flight from a to b. When is (a, b) in

a) R^2?

b) R^3?

c) R^*?

Solution:

a) The pair $(a, b) \in R^2$ when there is a city c such that there is direct flight from a to c and a direct flight from c to b.

b) The pair $(a, b) \in R^3$ when there are cities c and d such that there is a direct flight from a to c, a direct flight from c to d, and a direct flight from d to b.

c) The pair $(a, b) \in R^*$ when it is possible to fly from a to b.

□

P607**, Ex.** 22

Suppose that the relation R is reflexive. Show that R^* is reflexive.

Solution:

Since $R \subseteq R^*$, it is clear that if for all $a \in A$ there is $(a, a) \in R$, then $(a, a) \in R^*$.

□

P607**, Ex.** 23

Suppose that the relation R is symmetric. Show that R^* is symmetric.

Solution: The result follows from

$$(R^*)^{-1} = (\cup_{n=1}^{\infty} R^n)^{-1} = \cup_{n=1}^{\infty} (R^n)^{-1} = \cup_{n=1}^{\infty} R^n = R^*.$$

□

P607**, Ex.** 24

Suppose that the relation R is irreflexive. Is the relation R^2 necessarily irreflexive?

Solution:

R^2 might not be irreflexive. For example, $R = \{(1,2),(2,1)\}$.

□

P615**, Ex.** 16

Let R be the relation on the set of ordered pairs of positive integers such that $((a,b),(c,d)) \in R$ if and only if $ad = bc$. Show that R is an equivalence relation.

Solution:

For reflexivity, $((a,b),(a,b)) \in R$ because $a \cdot b = b \cdot a$. If $((a,b),(c,d)) \in R$ then $ad = bc$, which also means that $cb = da$, so $((c,d),(a,b)) \in R$; this tells us that R is symmetric. Finally, if $((a,b),(c,d)) \in R$ and $((c,d),(e,f)) \in R$ then $ad = bc$ and $cf = de$. Multiplying these equations gives $acdf = bcde$, and since all these numbers are nonzero, we have $af = be$, so $((a,b),(e,f)) \in R$; this tells us that R is transitive.

□

P616**, Ex.** 40

a) What is the equivalence class of $(1,2)$ with respect to the equivalence relation in Exercise 16?

b) Give an interpretation of the equivalence classes for the equivalence relation R in Exercise 16. [Hint: Look at the ratio a/b corresponding to (a, b).]

Solution:

a) The equivalence class of $(1, 2)$ is the set of all pairs (a, b) such that the fraction a/b equals $1/2$.

b) The equivalence classes are the positive rational numbers.

□

P630**, Ex.** 6

Which of these are posets?

a) $(\mathbf{R}, =)$

b) $(\mathbf{R}, <)$

c) $(\mathbf{R}, \leq)$

d) $(\mathbf{R}, \neq)$

Solution:

a) Yes. (It is the smallest partial order: reflexivity ensures that very partial order contains at least all pairs (a, b).)

b) No. It is not reflexive.

c) Yes.

d) No. The relations is not reflexive, not antisymmetric, not transitive.

□

P631**, Ex.** 32

Answer these euqstions for the partial order represented by this Hasse diagram.

a) Find the maximal elements.

b) Find the minimal elements.

c) Is there a greatest element?

d) Is there a least element?

e) Find all upper bounds of $\{a, b, c\}$.

f) Find the least upper bound of $\{a, b, c\}$, if it exists.

g) Find all lower bounds of $\{f, g, h\}$.

h) Find the greatest lower bound of $\{f, g, h\}$, if it exists.

Solution:

a) The maximal elements are the ones with no other elements above them, namely l and m.

b) The minimal elements are the ones with no other elements below them, namely a, b and c.

c) There is no greatest element, since neither l nor m is greater than the other.

d) There is no least elements, since neither a nor b is less than the other.

e) We need to find elements from which we can find downward paths to all of a, b, and c. It is clear that k, l and m are the elements fitting this description.

f) Since k is less than both l and m, it is the least upper bound of a, b and c.

g) No element is less than both f and h, so there are no lower bounds.

h) Since there is no lower bound, there cannot be greatest lower bound.

□