Solutions for Boolean Functions and Computer Arithmetic

BF-1.1 The idea of this problem is to show how English phrases are translated into logical expressions.

(a) $f \wedge s$. In English, "but" is "and" with an underlying message: The use of "but" in this way often (but not always) indicates surprise. You might say, "The animal is a fish *and* it lives in the water." $(F \wedge W)$ Or you might say "The animal is a fish *but* it lives on dry land." $(F \wedge L)$ Logic doesn't make a fuss over surprises.

(b) Either of the equivalent functions $\sim(f \vee s)$ and $(\sim f) \wedge (\sim s)$. Some people think of "Neither A nor B nor ..." as "None of A and B and ...," which is the first form. Other people think of "Neither A nor B nor ..." as "Not A and not B and ...," which is the second form.

BF-1.2 $r \wedge \sim v$. Same idea as the previous exercise. It may or may not be a surprise since most registered voters don't vote, but we don't need to know that to write it in logic notation.

BF-1.3 It is helpful to include intermediate columns in the table to help with the computation of $f(p,q) = \sim\big((p \wedge q) \vee \sim(p \vee q)\big)$. In this case, we have included columns for $p \wedge q$ $p \vee q$ and $\sim(p \vee q)$. With more practice, less columns are needed.

p	q	$p \wedge q$	$p \vee q$	$\sim(p \vee q)$	f
0	0	0	0	1	0
0	1	0	1	0	1
1	0	0	1	0	1
1	1	1	1	0	0

BF-1.4

p	q	r	$q \vee \sim r$	$\sim p \wedge (q \vee \sim r)$
0	0	0	1	1
0	0	1	0	0
0	1	0	1	1
0	1	1	1	1
1	0	0	1	0
1	0	1	0	0
1	1	0	1	0
1	1	1	1	0

BF-1.5 Before making a truth table, it may help to simplify the expression. Using the associative law $p \vee (\sim p \vee q) = (p \vee \sim p) \vee q = 1 \vee q = 1$. Thus

$$\big(p \vee (\sim p \vee q)\big) \wedge \sim(q \wedge \sim r) = 1 \wedge \sim(q \wedge \sim r) = \sim(q \wedge \sim r) = \sim q \vee r,$$

where the last is by DeMorgan's Law. Now we are ready to make the table. We don't even need to include p since it does not enter into the final function!

q	r	$\sim q \vee r$
0	0	1
0	1	1
1	0	0
1	1	1

BF-1.6 Let $m =$ "Mary is a musician" and let $c =$ "Mary plays chess." The statement is $m \wedge c$ and its negation is $\sim(m \wedge c) = \sim m \vee \sim c$ by DeMorgan's law. Now put the final statement into words: "Either Mary is not a musician or she does not play chess."

BF-1.7 Let $g =$ "The car has gas" and let $f =$ "The fuel line is plugged." The statement is $\sim g \vee f$. Its negation is $\sim(\sim g \vee f) = g \wedge \sim f$. In words, "The car has gas and the fuel line isn't plugged."

You could have taken $g =$ "The car is out of gas". The statement and its negation would be $g \vee f$ and $\sim(g \vee f) = \sim g \wedge \sim f$. In words, "The car is not out of gas and the fuel line isn't plugged." There is a double negative in "is not out of gas," which you could simplify to "has gas."

BF-1.8 Here is the standard beginners way of doing this: $p \vee (p \wedge q) = (p \vee p) \wedge (p \vee q)$ by the distributive rule. This is $p \wedge (p \vee q)$ by the idempotent rule. This becomes p by the absorption rule. This is perfectly correct.

We assume from now on that you can look up or memorize the names of the rules, and we do not require you to write down the names each time you use a rule. Generally, you need only write the steps, showing the changes in the forms of functions that result from the basic rules. Here is all you need to write for this problem:

$$p \vee (p \wedge q) = (p \vee p) \wedge (p \vee q) = p \wedge (p \vee q) = p.$$

There are often different ways to apply the basic rules to reduce one function to another. If done correctly, they are all "full credit." The goal is clarity. If you feel that certain steps are made clearer by including the names of the rules (distributive, associative, etc.) then include them. If you combine two short steps and want to indicate that (e.g, associative law and distributive law) do so. It is up to you to be clear and correct.

You don't need to make up a truth table for equal functions when you can reduce one to the other using algebraic manipulation. However, unless you are specifically asked for an algebraic proof, you can give a truth table proof.

BF-1.9 No. For $h(p, q, r) = (p \wedge q) \vee r$ and $g(p, q, r) = p \wedge (q \vee r)$ we have $h(0, 0, 1) = 1$ and $g(0, 0, 1) = 0$, so the functions are *not* equal. **But wait** — they seem to be equal by the associative law. What's wrong with that?

BF-1.10 No. For $h(p, q, r) = (p \vee q) \vee (p \wedge r)$ and $g(p, q, r) = (p \vee q) \wedge r$ we have $h(1, 0, 0) = 1$ and $g(1, 0, 0) = 0$, so the functions are *not* equal. Note also that $h(p, q, r) = p \vee q$. Show this and explain why this makes it easy to see that $h(p, q, r) \neq g(p, q, r)$.

BF-1.11 If no choice of variables comes to mind, one can simplify functions and then either look at them and see the situation or compute truth tables. We leave the truth tables to you and take the algebraic approach. We want to simplify $f(p, q, r) = \big((\sim p \vee q) \wedge (p \vee \sim r)\big) \wedge (\sim p \vee \sim q)$ and then see where we are. Since $f(p, q, r)$ is of the form $A \wedge B \wedge C$ — parentheses not neeeded because of the associative law — where A, B and C involve "ors," a good strategy is to use the distributive laws to rearrange the "ands" and "ors" and use DeMorgan's law as needed. Also note that the order of A, B and C in $A \wedge B \wedge C$ does not matter because of the commutative law. Which two of the three possibilities (namely $\sim p \vee q$, $p \vee \sim r$ and $\sim p \vee \sim q$) should we combine first? In the end, it doesn't matter since it will all lead to the same answer. The easiest is $(\sim p \vee q) \wedge (\sim p \vee \sim q)$, which you should be able to simplify to $\sim p \vee (q \wedge \sim q) = \sim p$ with the distributive law.

Thus we have $f(p,q,r) = {\sim}p \wedge (p \vee {\sim}r)$, which, with the distributive law, becomes $({\sim}p \wedge p) \vee ({\sim}p \wedge {\sim}r) = {\sim}p \wedge {\sim}r$. This is equal to the other function by DeMorgan's law. The key to solving it this way was to keep using the distributive law and simplifying expressions such as ${\sim}p \wedge p$ that arose along the way.

BF-1.12 If we want to use the algebraic method, this may be another case for the algebraic method, just like the previous problem. We have $(r \vee p) \wedge (r \vee q) = r \vee (p \wedge q)$. Thus the first function in the problem is

$$\big({\sim}r \vee (p \wedge q)\big) \wedge \big(r \vee (p \wedge q)\big) = ({\sim}r \wedge r) \vee (p \wedge q) = p \wedge q.$$

Thus, they are the same.

BF-1.13 Yes. Write the first function as $({\sim}p \wedge q) \vee ({\sim}p \wedge {\sim}q)$ with the help of DeMorgan's law. Now you should be able to use the distributive law.

BF-1.14 No. Since there are only two variables, a truth table will have only four rows, so that is probably the quickest way for you to do it. You could try algebraic simplification. You should try those two methods just for the practice. Here's another trick. What happens when $q = 0$? when $q = 1$? With $q = 0$, the first function becomes

$${\sim}\big(({\sim}p \wedge 0) \vee ({\sim}p \wedge 1)\big) \vee (p \wedge 0) = {\sim}(0 \vee {\sim}p) \vee 0 = p,$$

which is not ${\sim}p$. This leads to a possible choice for p and q: either $(p,q) = (0,0)$ or $(p,q) = (1,0)$. Since the first function simplifies to p and the second function is ${\sim}p$, we'll get different values. You can try $q = 1$ and see what happens.

BF-1.15 No. The solution to the previous exercise gives three approaches. You should try all three. For the algebraic approach, it's easiest to first use DeMorgan's law on ${\sim}({\sim}p \vee q)$.

BF-2.1 These problems are routine: First write the information in the truth table as a Boolean function as done in the proof of Theorem 1, then perhaps simplify the function, and finally construct a circuit for the function. Many circuits are possible, depending on the final form of the function.

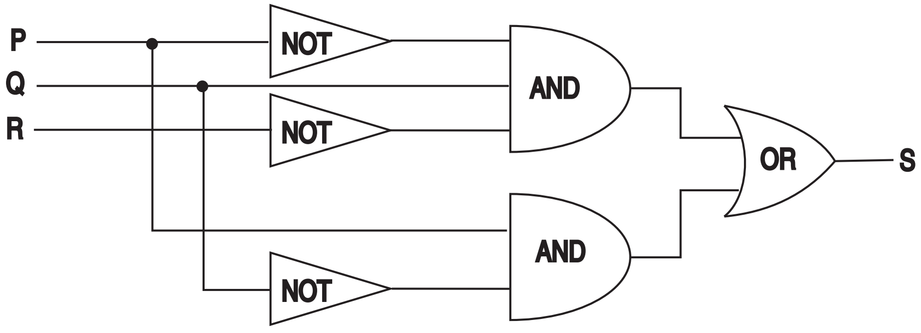
(a) Directly from the truth table we have the function

$$({\sim}P \wedge Q \wedge {\sim}R) \vee (P \wedge {\sim}Q \wedge {\sim}R) \vee (P \wedge {\sim}Q \wedge R).$$

The last two terms can be combined using the distributive law:

$$({\sim}P \wedge Q \wedge {\sim}R) \vee (P \wedge {\sim}Q).$$

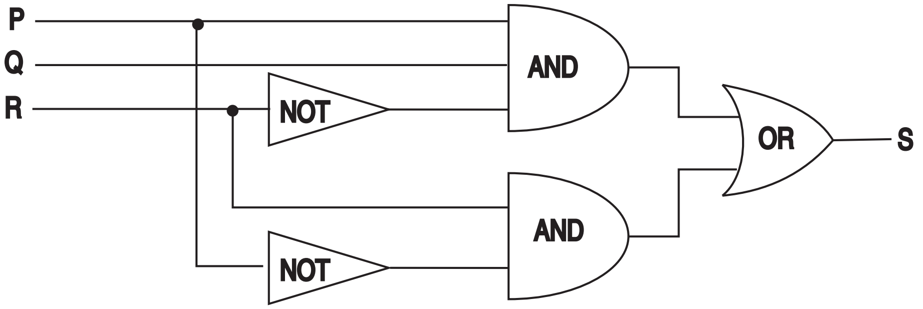
Allowing a 3-input **and** gate, we can represent it with the following circuit.



(b) From the truth table we have

$$(P \wedge Q \wedge \sim R) \vee (\sim P \wedge Q \wedge R) \vee (\sim P \wedge \sim Q \wedge R).$$

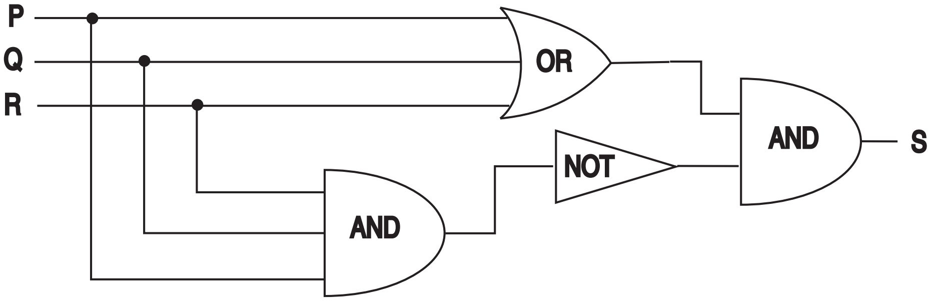
Combining the last two parenthesized expressions reduces this to $(P \wedge Q \wedge \sim R) \vee (\sim P \wedge R)$.



BF-2.2 It's simpler to construct $\sim S$ and then negate it. This gives us

$$S = \sim\big((P \wedge Q \wedge R) \vee (\sim P \wedge \sim Q \wedge \sim R)\big) = \big(\sim(P \wedge Q \wedge R)\big) \wedge (P \vee Q \vee R),$$

where we used DeMorgan's rule.



BF-2.3 In general, with k switches such that moving any one changes the state of the lights, the function is $f = s_1 \oplus s_2 \oplus \cdots \oplus s_k$. The associative and commutative rules hold for $\oplus$ just as they do for $\wedge$ and $\vee$, so we can rearrange and parenthesize this expression any way we wish.

Another solution is $f \oplus 1$. You can think of $s_i \oplus 1$ as rotating the ith switch 180° in its switch box. Clearly we can do this with any of the switches, for example

$$(s_1 \oplus 1) \oplus s_2 \oplus s_3 \oplus (s_4 \oplus 1) \oplus (s_5 \oplus 1).$$

BF-2.4 We could compute tables of the two functions or we could manipulate them algebraically. We'll let you construct tables. The first circuit computes $S(P,Q) = (P \wedge Q) \vee (P \oplus Q)$. Using $P \oplus Q = (P \wedge \sim Q) \vee (\sim P \wedge Q)$, we have

$$\begin{aligned} S(P,Q) &= (P \wedge Q) \vee (P \wedge \sim Q) \vee (\sim P \wedge Q) = \big(P \wedge (Q \vee \sim Q)\big) \vee (\sim P \wedge Q) \\ &= P \vee (\sim P \wedge Q) = (P \vee \sim P) \wedge (P \vee Q) = P \vee Q. \end{aligned}$$

BF-2.5 This can be done like the previous exercise. We leave the tabular method to you. For the algebraic method, use $P \oplus Q = (P \wedge {\sim}Q) \vee ({\sim}P \wedge Q)$ to note that the first circuit computes

$$(P \vee Q) \wedge \big((P \wedge {\sim}Q) \vee ({\sim}P \wedge Q)\big),$$

which you should simplify to $(P \wedge {\sim}Q) \vee ({\sim}P \wedge Q)$.
Here is another approach. Look at the first circuit. When the result of the **or** is 1, the result of the **and** will be the result of the **xor**. Thus the circuit computes $P \oplus Q$ except possibly when $P = Q = 0$. This case is easily checked.

BF-2.6 You are asked to show that $({\sim}P \wedge {\sim}Q) \vee (P \oplus Q) = {\sim}(P \wedge Q)$. Having done the previous exercises, you should be able to do this. Another way to do it is to notice that, once you write ${\sim}(P \wedge Q) = {\sim}P \vee {\sim}Q$ and $P \oplus Q = {\sim}P \oplus {\sim}Q$, this is Exercise 2.4 with P and Q replaced by ${\sim}P$ and ${\sim}Q$.

BF-2.7 From the truth table, the function is

$$\begin{aligned} S &= (P \wedge {\sim}Q \wedge {\sim}R) \vee (P \wedge {\sim}Q \wedge R) \vee (P \wedge Q \wedge R) \\ &= \big((P \wedge {\sim}Q \wedge {\sim}R) \vee (P \wedge {\sim}Q \wedge R)\big) \vee \big((P \wedge {\sim}Q \wedge R) \vee (P \wedge Q \wedge R)\big) \\ &= (P \wedge {\sim}Q) \vee (P \wedge R). \end{aligned}$$

This can be built with an **or** gate, an **and** gate and a gate the computes $f(x, y) = x \wedge {\sim}y$. You might object that this requires a "nonstandard" gate and so you've been tricked. We can get a solution with standard gates:

$$\begin{aligned} S &= (P \wedge {\sim}Q \wedge {\sim}R) \vee (P \wedge {\sim}Q \wedge R) \vee (P \wedge Q \wedge R) \\ &= P \wedge \Big(({\sim}Q \wedge {\sim}R) \vee ({\sim}Q \wedge R) \vee (Q \wedge R)\Big) \\ &= P \wedge \Big({\sim}Q \vee (Q \wedge R)\Big) \\ &= P \wedge ({\sim}Q \vee R), \end{aligned}$$

where the last step omitted some manipulation. We can get this directly from the truth table. First note that $S = P \wedge f(Q, R)$ for some function f. Since the truth table for f contains three ones and only one zero, f can be written as an **or**. Since $f(Q, R) = 0$ only when $Q = 1$ and $R = 0$, it is the **or** of ${\sim}Q$ and R. The function $P \wedge ({\sim}Q \vee R)$ requires only three standard gates. If we allow nonstandard gates, we can get by with two — one to compute f and an **and** gate.

BF-2.8 1011101. You can use the standard "human" subtraction procedure, or you can use two's-complement arithmetic, making sure the register is big enough so that 1110100 appears to be positive. We can do that with eight bits. Then 1110100 is 01110100 and the two's-complement of 00010111 is 11101001. Adding these gives 01011101, with a carry of 1 discarded.

BF-2.9 $\texttt{B7C5}_{\mathbf{16}} = 133705_{\mathbf{8}}$.

BF-2.10 (a) $61502_{\mathbf{8}} = 6 \times 8^4 + 1 \times 8^3 + 5 \times 8^2 + 2 = 25410$.

(b) $\texttt{EB7C5}_{\mathbf{16}} = 1110\,1011\,0111\,1100\,0101_{\mathbf{2}} = 11\,101\,011\,011\,111\,000\,101_{\mathbf{2}} = 3533705_{\mathbf{8}}$.

BF-2.11 Since we work most easily with base 10, we converted the given number to base 10 and then converted that to the required base. We obtained
(a) $jhecmnwdyh$ (b) $study - hard$

Solutions for Boolean Functions and Computer Arithmetic

BF-2.12 First method: $67_{\mathbf{10}} = 01000011_{\mathbf{2}}$. The two's complement is 10111101.
Second method: By definition, the 8-bit two's complement is $2^8 - 67 = 189$. Covert 189 to binary to obtain 10111101.

BF-2.13 $108_{\mathbf{10}} = 01101100_{\mathbf{2}}$ (using 8 bits total). Using our algorithm for computing, we fix the 100 pattern of bits on the right and complement all others to get 10010100.

BF-2.14 First method: Start with 10001001. Using the two's complement algorithm this converts to 01110111 which is $64 + 32 + 16 + 4 + 2 + 1 = 119$ and so $k = 119$.
Second method: $100001001_{\mathbf{2}} = 128 + 8 + 1 = 137$. It's two's complement in an 8-bit register is $2^8 - 137 = 119$.

BF-2.15 The two's complement of the given number is 01000110, which equals $2^6 + 2^2 + 2^1 = 70$. Thus the original number is -70. Equivalently, 10111010, without considering two's complement, is $2^7 + 2^5 + 2^4 + 2^3 + 2^1 = 186$. Because it is 8-bit two's complement, it represents $2^8 - 186 = 70$.

BF-2.16 $79_{\mathbf{10}} = 1001111_{\mathbf{2}}$ and $43_{\mathbf{10}} = 101011_{\mathbf{2}}$. The calculations:

Two's complement

1001111 regular		01001111 8-bit
-101011 arithmetic	00101011	11010101 register
100100	11010101	**1**00100100

The boldface **1** is a carry off the end of the register, which we discard because we are combining a positive and negative number.

BF-2.17 This proceeds much like the previous exercise, with a couple of changes. We do just the two's-complement arithmetic. We want $(-15) + (-46)$. Since $15_{\mathbf{10}} = 1111_{\mathbf{2}}$, its two's complement is 11110001 Since $46_{\mathbf{10}} = 101110_{\mathbf{2}}$, its two's complement is 11010010. Adding gives us 1100011, where we have discarded the leftmost carry bit. (This is the two's complement of 00111101, which is 61.)
This could have been done by writing it as $-(15+46)$. We would do the addition and take the two's complement of the result.

Now for $46+46+46$. From the previous work, the register for 46 is 00101110. Adding this to itself, we get 01011100. Since we added two positive numbers and the result is positive, there has been no overflow. Adding 00101110 to this we obtain 10001010. Since we added two positive numbers and the result is negative, there was overflow.

BF-2.18 The n-bit two's complement of x is $2^n - x$, which is obtained by counting backwards from 2^n. (Remember the clock — time before the hour is $60 - \mathit{minutes}$.) Similarly, the n-bit ten's complement of x is $10^n - x$. Is there a short-cut way to compute it. Yes. Scan from right to left, stopping at the first nonzero digit. Subtract that digit from 10 and all digits to the left from 9. Thus the 8-digit ten's complement of 67834000 is 32166000. To do subtraction such as $71121333 - 67834000$, you can do it in the usual way, or you add the ten's complement: $71121333 + 32166000 = 103287333$. A carry into the ninth digit should be discarded since we're doing 8-digit ten's-complement arithmetic. Thus the answer is 3287333. You should give a more complete explanation of why this works and you should compare it carefully to the two's complement to explain the analogies in more detail.

Solutions for Logic

Lo-1.1 We noted that exclusive or is seldom used in logic. In set theory, it corresponds to the symmetric difference.

Lo-1.2 “But” means “and.” It usually indicates that what follows “but” is surprising given what came before “but.”

(a) $h \wedge w \wedge {\sim}s$.

(b) ${\sim}w \wedge (h \wedge s)$, which can be rearranged by the commutative law if you wish.

(c) ${\sim}h \wedge {\sim}w \wedge {\sim}s$ or ${\sim}(h \vee w \vee s)$, which is equivalent by DeMorgan’s law.

Lo-1.3 $(n{\vee}k){\wedge}{\sim}(n{\wedge}k)$. Two other possible forms are $(n{\vee}k){\wedge}({\sim}n{\vee}{\sim}k)$ and $(k{\wedge}{\sim}n){\vee}({\sim}k{\wedge}n)$. Can you show symbolically that they are equivalent? What about exclusive or? Can’t we also write $n \oplus k$? Yes and no. Thinking in terms of Boolean functions, this is fine; however, $\oplus$ is seldom used in logic.

Lo-1.4 (a) $p \wedge q \wedge r$ (i.e. all three occur).

(b) $p \wedge {\sim}q$ (ZIP can be anything).

(c) $p \wedge ({\sim}q \vee {\sim}r)$ — same as $p \wedge {\sim}(q \wedge r)$ and $(p \wedge {\sim}q) \vee (p \wedge {\sim}r)$. Note that “however” is used in the same way as “but.”

(d) ${\sim}p \wedge q \wedge {\sim}r$ or ${\sim}(p \vee {\sim}q \vee r)$ (Do you see why?)

(e) ${\sim}p \vee (p \wedge q)$

Lo-1.5 One can construct a truth table or manipulate the statement form algebraically. We choose the latter approach. Note that

$${\sim}p \vee (p \wedge {\sim}q) \Leftrightarrow ({\sim}p \vee p) \wedge ({\sim}p \vee {\sim}q) \Leftrightarrow {\sim}p \vee {\sim}q \Leftrightarrow {\sim}(p \wedge q).$$

With $S = p \wedge q$, the statement form becomes $S \vee {\sim}S \vee r$, which is a tautology.

Here is another way to look at it. With $r = 1$, the value of the statement form is 1, so it cannot be a contradiction. With $r = 0$, the value of the statement form is $(p \wedge q) \vee \big({\sim}p \vee (p \wedge {\sim}q)\big)$. One can construct a truth table for this or, use the previous manipulations to see that it is equivalent to $S \vee {\sim}S$.

Lo-1.6 One can use any of the ideas in the previous problem. Using the algebraic approach:

$$\begin{aligned}(p \wedge {\sim}q) \wedge ({\sim}p \vee q) &\Leftrightarrow p \wedge \big({\sim}q \wedge ({\sim}p \vee q)\big) \Leftrightarrow p \wedge \big(({\sim}q \wedge {\sim}p) \vee ({\sim}q \vee q)\big)\\ &\Leftrightarrow p \wedge ({\sim}q \wedge {\sim}p) \Leftrightarrow {\sim}q \wedge (p \wedge {\sim}p) \Leftrightarrow 0.\end{aligned}$$

Thus the original statement form is equivalent to $0 \wedge r$, a contradiction.

Lo-1.7 Again we use the algebraic method. You may ask, “Why don’t you ever use a truth table?” Truth tables are a mechanical approach and you should be able to use them without any help. With the algebraic method, there are many choices. While all algebraic simplifications will eventually lead to the answer, some choices do so much more quickly than others. By showing which choices lead quickly to solutions, we hope you’ll gain some ability to make such choices.

$$\big(({\sim}p \wedge q) \wedge (q \vee r)\big) \wedge {\sim}q \wedge r \Leftrightarrow {\sim}p \wedge q \wedge (q \vee r) \wedge {\sim}q \wedge r.$$

Combining the q and $\sim q$, we obtain 0. Since we have a bunch of things joined by "and," the entire statement form becomes 0.

Lo-1.8 Remember that we can simplify a statement form before constructing a truth table. Note that

$$p \vee (\sim p \wedge q) \Leftrightarrow (p \vee \sim p) \wedge (p \vee q) \Leftrightarrow p \vee q.$$

Thus the statement form of this problem can be written $(p \vee q) \Rightarrow q$, which is 0 if and only if $p = 1$ and $q = 0$. (Incidentally, it can be simplified further to $p \Rightarrow q$.)

Lo-1.9 By the previous exercise, the statement form is equivalent to $(p \vee q) \Rightarrow \sim q$, which is equivalent to $\sim q$.

Lo-1.10 This statement is equivalent to $q \Rightarrow p$.

Lo-1.11 The negation $\sim(p \Rightarrow q)$ of "if p then q" can be written as $p \wedge \sim q$. We use this form.

(a) P is a pentagon, but P is not a polygon.

(b) Let T, J, S and M be statement variables for "Tom is Ann's father," "Jim is Ann's uncle," and so on. The negation is $T \wedge \sim(J \wedge S \wedge M)$. Use DeMorgan's law to move the negation inside. Thus we have "Either Jim is not Ann's uncle or Sue is not her aunt or Mary is not her cousin, but Tom is Ann's father.

Lo-1.12 (a) Converse: If P is a polygon then P is a pentagon.
Inverse: If P is not a pentagon then P is not a polygon.

(b) Converse: If Jim is Ann's uncle and Sue is her aunt and Mary is her cousin, then Tom is Ann's father.
Inverse: If Tom is not Ann's father, then either Jim is not her uncle or Sue is not her aunt or Mary is not her cousin.

Lo-1.13 Of course, one can simply say they are equivalent because they are both contradictions and all contradictions are equivalent. However, we hoped yo would notice that the contrapositive of the converse is the inverse.

Lo-1.14 (a) If P is not a polygon, then P is not a pentagon.

(b) If Jim is not Ann's uncle or Sue is not her aunt or Mary is not her cousin, then Tom is not Ann's father.

Lo-1.15 If Dennis enters the America's Cup, then he is sure of victory.

Lo-1.16 No. The statement "p only if q" means $p \Rightarrow q$; that is, $H \Rightarrow ((M \vee C) \wedge B \wedge A)$. We know that A, B and C are true, but that says nothing about H. Why does it feel like you were lied to? Probably because the requirements were spelled out in such detail. As a result you thought he meant either "if" or "if and only if" when he said "only if." Of course, maybe your high school principal wasn't that familiar with logic and he thought he was lying just to get you to work more.

Lo-1.17 Let L stand for "learning to program in L." The given statement is C++ ⇒ C. Thus, "If you learn to program in C++, then you learn to program in C." The other equivalent form is the contrapositive: "If you don't learn to program in C, then you don't learn to program in C++."

Lo-1.18 Using DeMorgan's laws a couple of times, we have

$$\begin{aligned} \sim(\sim p \vee q) \vee (r \vee \sim q) &\Leftrightarrow (p \wedge \sim q) \vee r \vee \sim q \\ &\Leftrightarrow \sim\bigl(\sim(p \wedge \sim q) \wedge \sim r \wedge q\bigr) \end{aligned}$$

There are other ways to do this.

Lo-1.19 We have

$$\begin{aligned} p \Rightarrow (q \Rightarrow r) &\Leftrightarrow {\sim}p \vee ({\sim}q \vee r) \\ &\Leftrightarrow {\sim}p \vee {\sim}q \vee r \end{aligned}$$

and

$$\begin{aligned} (p \wedge q) \Rightarrow r &\Leftrightarrow {\sim}(p \wedge q) \vee r \\ &\Leftrightarrow {\sim}p \vee {\sim}q \vee r. \end{aligned}$$

Hence the expression in large parentheses in the problem is always true. Thus the problem reduces to rewriting ${\sim}p \wedge {\sim}q \wedge {\sim}r$. By DeMorgan's law, this equals ${\sim}(p \vee q \vee r)$.

Lo-1.20 "A is a sufficient condition for B" means that A forces B; that is, "If A then B." Applied here: "If I get up when the alarm rings, then I will get to work on time."

Lo-1.21 If the sides of a triangle have lengths 3, 4, and 5 then the triangle is a right triangle.

Lo-1.22 This can be done using either Example 5 or the method in Example 6. We use the latter. The statement is false if Jane doesn't do the programming but passes anyway. By the method in Example 6, we can write either "If Jane passes her Java course, then she did all the programming assignments" or "If Jane does not do all the programming assignments, then she will not pass her Java course."

Lo-1.23 Since all the statements are implications, it is sufficient to check for the single false situation. The given statement is false if the program is running and there is less than 250K of RAM. Therefore, we ask the following question in each of (a)–(f): Is the statement false when the program is running and there is less than 250K of RAM. If "yes," it is false when the given implication is false and so they are equivalent; if "no," they are not equivalent. Here are the answers:

(a) No (b) Yes (c) Yes (d) No (e) Yes (f) No

You should fill in the explanations as the why each answer is "yes" or "no."

Lo-2.1 (a) $\forall\, x \in \mathbb{R},\ \big((x < 0) \vee (x = 0) \vee (x > 0)\big)$

(b) Let $\mathcal{C}$ be the set of computer scientists, let $\mathcal{U}$ be the set of unemployed people and let $\mathcal{E}$ be the set of employed people. We could say

$$\forall\, x \in \mathcal{C},\ x \notin \mathcal{U} \quad \text{or} \quad \forall\, x \in \mathcal{C},\ x \in \mathcal{E}.$$

We could use words instead of the sets $\mathcal{C}$, $\mathcal{U}$ and $\mathcal{E}$:

$\forall$ computer scientists x, x is not unemployed.
$\forall$ computer scientists x, x is employed.

The former is a straight translation of the text. The latter involves knowing that, with the set of people the universal set, $\mathcal{U}^c = \mathcal{E}$. As such, it involves some knowledge of the world and so is not a direct translation of (b) into logic.

Lo-2.2 The original statement is true. Statements (b), (d) and (e) say the same thing and so are also true. However, they are open to misinterpretation. The standard interpretation of (b) and (e) is that they are true regardless of what integer one comes up with. But suppose you tell someone "I noticed that 276^2 is even." He might answer with (b), now thinking of (b) as applying only to 276. Of course, he should have said "If that integer...," not "If a given integer...," but people are often careless in speech. What about (a), (c) and (f)? Since $1^2 = 1$ is odd, (a) is false. While (c) is true, it does not say the same thing as the original statement. Statement (f) may appear to be the same as the original, but it is not. It is the converse. It says "$\forall n \in \mathbb{N}$, if n is even then n^2 is even."

Lo-2.3 (a) $\forall$ correct algorithms A, (A is correctly coded)$\Rightarrow$(A runs correctly).

(b) $\forall\, s,t \in \mathbb{Z},\ \big((s \text{ odd}) \wedge (t \text{ odd})\big) \Rightarrow (st \text{ odd})$.

(c) This is the converse of (b): $\forall\, s,t \in \mathbb{Z},\ (st \text{ odd}) \Rightarrow \big((s \text{ odd}) \wedge (t \text{ odd})\big)$.

Lo-2.4 (a) "$\forall$ S, (S is a computer science student) $\Rightarrow$ (S needs to take Java programming)."

(b) "$\forall$ computer science students S, S needs to take Java programming."

Note the sets over which quantification takes place (i.e., the sets to which S belongs) is different in the two answers. In (b), "$\forall$ computer science students S" tells us that S runs through the set of computer science students. For (a), common sense tells us that the set can be any set that includes all computer science students; however, the set was not specified. Perhaps it's the set of all fish, in which case the statement is trivial if no fish are computer science students. Thus, the correct form for (a) would be as follows.

(a) "$\forall$ S $\in \mathcal{S}$, (S is a computer science student) $\Rightarrow$ (S needs to take Java programming)," where $\mathcal{S}$ is ... (e.g., the set of all people).

Lo-2.5 (a) "$\exists$ a question Q such that Q is easy." or
"$\exists$ a question Q, Q is easy."

(b) "$\exists$ S $\in \mathcal{S}$, (S is a question) $\wedge$ (S is easy)," where $\mathcal{S}$ is the set of all sentences.

Lo-2.6 The proposed negation is incorrect. A correct version is "There exists an irrational number x and a rational number y such that the product xy is rational."
The negation is true since we could take x to be any irrational number and $y = 0$. If we start with "The product of any irrational number and any nonzero rational number is irrational," then that statement is true and its negation, "There exists an irrational number x and a nonzero rational number y such that the product xy is rational," is false.
The incorrect "negation" given in the problem is also true.

Lo-2.7 There exists a computer program P such that P is correctly programmed and P compiles with warning messages. Which is true depends on your interpretation of "correctly programmed." Often a program will run just fine with warning messages. For example, many compilers give a warning message if a loop has no code in its body, but the empty body may be intentional.

Lo-2.8 The proposed negation is incorrect. A correct negation is "There exist real numbers x and y such that $x^2 = y^2$ but x does not equal y." The negation is true (take $x = -1$ and $y = 1$).
The incorrect "negation" has the contrapositive of the original statement inside the "for all" quantifier. Since a statement and its contrapositive are equivalent, this statement is also false (take $x = -1$ and $y = 1$ just as in the original).

Lo-2.9 "There exists $p \in \mathbb{P}$ such that p is even and $p \neq 2$." The original statement is true.

Lo-2.10 "There exists an animal x such that x is a tiger and either x has no stripes or x has no claws." There is probably a declawed captive tiger, in which case the negation is true.

Lo-2.11 (a) "$\forall\, x \in \mathbb{R},\ \exists$ negative $y \in \mathbb{R},\ x > y$." Both statements are true. For the original statement, take $x = 1$. For the statement here, take $y = -|x| - 1$.

(b) Applying Theorem 2, we move negation through the quantifiers one at a time. Let $\mathbb{R}^-$ be the negative reals. We have

$$\begin{aligned} \sim(\exists\, x \in \mathbb{R},\ \forall\, y \in \mathbb{R}^-,\ x > y) \quad &\Leftrightarrow \quad \forall\, x \in \mathbb{R},\ \sim(\forall\, y \in \mathbb{R}^-,\ x > y) \\ &\Leftrightarrow \quad \forall\, x \in \mathbb{R},\ \exists\, y \in \mathbb{R}^-,\ x \leq y. \end{aligned}$$

This cannot be true since it is the negation of a true statement. Again, take $x = 1$.

Lo-2.12 Contrapositive: "For all computer programs P, if P compiles with error messages then P is incorrect."
Converse: "For all computer programs P, if P compiles without error messages then P is correct."
Inverse: "For all computer programs P, if P is incorrect then P compiles with error messages."

Lo-2.13 Contrapositive: "$\forall\, n \in \mathbb{N}$, if n is odd then its square is odd."
Converse: "$\forall\, n \in \mathbb{N}$, if n is even then its square is even."
Inverse: "$\forall\, n \in \mathbb{N}$, If n^2 is odd then n is odd."
All statements are true in this problem because the square of an integer is even if and only if the integer is even. The "if" part is proved using the contrapositive and the "only if" part is proved using the converse.

Lo-2.14 Contrapositive: "$\forall\, n \in N$, if n is even and not 2 then n is composite."
Converse: "$\forall\, n \in N$, if n is odd or equal to 2 then n is prime."
Inverse: "$\forall\, n \in N$, if n is composite then n is even and not equal to 2."
The statement and its contrapositive are true. The converse and the inverse are false.

Lo-2.15 (a) $\forall\, x \in P,\ H(x) \Rightarrow L(x)$.

(b) Everyone who is happy has a large income.

(c) We have

$$\begin{aligned} &\sim\bigl(\forall\, x \in P,\ H(x) \Rightarrow L(x)\bigr) \\ &\qquad\qquad \Leftrightarrow \quad \exists\, x \in P \sim\bigl(\sim H(x) \vee L(x)\bigr) \\ &\qquad\qquad \Leftrightarrow \quad \exists\, x \in P\ \bigl(H(x) \wedge \sim L(x)\bigr). \end{aligned}$$

(d) There is someone who is happy and does not have a large income.

Lo-2.16 (a) False: For $x = 1$ and $x = -1$, both x and $1/x$ are integers.

(b) True: If $x \in \mathbb{R}$ and $x + y = 0$, then $y = -x$ and so $y \in \mathbb{R}$ and y is unique. Alternatively for uniqueness: Suppose $x + y = 0$ and $x + z = 0$. Then $x + y = x + z$ and so $y = z$.

Lo-2.17 $\Bigl(\exists\, x \in D,\ S(x)\Bigr) \wedge \forall\, x, y \in D,\ \bigl(S(x) \wedge S(y)\bigr) \Rightarrow (x = y)\Bigr)$

Lo-2.18 Both are true. Since there are infinitely many primes, there is $p \in \mathbb{P}$ with $p > m$ and p odd.

(a) Let $n = p + 3$ and $q = 3$.

(b) Let $n = p + 2$ and $q = 2$.

Lo-2.19 (a) Equivalent statements: If the first is true, then $\forall\, x \in D\ P(x)$. Likewise, $\forall\, x \in D\ P(x)$. Thus the second is true. Suppose the first is false, then there is $x \in D$ such that either $P(x)$ is false or $Q(x)$ is false. If $P(x)$ is false, then so is "$\forall\, x \in D,\ P(x)$" and hence the second statement is false. If $Q(x)$ is false, similar reasoning applies.

(b) Not equivalent statements: Let $D = \mathbb{Z}$, let $P(x)$ be "x is even" and let $Q(x)$ be "x is odd." Then the first statement is true and the second is false.

(c) Not equivalent statements: The example for (b) works here also.

(d) Equivalent: If the first is true, then there is some $x \in D$ such that either $P(x)$ is true or $Q(x)$ is true. Hence either "$\exists\, x \in D,\ P(x)$" is true or "$\exists\, x \in D,\ P(x)$" is true. Thus the second statement is true. Suppose the first is false, then for all $x \in D$, both $P(x)$ and $Q(x)$ are false. From this you can conclude that the second statement is false.

Note: You actually only need to do one of (a) and (d) and one of (b) and (c) because of negation. Negating both statements in (a) gives both statements in (d) with the predicates $\sim P$ and $\sim Q$ in place of the predicates P and Q. Likewise for (b) and (c).

Lo-2.20 Let $n = ab$. By the formula for summing a geometric series,

$$1 + 2^a + (2^a)^2 + \cdots + (2^a)^{b-1} = \frac{1 - (2^a)^b}{1 - 2^a} = \frac{2^n - 1}{2^a - 1}.$$

Multiplying by $2^a - 1$ gives us a factorization of $2^n - 1$.

Lo-2.21 Let $p = 2^n - 1$. The divisors of N are 2^k and $2^k p$ where $0 \le k \le n - 1$. Thus, the sum of the divisors, including N, is two geometric series:

$$(1+2+2^2+\cdots+2^{n-1}) + (p+2p+2^2p+\cdots+2^{n-1}p) = (1+2+2^2+\cdots+2^{n-1})(1+p).$$

The sum of the geometric series is $2^n - 1$ and $p + 1 = 2^n$. Thus the sum of the divisors of N is $(2^n - 1)2^n = 2N$. Since we included the divisor N, the sum of the divisor of N that are less than N is $2N - N = N$.

Solutions for Number Theory and Cryptography

NT-1.1 (a) True. Assume, without loss of generality, that x is even and y is odd. Then $x = 2k$ and $y = 2j + 1$, whence $x + y = 2k + 2j + 1 = 2(k + j) + 1$, which is odd.

(b) True. Use the contrapositive. First suppose that both x and y are odd, say $x = 2k + 1$ and $y = 2j + 1$. Then $x + y = 2(k + j + 1)$ is even. Now suppose that both x and y are even, say $x = 2k$ and $y = 2j$. Then $x + y = 2(k + j)$ is even.

NT-1.2 (a) False. Counterexample: $5 - 3 = 2$.

(b) False. Counterexample: $1 + 3 = 4$.

NT-1.3 (a) True. Negating both A and B in "A if and only if B" gives an equivalent statement. (It's the contrapositive.) In this case, the result is "The product of two integers is odd if and only if neither of them is even." Since "neither of them is even" is the same thing as "both of them are odd," this is the closure property mentioned in Example 1. You could also prove it from scratch. We do that now. For the "if" part, assume that x and y are integers and $x = 2k$ is even. Then $xy = 2ky = 2(ky)$ is even. For the "only if" part, use the contrapositive: "If x and y are both odd, there product is odd." Assume that $x = 2k + 1$ and $y = 2j + 1$. Then $xy = 2(2kj + k + j) + 1$ is odd.

(b) False. Counterexample: $3 \times 2 = 6$.

NT-1.4 (a) True: One can write out various proofs, breaking things down into cases depending on whether m and n are even or odd. Alternatively, one can construct a table with four cases Here's the table:

m	n	$m - n$	m^3	n^3	$m^3 - n^3$
even	even	even	even	even	even
even	odd	odd	even	odd	odd
odd	even	odd	odd	even	odd
odd	odd	even	odd	odd	even

By comparing the $m - n$ and $m^3 - n^3$ columns, we see that the result is true.
An alternative proof can be obtained by doing calculations modulo 2. This is because "even" corresponds to 0 (mod 2) and "odd" to 1 (mod 2). We have $m^3 = m \pmod 2$ and $n^3 = n \pmod 2$. Therefore $m^3 - n^3 = m - n \pmod 2$.

(b) True: In fact, this is equivalent to (a) because $A \Leftrightarrow B$ is true if and only if $\sim\!A \Leftrightarrow \sim\!B$ is true.

NT-1.5 (a) False: Try $n = 3$. (What is the answer for $n > 3$?)

(b) True: Note that $(-1)^2 = 1$. If $n = 2k$, then $(-1)^{2k} = \big((-1)^2\big)^k = 1^k = 1$. If $n = 2k + 1$, then $(-1)^{2k+1} = -(-1)^{2k} = -1$.

NT-1.6 (a) True: One of n and $n + 1$ is even. Therefore $n(n + 1) = n^2 + n$ is even. Therefore, since 5 is odd, $(n^2 + n) + 5$ is odd.

(b) True: With a little algebra $6(n^2 + n + 1) - (5n^2 - 3) = (n + 3)^2$.

(c) False: For every $M > 0$, let $n = 11M > M$. Note that

$$n^2 - n + 11 = 11(11M^2 - M + 1),$$

which is composite because $11M^2 - M + 1 \geq M(11M - 1) > 1$.

(d) True: Factor $n^2 + 2n - 3$ to get $(n + 3)(n - 1)$. For this to be a prime, we must choose n so that one factor is ± 1 and the other is $\pm p$, where p is a prime and both factors have the same sign. Thus, either $n + 3 = p$ and $n - 1 = 1$ or $n + 3 = -1$ and $n - 1 = -p$. The first pair of equations give $n = 2$ and $p = 5$, which is a prime. The second pair of equations give $n = -4$ and $p = 5$, which is the same prime. You may ask about the choices $n + 3 = 1$ and $n - 1 = p$ or $n + 3 = 1$ and $n - 1 = p$. They lead to negative values for p and primes must be positive by definition.

NT-1.7 (a) False: You should be able to prove that 7 is a counterexample since the only possible values for x, y and z are 0, 1 and 4.

(b) True: We can write such a product as $N(k) = k(k + 1)(k + 2)(k + 3)$. Let's look at some values: $N(1) = 24 = 5^2 - 1$, $N(2) = 120 = 11^2 - 1$, $N(3) = 360 = 19^2 - 1$. It looks like N is always one less than a square. Since squares are not very close together this would mean that N is not a square. We have a plan. Let's write a proof. Since $k(k + 3)$ and $(k + 1)(k + 2)$ are close together, we rewrite the product as

$$N = \big(k(k + 3)\big)\big((k + 1)(k + 2)\big) = \big(k(k + 3)\big)\big(k(k + 3) + 2\big) = n(n + 2) > n^2,$$

where $n = k(k + 3)$. Now $n(n + 2) = (n + 1)^2 - 1$ — one less than a square as we conjectured. Thus $N < (n + 1)^2$. We've shown that N lies between two consecutive squares; that is, $n^2 < N < (n + 1)^2$. Hence N cannot be a square.

NT-1.8 (a) True: Let $x = m^{1/2} + n^{1/2}$ and $y = m^{1/2} - n^{1/2}$. Then $xy = m - n$ is a nonzero integer. Hence x and y are either both rational or both irrational. (See discussion in Example 3.)

(b) True: Define x and y as in (a). Since at least one is rational, they are both rational by (a). Thus $(x + y)/2 = m^{1/2}$ is rational and so m is a perfect square by Theorem 3. Likewise, $(x - y)/2 = n^{-1/2}$ is also a perfect square.

(c) True: Note that $m + 2m^{1/2}n^{1/2} + n = (m^{1/2} + n^{1/2})^2$. Clearly this is a perfect square if m and n are perfect squares. Conversely, suppose this is a perfect square. Then $m^{1/2} + n^{1/2}$ is rational and so m and n are perfect squares by (b).

(d) You should be able to see that (a) and (b) are false whenever $m = n$ is *not* a perfect square. If $m = n$, $m + 2m^{1/2}n^{1/2} + n = 4m$ and hence is a perfect square if and only if m is a perfect square. Thus (c) is true.

NT-1.9 The "if" part is obvious. We prove the "only if" part. Suppose n is composite. Let p be the smallest prime dividing n. Then $n = pm$ where $m > 1$ since n is composite. Let q be a prime dividing m. Then $q \leq m$. Since p is the smallest prime dividing n, $p \leq q$. Hence $n = pm \geq pq \geq p^2$ and so $p \leq n^{1/2}$.

NT-1.10 If x terminates with d digits after the decimal place, we can write it as $10^d x/10^d$. For (a), $d = 4$ and so we can write it as 31415/10000. This is not in lowest terms, but you need not reduce it.

We call a decimal in which a pattern repeats a *repeating decimal.* Thus (b) and (c) are repeating decimals. The *period* is the number of digits in the repeating pattern. In (b) the period is two because of the pattern 30. In (c) the period is three because of the pattern 215. If x is a repeating decimal with period k, then $10^k x - x$ will be a terminating decimal, which can be written as a rational number a/b by the previous discussion. Thus $x = a/(b(10^k - 1))$. We now apply this.

(b) Since $x = 0.303030\ldots$, $k = 2$, $10^2x - x = 30$, and so $x = 30/99$.

(c) $x = 6.3215215215\ldots$, $k = 3$,

$$10^3x - x = 6321.5215215\ldots - 6.3215215\ldots = 6315.2 = 63152/10,$$

and so $x = 63152/9990$.

NT-1.11 Yes: We can solve for x to obtain $x = \frac{d-b}{a-c}$. Fill in the missing steps.

NT-1.12 (a) True: Note that $(k-1) + k + (k+1) = 3k$ which equals 0 mod 3. Equivalently, for three consecutive integers, in some order, one is equal to 0 (mod 3), one is equal to 1 (mod 3), and one is equal to 2 (mod 3). The sum is equal to $0 + 1 + 2 = 3 = 0$ (mod 3).

(b) True: Let the even integers be $2k$ and $2j$. Then $2k \times 2j = 4kj = 0$ (mod 4). Equivalently, an even integer is equal to 0 (mod 4) or 2 (mod 4). Modulo 4, the product of two even integers is either 0 or $2 \times 2 = 4$. In both cases the product equals 0 (mod 4).

(c) True: If $n = 16k$ then $n = 8(2k)$, so n is divisible by 8.

(d) True: Let $n = 2k + 1$. Then $3n + 3 = 6k + 3 + 3 = 6(k + 1)$ is divisible by 6.

NT-1.13 (a) True: If $b = ak$ then $bc = akc$.

(b) True: Since $b \mid c$, we have $c = bd$ for some $d \in \mathbb{Z}$. Use (a) with $a = a$, $b = b$ and $c = d$.

(c) False: Let $a = 2$, $b = 3$, $c = 4$.

NT-1.14 (a) False: Let $a = 2$ and $b = c = 1$.

(b) False: Let $a = 6$, $b = 2$ and $c = 3$.

(c) True: If $a \mid b$, then $b = ka$ for some $k \in \mathbb{Z}$. Then $b^2 = (k^2)a^2$ and so $a^2 \mid b^2$.

(d) False: Let $a = 4$ and $b = 2$.

NT-1.15 (a) $1404 = 2^2\,3^3\,13$ (b) $9702 = 2\,3^2\,7^2\,11$ (c) $89250 = 2\,3\,5^3\,7\,17$

NT-1.16 (a) $p_1^{me_1} \cdots p_k^{me_k}$.

(b) Yes. We give a proof by contradiction along similar lines to the proof that $n^{1/2}$ must be irrational when n is not a perfect square as done in Example 3. Suppose $s^{1/m}$ is rational and not an integer. Then $s^{1/m} = a/b$ for some integers a and b. We can suppose that a/b is in lowest terms and that $b > 1$. From $s^{1/m} = a/b$, we have $a^m = sb^m$. If $p \mid b$, then $p \mid a^m$. As in Example 3, $p \mid a$, a contradiction.

NT-1.17 We have

$$\begin{aligned} 20! =& (2^2 \times 5) \times (19) \times (2 \times 3^2) \times (17) \times (2^4) \times (5 \times 3) \\ & \times (2 \times 7) \times (13) \times (3 \times 2^2) \times (11) \times (2 \times 5) \times (3^3) \\ & \times (2^3) \times (7) \times (2 \times 3) \times (5) \times (2^2) \times (3) \times (2) \times (1) \\ =& 19 \times 17 \times 13 \times 11 \times 7^2 \times 5^4 \times 3^8 \times 2^{18}. \end{aligned}$$

Every zero at the end of 20! corresponds to a factor of $10 = 2 \times 5$. Since we have 2^{18} and 5^4, there will be four zeroes at the end.

For (b) and (c), the powers in the prime factorization are doubled and tripled, respectively. Thus the same happens to the number of zeroes at the end, giving us eight and twelve.

NT-1.18 Suppose we are given a number $A = a_n a_{n-1} \ldots a_1 a_0$. The statement $3 \mid A$ is equivalent to the statement $A \pmod 3 = 0$. Note that $10 = 1 \pmod 3$ and so $10^k = 1 \pmod 3$ for all $k \in \mathbb{N}$. We have

$$\begin{aligned} A &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \\ &= a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3. \end{aligned}$$

Thus A equals the sum of its digits modulo 3 and so we are done.
Can you find similar results for divisibility by 5? by 9? by 11?

NT-1.19 We prove it. If you list the remainders of all nonnegative integers, $0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots$ when divided by four you get $0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, \ldots$. Given any four consecutive integers, one, call it x, must be divisible by 4 (remainder 0) and one other, call it y has remainder 2 when divided by 4 and so is even. Thus $x = 4j$ and $y = 2k$ for some k and j and thus $xy = 8kj$ is divisible by 8. Since the product of all four consecutive integers includes xy as a factor, it is also divisible by 8.

NT-1.20 If n is even, n^2 is even and so $n^2 \neq 3 \pmod 4$. If n is odd, then $n = 2k + 1$ for some k. Then

$$n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Thus $n = 1 \pmod 4$.

NT-1.21 Let $n = 2k + 1$ By the solution to the previous exercise, $n^2 = 4k(k+1) + 1$. One of k and $k + 1$ is even. Thus $k(k+1)$ is even and so $8 \mid 4k(k+1)$. Thus $n^2 = 8j + 1$ for some j. Hence $n^4 = 64j^2 + 16j + 1 = 1 \pmod{16}$.

NT-1.22 Yes. Since $m - n = 0 \pmod d$ and $n = n \pmod d$, it follows from Theorem 4 that $(m - n) + n = 0 + n \pmod d$. Thus $m = n \pmod d$. This is the same as saying m and n have the same remainder when divided by d.

NT-1.23 No. Let $m = n = a = b = 2$, $d = 3$. Then $(m + n) \bmod d = 1$.

NT-1.24 (a) Since $k = j$ (mod!d), $j - k = id$ for some $i \in \mathbb{Z}$ If $x \in d\mathbb{Z} + j$, we have $x = md + j$ for some $m \in \mathbb{Z}$. Then $x = md + k + (j - k) = (m + i)d + k$ and so $x \in d\mathbb{Z} + k$. Similarly, if $y \in d\mathbb{Z} + k$, then $y \in d\mathbb{Z} + j$.

(b) We give a proof by contradiction. Suppose $x \in (d\mathbb{Z}+j) \cap (d\mathbb{Z}+k)$. Then $x \in (d\mathbb{Z}+j)$ and $x \in (d\mathbb{Z} + k)$. Thus $x = j \pmod d$ and $x = k \pmod d$. It follows that $j = k \pmod d$, a contradiction since we are given that $j \neq k \pmod d$.

NT-1.25 (a) We give a proof by contradiction. Suppose $log_p(q) = a/b$. Then $q = p^{a/b}$ and so $q^b = p^a$. This is impossible by the uniqueness of prime factorization.

(b) It is not true. Let $q = p^2$.

(c) Suppose $\log_a(b) = k/m$. By the definition of $\log_a$, we have $b = a^{\log_a(b)} = a^{k/m}$. Taking the m^{th} power of both sides, we have $b^m = a^k$.

Conversely, suppose $b^m = a^k$. Taking the m^{th} root of both sides, we have $b = a^{k/m}$. By the definition of $\log_a$, we have $\log_a(b) = k/m$.

NT-1.26 (a) False: Let $x = 1.1$ and $y = 0.9$. Then $\lfloor 1.1 - 0.9 \rfloor = \lfloor 0.2 \rfloor = 0$, $\lfloor 1.1 \rfloor = 1$ and $\rfloor 0.9 \rfloor = 0$.

(b) True: Suppose $n \le x < n+1$. Then $\lfloor x \rfloor = n$ and, since $n-k \le x-k < (n-k)+1$, $\lfloor x-k \rfloor = n-k$. The same is true for the ceiling function. The statements are also true with "+" in place of "−."

(c) False: Let $k = 2$ and $x = 1.5$.

NT-1.27 (a) True: Let $n = kq + r$ where $0 \le r < k$. Then $\frac{n}{k} = q + \frac{r}{k}$ and so $q \le \frac{n}{k} < q+1$. Hence $\lfloor \frac{n}{k} \rfloor = q = \frac{n-r}{k}$.

(b) False: Take $a = b = 2$ and $x = 1/2$.

NT-1.28 We prove both of them. Let $x = n + r$ where $n \in \mathbb{Z}$ and $0 < r < 1$. Then $-x = (-n-1) + (1-r)$ where $0 < 1-r < 1$ You should verify that

$$\lfloor x \rfloor = n \qquad \lceil x \rceil = n+1 \qquad \lfloor -x \rfloor = -n-1 \qquad \lceil -x \rceil = -n.$$

Now (a) and (b) follow easily.

NT-2.1 (a) The algorithm gives $1001 > 544 > 457 > 87 > 22 > 21 > 1 > 0$. Thus $\gcd(1001, 544) = 1$ (the numbers are "relatively prime") and 1 is the only common divisor.

(b) The algorithm gives $3510 > 672 > 150 > 72 > 6 > 0$. Thus $\gcd(3510, 652) = 6$ and the common divisors are the divisors of 6, namely 1, 2, 3 and 6.

Both answers can be checked by factoring the numbers looking at the result to find the gcd. For example $1001 = 7 \times 11 \times 13$ and $544 = 2^5 \times 17$, so they have no common factor.

NT-2.2 The algorithm gives $252 > 180 > 72 > 36 > 0$. The common divisors are the divisors of $\gcd(252, 180) = 36$. Since $36 = 2^2 \times 3^2$, the common divisors are found by multiplying one of $\{1, 2, 2^2\}$ by one of $\{1, 3, 3^2\}$. We obtain 1, 2, 3, 4, 6, 9, 12, 18, 36.

NT-2.3 The Euclidean algorithm gives $59400 > 16200 > 10800 > 5400 > 0$. Thus $\gcd(59400, 16200) = 5400$. Factoring: $5400 = 2^3 \times 3^3 \times 5^2$. The common divisors are of the form $2^a \times 3^b \times 5^c$ where $0 \le a \le 3$, $0 \le b \le 3$ and $0 \le c \le 2$. There are four choices for a, four for b, and three for c. Thus there are $4 \times 4 \times 3 = 48$ common divisors.

NT-2.4 We compute the remainders and quotients:

$$\begin{array}{ccccccccc} 252 & > & 180 & > & 72 & > & 36 & > & 0 \\ & & 1 & & 2 & & 2 & & \end{array}$$

Thus $72 = 252 - 1 \times 180$ and $36 = 180 - 2 \times 72$ whence

$$\begin{aligned} 36 &= 180 - 2 \times (252 - 1 \times 180) = 180 - 2 \times 252 + 2 \times 180 \\ &= -2 \times 252 + 3 \times 180. \end{aligned}$$

Hence $A = -2$ and $B = 3$.

NT-2.5 We can proceed as in the previous exercise; however, to keep numbers smaller, we could first divide m and n by a common factor; that is any divisor of $\gcd(59400, 16200)$, which we found in Exercise 2.3 to be 5400. To keep it simple, we'll just divide by 100. Computing the remainders and quotients:

$$\begin{array}{ccccccccc} 594 & > & 162 & > & 108 & > & 54 & > & 0 \\ & & 3 & & 1 & & 2 & & \end{array}$$

Thus $108 = 594 - 3 \times 162$ and $54 = 162 - 1 \times 108$ whence

$$\begin{aligned} 54 &= 162 - 1 \times 108 = 162 - 1 \times (594 - 3 \times 162) \\ &= -1 \times 594 + 4 \times 162. \end{aligned}$$

Hence $A = -1$ and $B = 4$.

NT-2.6 We compute the remainders and quotients:

$$\begin{array}{ccccccccccccccc} 163 & > & 86 & > & 77 & > & 9 & > & 5 & > & 4 & > & 1 & > & 0 \\ & & 1 & & 1 & & 8 & & 1 & & 1 & & 4 & & \end{array}$$

We won't bother to list the equations for each remainder, but just use them as needed. We have

$$\begin{aligned} 1 &= 5 - 1 \times 4 = 5 - 1 \times (9 - 1 \times 5) \\ &= -1 \times 9 + 2 \times 5 = -1 \times 9 + 2 \times (77 - 8 \times 9) \\ &= 2 \times 77 - 17 \times 9 = 2 \times 77 - 17 \times (86 - 1 \times 77) \\ &= -17 \times 86 + 19 \times 77 = -17 \times 86 + 19 \times (163 - 1 \times 86) \\ &= 19 \times 163 - 36 \times 86. \end{aligned}$$

NT-2.7 One way to do it is to note that, since $\gcd(a, b) \mid a$ and $a \mid \operatorname{lcm}(a, b)$, it follows that $\gcd(a, b) \mid \operatorname{lcm}(a, b)$ by Exercise 1.13(b).

Another way to do it is to use the prime factorizations in Theorem 6. The power of p_i in $\gcd(a, b)$ is $\min(e_i, f_i)$ and the power of p_i in $\operatorname{lcm}(a, b)$ is $\max(e_i, f_i)$. Since $\min(e_i, f_i) \le \max(e_i, f_i)$, divisibility follows.

NT-2.8 (a) $120 = 2^3 \times 3 \times 5$ and $108 = 2^2 \times 3^3$. Thus $\operatorname{lcm}(120, 108) = 2^3 \times 3^3 \times 5 = 1080$.

(b) By the Euclidean algorithm (We omit the steps.), we have $\gcd(120, 108) = 12$. Since $\gcd(a, b)\operatorname{lcm}(a, b) = ab$, we have $\operatorname{lcm}(120, 108) = 120 \times 108/12 = 1080$.

NT-2.9 Since $a \mid b$ and $b \mid b$, b is a common multiple of a and b. It is clearly the *least* strictly positive multiple of b and so is the *least* common multiple of a and b.

NT-2.10 As in the example, A sends $11^{13} \,\%\, 163 = 19$ to B. However, B sends $11^{15} \,\%\, 163 = 17$ to A. Now A computes $17^{13} \,\%\, 163 = 142$ and B computes $19^{15} \,\%\, 163$ which, of course, is also 142. This is their shared key K.

NT-2.11 We use the notation of the example. Suppose computer A chooses $s = 1$. It then sends $S = b^1 = b$, so if Joe sees that b is sent by computer A, he knows that $s = 1$. Computer B sends T and the shared secret is $K = T^s = T$. Since Joe sees T, he knows K.

NT-2.12 Since N is a prime, $\phi(N) = N - 1$. Joe solves the equation $ed = 1 \pmod{(N - 1)}$ for d using the method in Example 13. Since he has d, he can compute $C^d \,\%\, N$, which equals M for the same reason explained in Example 17.

NT-2.13 We need to compute $2^d \,\%\, N$; that is $2^{37} \,\%\, 77$. This can be done in a variety of ways. Here is one way to do it without even using a calculator, with all calculations modulo 77:

$$\begin{array}{lll} 2^7 = 128 \equiv 51, & 2^8 \equiv 2 \times 51 \equiv 25, & 2^{10} \equiv 4 \times 25 \equiv 23, \\ 2^{12} \equiv 4 \times 23 \equiv 15, & 2^{24} \equiv 15 \times 15 = 225 \equiv -6, & \\ 2^{36} \equiv (-6) \times 15 = -13, & 2^{37} \equiv 2 \times (-13) \equiv 51. & \end{array}$$

NT-2.14 Since $N = 5 \times 13$, $\phi(N) = 4 \times 12 = 48$. Thus we must solve $7d = 1 \bmod 48$. We can do this by writing $7d + 48x = 1$ and using Example 13. We omit details. In this case, we could also observe that $7 \times 7 = 49$ and so $d = 7$.

NT-2.15 Since $ed = 1 \pmod{\phi(N)}$, $\phi(N)$ must divide $ed - 1$. Since $\phi(N) = (p-1)(q-1)$, it is even and so $ed - 1$ is even. Thus ed is odd. Hence both d and e are odd.

Solutions for Sets and Functions

SF-1.1 (a) Yes.

(b) No. 2 is in $\{1,2,3,4\}$ but $\{2\}$ is not.

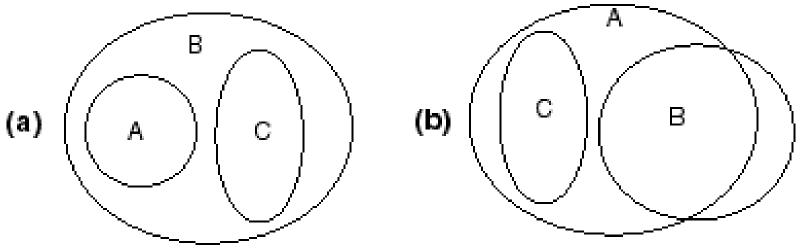
(c) Yes.

(d) Yes. All elements of $\{1,2\}$ (namely 1 and 2) are also elements of $\{1,\ 2,\ \{1,2\},\ \{3,4\}\}$.

(e) No. $\{1\}$ is an element, but 1 is not.

(f) Yes. A set is always a subset of itself.

SF-1.2 Be sure to draw these diagrams in "most general form." In (b), for example, B and C are disjoint, but A and B should show no special relationship.



SF-1.3 (a) In lexicographic order, the elements of $A \times B$ are

$$(w,a),\ (w,b),\ (x,a),\ (x,b),\ (y,a),\ (y,b),\ (z,a),\ (z,b).$$

This is the order that the words *wa*, *wb*, *xa*, *xb*, etc., would appear in Webster's Baby-Talk Dictionary. The set $A \times B = \{(w,a),(w,b),(x,a),(x,b),(y,a),(y,b),(z,a),(z,b)\}$, when written in braces, does not formally imply any particular ordering of the elements. Generally though, any representation of a set will utilize some implicit ordering of the elements as a part of the "data structure" used.

(b) In lexicographic order (called lex order for short), the elements of $B \times A$ are

$$(a,w),\ (a,x),\ (a,y),\ (a,z),\ (b,w),\ (b,x),\ (b,y),\ (b,z).$$

(c) (w,w), (w,x), (w,y), (w,z), (x,w), (x,x), (x,y), (x,z), (y,w), (y,x), (y,y), (y,z), (z,w), (z,x), (z,y), (z,z).

(d) (a,a), (a,b), (b,a), (b,b).

SF-1.4 (a) In lex order the list is $(1,(u,m))$, $(1,(u,n))$, $(1,(v,m))$, $(1,(v,n))$, $(2,(u,m))$, $(2,(u,n))$, $(2,(v,m))$, $(2,(v,n))$, $(3,(u,m))$, $(3,(u,n))$, $(3,(v,m))$, $(3,(v,n))$. This list has twelve elements, each a pair of elements. The first elements of the pair are ordered by the order on integers $(1,2,3)$. The second elements are ordered lexicographically based on the order of the alphabet. Lexicographic order as we are using it deals with "words over an alphabet," where the underlying alphabet is linearly ordered, or equivalently products of linearly ordered sets. Lexicographic order is itself a linear order.

(b) In lex order: $((1,u),m)$, $((1,u),n)$, $((1,v),m)$, $((1,v),n)$, $((2,u),m)$, $((2,u),n)$, $((2,v),m)$, $((2,v),n)$, $((3,u),m)$, $((3,u),n)$, $((3,v),m)$, $((3,v),n)$. The first components of these pairs are ordered lexicographically based on lex order of $A\times B$ (numerical in the first component and alphabetic in the second component).

(c) In lex order: $(1,u,m)$, $(1,u,n)$, $(1,v,m)$, $(1,v,n)$, $(2,u,m)$, $(2,u,n)$, $(2,v,m)$, $(2,v,n)$, $(3,u,m)$, $(3,u,n)$, $(3,v,m)$, $(3,v,n)$. This is lex order on $A\times B\times C$ based on numerical order in the first component and alphabetic order in each of the remaining two components. As a set,

$$\begin{aligned}A\times B\times C = \big\{&(1,u,m),(1,u,n),(1,v,m),(1,v,n),(2,u,m),(2,u,n),\\ &(2,v,m),(2,v,n),(3,u,m),(3,u,n),(3,v,m),(3,v,n)\big\}.\end{aligned}$$

SF-1.5 (a) Here is the set of palindromes of length less than or equal to 4, listed in lex order: ϵ, x, xx, xxx, xxxx, xyx, xyyx, y, yxxy, yxy, yy, yyy, yyyy.

(b) In length-first lex order: x, xx, xy, xxx, xxy, xyx, xyy. In (ordinary) lex order: x, xx, xxx, xxy, xy, xyx, xyy. Do you see how to describe the difference? If a dictionary used length-first lex, zoo would come before able in the dictionary.

(c) xxxx, xxxy, xxyx, xxyy, xyxx, xyxy, xyyx, xyyy, yxxx, yxxy, yxyx, yxyy, yyxx, yyxy, yyyx, yyyy.

SF-1.6 We omit the Venn diagram. There can be more than one example in each case, so your examples may not be the same as the ones given here.

(a) Take A and B to be nonempty disjoint sets and take $C=A$.

(b) Take $C=\emptyset$ and $A\neq\emptyset$.

(c) Take $A=C\neq\emptyset$ and take $B=\emptyset$. The left hand side is A, the right hand side is $\emptyset$.

(d) Take $C=\emptyset$ and take A to be a proper subset of B; that is, $A\subseteq B$, but $A\neq B$.

(e) Take C to be nonempty, $A=C$, $B=\emptyset$.

(f) Take $A=B=C\neq\emptyset$. Then $A-(B-C)=A$, $(A-B)-C=\emptyset-C=\emptyset$.

SF-1.7 (a) Suppose $x\in A$. Since $A\subseteq B$ and $A\subseteq C$, $x\in B$ and $x\in C$. Thus $x\in B\cap C$ and so $A\subseteq B\cap C$.

(b) Suppose $x\in A\cup B$. Thus either $x\in A$ or $x\in B$. Since $A\subseteq C$ and $B\subseteq C$, $x\in C$. Thus $A\cup B\subseteq C$.

SF-1.8 If $x\in(A-B)\cap(C-B)$, then $x\in A-B$ and hence $x\in A$. Also, $x\in C-B$ and hence $x\in C$. Thus, $x\in A\cap C$. Also, $x\notin B$ because $x\in A-B$. Since $x\in A\cap C$ and $x\notin B$, $x\in(A\cap C)-B$. Thus $(A-B)\cap(C-B)\subseteq(A\cap C)-B$.

Conversely, suppose $x\in(A\cap C)-B$. Then $x\in A$ and $X\in C$ but $x\notin B$. Thus $x\in A-B$ and $x\in C-B$, and so $x\in(A-B)\cap(C-B)$. Thus $(A\cap C)-B\subseteq(A-B)\cap(C-B)$.

Thus, $(A-B)\cap(C-B)=(A\cap C)-B$. Note the general form of the element argument used to show two sets X and Y are equal. First assume x is in X and show it is in Y, then assume x is in Y and show it is in X. You must show both directions.

SF-1.9 (a) Let U be the universal set. If $A \subseteq B$, then we show that $U - B \subseteq U - A$. Suppose $x \in U - B$. Then $x \notin B$. Since $A \subseteq B$, $x \notin A$. Thus $x \in U - A$. Thus $U - B \subseteq U - A$.

(b) Assume $x \in A \cap C$. Since $A \subseteq B$, $x \in B$. Thus $x \in B \cap C$ and so $A \cap C \subseteq B \cap C$.

(c) By (a), $A \subseteq B$ implies that $B^c \subseteq A^c$. With (b) applied to C^c, this implies that $B^c \cap C^c \subseteq A^c \cap C^c$. By (a), this implies that $(A^c \cap C^c)^c \subseteq (B^c \cap C^c)^c$. By DeMorgan's rule, this implies that $A \cup C \subseteq B \cup C$, which is what was to be shown.

SF-1.10 A mathematician would make use of "if and only if" statements used in succession here, with "iff" standing for "if and only if."

(a) $(x,y) \in A \times (B \cup C)$ iff $(x \in A)$ and $(y \in B \cup C)$
iff $(x \in A)$ and $(y \in B$ or $y \in C)$
iff $(x \in A$ and $y \in B)$ or $(x \in A$ and $y \in C)$
iff $\Big((x,y) \in A \times B\Big)$ or $(x,y) \in A \times C\Big)$ iff $(x,y) \in (A \times B) \cup (A \times C)$.
Thus $A \times (B \cup C) = (A \times C) \cup (A \times C)$.

(b) $(x,y) \in A \times (B \cap C)$ iff $(x \in A)$ and $(y \in B \cap C)$
iff $(x \in A)$ and $(y \in B$ and $y \in C)$
iff $(x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$
iff $(x,y) \in A \times B$ and $(x,y) \in A \times C$ iff $(x,y) \in (A \times B) \cap (A \times C)$.
Thus $A \times (B \cap C) = (A \times C) \cap (A \times C)$.

Note: This exercise shows that Cartesian product × distributes over both set union and intersection. You should draw a picture that represents these identities. One way is to use the Cartesian plane $\mathbb{R}^2$ just like you use in high school math. Let $[s,t] = \{x \mid x \in \mathbb{R} \text{ and } s \leq x \leq t\}$. Let $A = [0,3]$, $B = [0,1.25]$ and $C = [.75,2]$. Show the sets in the identities of (a) and (b) above.

SF-1.11 (a) Using $D - E = D \cap E^c$, we must prove that $(A \cap B^c) \cap C^c = A \cap (B \cup C)^c$. By the associative law and then DeMorgan's law,

$$(A \cap B^c) \cap C^c = A \cap (B^c \cap C^c) = A \cap (B \cup C)^c.$$

(b) Use (a) with the names of B and C interchanged to obtain $(A - C) - B = A - (C \cup B)$, which equals $A - (B \cup C)$ by the commutative law. By (a), this equals $(A - B) - C$.

(c) This is the same as proving $(A \cap B^c) \cup (B \cap A^c) = (A \cup B) \cap (A \cap B)^c$. By DeMorgan's law, the right side is $(A \cup B) \cap (A^c \cup B^c)$. Thus we want to prove $(A \cap B^c) \cup (B \cap A^c) = (A \cup B) \cap (A^c \cup B^c)$. The left side has $\cup$ as the outer operation and $\cap$ as the inner. The right side is just the reverse. Repeated use of the distributive, commutative and associative laws will convert one form to the other. We have

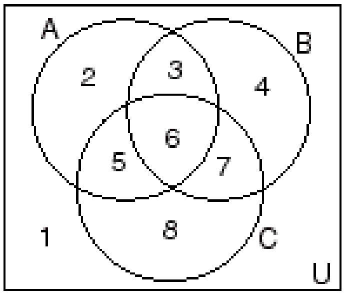
$$\begin{aligned}(A \cap B^c) \cup (B \cap A^c) &= \Big(A \cup (B \cap A^c)\Big) \cap \Big(B^c \cup (B \cap A^c)\Big) \\ &= (A \cup B) \cap (A \cup A^c) \cap (B^c \cup B) \cap (B^c \cup A^c).\end{aligned}$$

Since $X \cup X^c$ is the universal set U and since $X \cap U = X$, this becomes

$$(A \cup B) \cap U \cap U \cap (B^c \cup A^c) = (A \cup B) \cap (B^c \cup A^c),$$

which is what we needed to prove.

SF-1.12 (a) True. Below is the Venn diagram with the regions numbered 1 to 8. $A-C$ consists of regions $\{2,3\}$, $B-C$ consists of regions $\{3,4\}$, and $A-B$ consists of regions $\{2,5\}$. There is no region common to all three of these sets, so $(A-C)\cap(B-C)\cap(A-B)=\emptyset$.

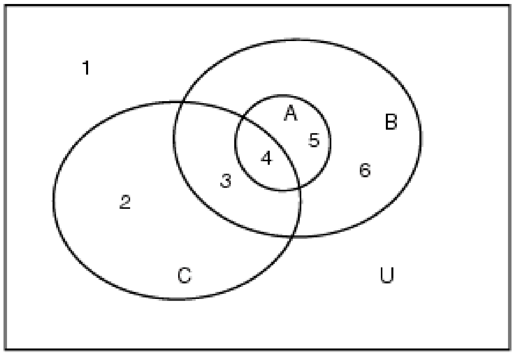


Here is an algebraic proof as well.

$$(A-C)\cap(B-C)\cap(A-B)=A\cap C^c\cap B\cap C^c\cap A\cap B^c=A\cap C^c\cap C^c\cap A\cap(B\cap B^c)=\emptyset$$

since $B\cap B^c=\emptyset$.

(b) True. Using the Venn diagram below, the proof that $A\cap(U-B)=\emptyset$ becomes $\{4,5\}\cap\{1,2\}=\emptyset$.

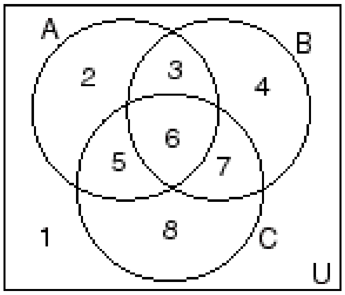


(c) False. Using the above Venn diagram: $A\cap(U-(B\cap C))$ becomes $\{4,5\}\cap\{1,2,5,6\}=\{5\}$ so the intersection is not empty. To construct a specific counterexample, we need to make sure that region 5 is not empty. That is, we want something in A that is not in C. We can take $A=B=\{a\}$ and $C=\emptyset$. Then $A\cap(U-(B\cap C))=\{a\}\neq\emptyset$.

(d) False. To find a counterexample, we can go to the Venn diagram for (a) and cross off the numbers of the regions that must be empty because of the condition $(B\cap C)\subseteq A$. In this case, it is region 7. We drop this number for all our calculations. Now $A-B$ corresponds to $\{2,5\}$ and $A-C$ to $\{2,3\}$. The intersection is $\{2\}$. Thus we can take $A=\{a\}$ and $B=C=\emptyset$. Of course, you may have seen this without using the Venn diagram, which is fine.

(e) False. Counterexample: $A=\{a\}$ and $B=\{b\}$. Then $A\times B=\{(a,b)\}$.

SF-1.13 Note that $A\oplus B=(A\cap B^c)\cup(B\cap A^c)$. By Exercise 1.11(c), $A\oplus B=A\cup B-(A\cap B)$. In words, $A\oplus B$ consists of everything in A or B that is not in both A and B. For this problem, we refer to the following Venn diagram.



(a) $B \oplus C$ consists of regions $\{3,4,5,8\}$. $A \oplus (B \oplus C)$ consists of regions $\{2,6,4,8\}$. $A \oplus B$ consists of regions $\{2,5,4,7\}$. $(A \oplus B) \oplus C$ consists of regions $\{2,4,6,8\}$. The final set of regions, $\{2,4,6,8\}$, is the same in both cases. Thus, $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.
Note: Since we have the associative and commutative laws we can combine a collection of sets using $\oplus$ in any order we wish and the answer will be the same. For example, $(A \oplus B) \oplus (C \oplus D) = D \oplus ((B \oplus C) \oplus A)$. Also note that $A \oplus (B \oplus C)$ consists of those elements that are in an *odd* number of A, B and C. This is true in general: $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ consists of those elements that are in an odd number of $A_1, A_2, \ldots, A_n$. You can apply this fact to get alternate proofs for parts (b), (c) and (d) of this problem.

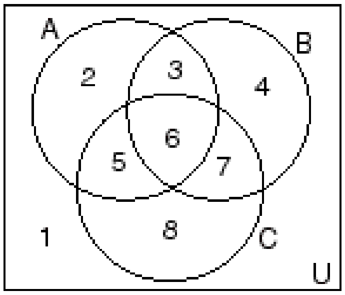
(b) $A \oplus \emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A$.

(c) $A \oplus A^c = (A \cup A^c) - (A \cap A^c) = U - \emptyset = U$. (Note: $A \oplus U = A^c$.)

(d) $A \oplus A = (A \cup A) - (A \cap A) = A - A = \emptyset$.

(e) If $A \oplus C = B \oplus C$ then $(A \oplus C) \oplus C = (B \oplus C) \oplus C$. Thus $A \oplus (C \oplus C) = B \oplus (C \oplus C)$ and so $A \oplus \emptyset = B \oplus \emptyset$. Finally, $A = B$.

SF-1.14 Use the Venn diagram:



(a) Must be disjoint. $A - B$ is regions $\{2,5\}$ and $B - C$ is regions $\{3,4\}$, so there are no regions in common.

(b) May not be disjoint. $A - B$ is regions $\{2,5\}$ and $C - B$ is regions $\{5,8\}$. Region 5 is common to both and may be nonempty.

(c) Must be disjoint. $A - (B \cup C)$ is region 2 and $B - (A \cup C)$ is region 4. There are no regions in common.

(d) May not be disjoint. $A - (B \cap C)$ consists of regions $\{2, 3, 5\}$ and $B - (A \cap C)$ consists of regions $\{3, 4, 7\}$. Region 3 is common to both and may be nonempty.

SF-1.15 (a) No because 1 appears in $\{1, 3, 5\}$ and in $\{1, 2, 6\}$.

(b) Yes because every element in $\{1, 2, \ldots, 8\}$ appears in exactly one block.

(c) Yes because a partition is a *set* and so we can ignore the fact that $\{2, 6\}$ was listed twice.

(d) No because 7 is missing.

SF-1.16 We can choose any refinement of $\{1, 3, 5\}$ (there are B_3), any refinement of $\{2, 6\}$, and any refinement of $\{4, 7, 8, 9\}$. The number of refinements is the product of the Bell numbers: $B_3 \times B_2 \times B_4 = 5 \times 2 \times 15 = 150$.

SF-1.17 (a) Suppose $x \in S \cup T$. Every element of $S \cup T$ appears in exactly one of S and T. If $x \in S$, then it appears in exactly one block σ. If $x \in T$, then it appears in exactly one block τ. Hence x appears in exactly one block of $\sigma \cup \tau$.

(b) We get each refinement of $\sigma \cup \tau$ by choosing a refinement of σ and choosing a refinement of τ. Thus there are $n_\sigma \, n_\tau$ refinements of $\sigma \cup \tau$.

SF-1.18 (a) $\{1, 2, 3\}$ has three elements. Here are the subsets and the characteristic functions with χ given as $\chi(1), \chi(2), \chi(3)$.

$\emptyset$	0,0,0	$\{1\}$	1,0,0	$\{2\}$	0,1,0
$\{1,2\}$	1,1,0	$\{3\}$	0,0,1	$\{1,3\}$	1,0,1
$\{2,3\}$	0,1,1	$\{1,2,3\}$	1,1,1		

(b) Since $X \times Y = \{(a, x), (a, y), (b, x), (b, y)\}$, we list χ in the order $\chi((a, x))$, $\chi((a, y))$, $\chi((b, x))$, $\chi((b, y))$.

$\emptyset$	0,0,0,0	$\{(a,x)\}$	1,0,0,0
$\{(a,y)\}$	0,1,0,0	$\{(a,x),(a,y)\}$	1,1,0,0
$\{(b,x)\}$	0,0,1,0	$\{(a,x),(b,x)\}$	1,0,1,0
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\{(a,x),(a,y),(b,x)\}$	1,1,1,0	$\{(a,x),(a,y),(b,x),(b,y)\}$	1,1,1,1

SF-1.19 Remember that the power set of a set S contains the empty set $\emptyset$, the set S itself, and all proper, nonempty subsets of S.

(a) Here $S = \emptyset$, which has no nonempty, proper subsets. Thus $\mathcal{P}(\emptyset) = \{\emptyset\}$. This is *not* the empty set — it is a one-element set and its element is the empty set.

(b) $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$, so $S = \{\emptyset\}$ is a set with one element. If we call this element a, then $\mathcal{P}(S) = \{\emptyset, \{a\}\}$. Replacing a with its value $\emptyset$, we have $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

(c) We are now starting with a two-element set, so it has four subsets. Thus

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \Big\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset, \{\emptyset\}\}\Big\}.$$

This looks confusing, but if you write down $\mathcal{P}(\{a, b\})$ and then replace a with $\emptyset$ and b with $\{\emptyset\}$, you should have no trouble.

Solutions for Sets and Functions

SF-1.20 (a) Since $A \subseteq A \cup B$, we have $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$. Similarly , $\mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ and so $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

If $A \subseteq B$, then $A \cup B = B$ and $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Thus $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$. Similarly, they are equal if $B \subseteq A$.

Suppose this is not the case so that $a \in A - B$ and $b \in B - A$. Then $\{a, b\} \in \mathcal{P}(A \cup B)$ but $\{a, b\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

In summary, if either $A - B = \emptyset$ or $B - A = \emptyset$, then the given sets are equal. Otherwise, $\mathcal{P}(A) \cup \mathcal{P}(B)$ is a proper subset of $\mathcal{P}(A \cup B)$.

(b) They are equal. Proof: $X \in \mathcal{P}(A \cap B)$ iff $X \subseteq A \cap B$
iff $X \subseteq A$ and $X \subseteq B$ iff $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$
iff $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. We have shown that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

(c) For any sets A and B, $\mathcal{P}(A) \times \mathcal{P}(B)$ and $\mathcal{P}(A \times B)$ have no elements in common! The set $\mathcal{P}(A) \times \mathcal{P}(B)$ consists of pairs of subsets (S, T) where $S \subset A$ and $T \subset B$. The set $\mathcal{P}(A \times B)$ has elements W which are collections of pairs (x, y) where $x \in A$ and $y \in B$. The pair of sets (S, T) cannot equal the set of pairs W.

Let's count the number of elements. Recall that $|\mathcal{P}(C) = 2^{|C|}$ and $|U \times V| = |U| \cdot |V|$. Thus

$$|\mathcal{P}(A) \times \mathcal{P}(B)| = |\mathcal{P}(A)| \cdot |\mathcal{P}(B)| = 2^{|A|} 2^{|B|} = 2^{|A|+|B|}$$

and

$$|\mathcal{P}(A \times B)| = 2^{|A \times B|} = 2^{|A| \cdot |B|}.$$

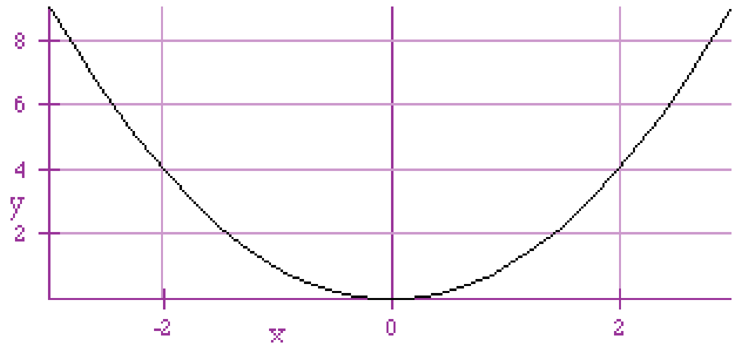
These two numbers will be equal if and only if $|A| + |B| = |A| \cdot |B|$. Thus we need to know what the solutions of $x + y = xy$ in nonnegative integers. We can rewrite this as $xy - x - y + 1 = 1$, which can be written $(x - 1)(y - 1) = 1$. The product of two integers is 1 if and only if both integers are $+1$ or both integers are -1. Thus the only solutions are $x - 1 = y - 1 = 1$ and $x - 1 = y - 1 = -1$. The first case says $|A| = |B| = 2$ and the second case says that $A = B = \emptyset$. In the first case, the two sets in the problem have $2^4 = 16$ elements and in the second case the two sets are $\{\emptyset\}$ and $\{(\emptyset, \emptyset)\}$. In all other cases, $|A| \cdot |B| > |A| + |B|$, which means that $\mathcal{P}(A \times B)$ has more elements than $\mathcal{P}(A) \times \mathcal{P}(B)$.

SF-1.21 We know that a set with m elements has 2^m subsets. Since T_1 is the set of all subsets of $\{2, \ldots, n\}$ (which has $n - 1$ elements), $|T_1| = 2^{n-1}$.

What about S_1? Here's one way. Every subset of S is either in S_1 (if it contains 1) or in T_1 (if it does not contain 1), but not both. Thus $|S_1| + |T_1| = 2^{|S|} = 2^n$ and so $|S_1| = 2^n - |T_1| = 2^n - 2^{n-1} = 2^{n-1}$.

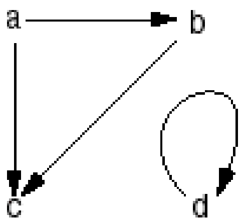
Here's another way. We can remove 1 from a subset in S_1 and obtain a subset in T_1. This process is reversible. Thus $|S_1| = |T_1|$.

SF-2.1 In the figure below, the set $\mathbb{R} \times \mathbb{R}$ is represented in the usual manner by points in plane. Of course, the figure only shows a portion of $\mathbb{R} \times \mathbb{R}$. Points satisfying the relation are dark, forming a curve — the parabola.

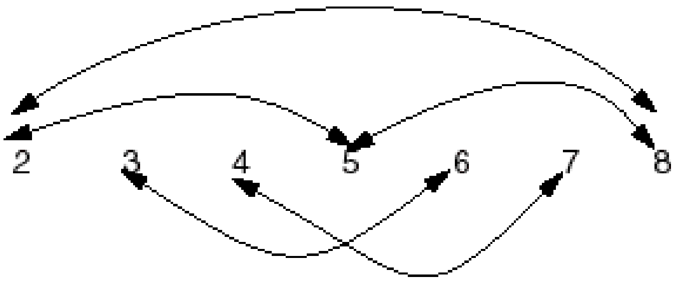


SF-2.2 (a) No (not true for empty set). (b) Yes. (c) No.

SF-2.3 (a) Pictorially, this relation S on B can be drawn as follows (there are many other ways ...):



(b) Since the relation is symmetric, an arrow from a to b means there is also one from b to a. To avoid cluttering the figure, we draw this as an arrow with heads at both ends.



SF-2.4 Altogether, there are sixteen relations of which four are functional. We can list those that are *not* functional by listing all sixteen relations and then removing those that are functional. A subset S of $\{a, b\} \times \{x, y\}$ will be functional if exactly one of (a, x) and (a, y) is in the subset (defines $f(a)$) and exactly one of (b, x) and (b, y) is in the subset (defines $f(b)$). In the following table, each column gives a subset of $\{a, b\} \times \{x, y\}$ in characteristic function form. The last row indicates whether it is functional (Y) or not (N).

$\chi((a,x))$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$\chi((a,y))$	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
$\chi((b,x))$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
$\chi((b,y))$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
functional?	N	N	N	N	N	Y	Y	N	N	Y	Y	N	N	N	N	N

SF-2.5 $S = \{(3,6),(4,4),(5,5)\}$ and $S^{-1} = \{(6,3),(4,4),(5,5)\}$.

SF-2.6 (a) $|A \times B| = mn$. For any set S there are $2^{|S|}$ subsets. Thus there are 2^{mn} subsets of $A \times B$ or, same thing, 2^{mn} relations from A to B.

(b) Consider the definition of a function. Each $x \in A$ must be paired with exactly one $y \in B$. For each $x \in A$ there are $|B|$ choices for $y \in B$. List the elements of A as $a_1, a_2, \ldots, a_{|A|}$. There are $|B|$ choices to pair with a_1, $|B|$ choices to pair with a_2, etc. until finally $|B|$ choices to pair with $a_{|A|}$. The total number of choices is $|B| \cdot |B| \cdots |B| = |B|^{|A|}$.

SF-2.7 There are 17 edges in the digraph. To explain, list them all or draw a picture of the digraph.

SF-2.8 (a) No. Since no order is given for the domain, we cannot specify f in one-line form. Since f takes the value 3 two times, it is not an injection and hence not a bijection. Since we know the range, we can see that f is a surjection.

(b) We know the range and domain. Using the implicit order of the domain, we know f. Its two-line form is $\begin{pmatrix} 1 & 2 & 3 \\ ? & < & + \end{pmatrix}$. It is an injection but not a surjection or a bijection since it never takes the value $>$.

(c) We know the range and domain and are given the function values. The two-line form is $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 3 & 2 \end{pmatrix}$. Using the implicit order of the domain, the one-line form $(4,3,2)$. It is an injection but not a surjection or a bijection since it never takes the value 1.

SF-2.9 (a) The domain and range of f are specified and f takes on exactly two distinct values. Since the coimage has blocks with more than one element, f is not an injection. Since we don't know what values f takes on, it is not completely specified; however, it is not a surjection since it would have to take on all 4 values in its range and the coimage has only two blocks.

(b) Since each block of the coimage has just one element, f is an injection. Since $|\text{Coimage}(f)| = 5 = |\text{range of } f|$, f is a surjection. Thus f is a bijection and, since the range and domain are the same, f is a permutation. In spite of all this, we don't know $f(x)$ for any $x \in \underline{5}$.

(c) We know the domain and range of f since $\{f^{-1}(2), f^{-1}(4)\}$ is a partition of the domain, we know $f(x)$ for all $x \in \underline{5}$. Thus we know f completely. It is neither a surjection nor an injection.

(d) We know that f is a surjection. It cannot be an injection because the domain is larger than the range. We cannot specify f.

(e) This specification is nonsense: Since Image(f) must be a subset of the range, it cannot have more than four elements.

(f) This specification is nonsense: Since each block of Coimage(f) corresponds to a different element of the image of f, it cannot have more than four blocks.

SF-2.10 (a) and (b) are contrapositives of each other and hence logically equivalent. Both are correct definitions of injective or one-to-one.

(c) No. What is being defined is a function and not all functions are one-to-one. For example, $A = \{a, b\}$, $B = \{c\}$, $f(a) = f(b) = c$ satisfies the definition.

(d) Correct. This is the definition of one-to-one.

SF-2.11 (a) g is one-to-on because $g(s) = g(t)$ means $3s - 1 = 3t - 1$ and so $s = t$.

(b) g is not onto. For example $g(s) = 0$ would mean $3s - 1 = 0$ and so $s = 1/3$, which is not an integer.

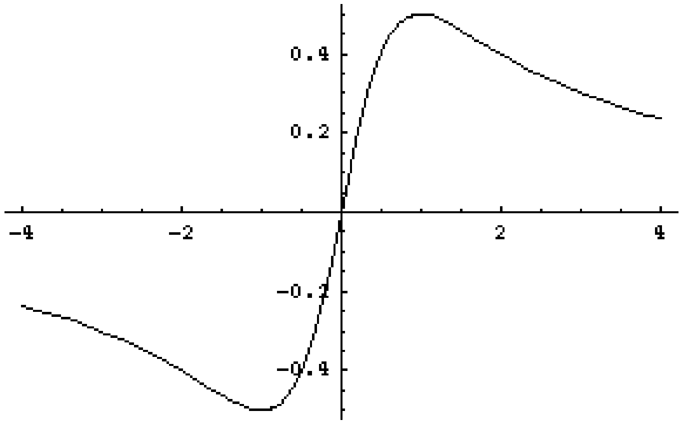
(c) g is onto in this case. Given $s \in \mathbb{R}$, we must find $x \in \mathbb{R}$ such that $g(x) = s$. In other words, we want $3x - 1 = s$, so let $x = (s+1)/3$. Then $g(x) = 3(s+1)/3 - 1 = s$.

SF-2.12 There are at least three ways to do this problem:

- Either find $x \neq y$ such that $f(x) = f(y)$ or prove that $f(x) = f(y)$ implies that $x = y$. This is the straightforward method, but it is not always convenient.
- Use calculus to show that $f(x)$ is strictly monotonic and hence one-to-one.
- Look at a carefully drawn graph of $f(x)$. This works if f is *not* one-to-one — you'll be able to see that there are x and y with $f(x) = f(y)$. You can't be sure when f is one-to-one because you can't graph $f(x)$ for *all* x in the domain. Calculus may help in this case.

We'll use various methods here.

(a) f is not one-to-one. Here is what the graph of $x/(x^2 + 1)$ looks like:



(b) f is one-to-one. It is easier to see if we write $f(x) = 2 + 1/x$. Suppose $f(s) = f(t)$. Then $1/s = 1/t$ and so $s = t$.

(c) f is one-to-one. $f(x) = 1 - 2/(x + 1)$. Proceed as in (b).

SF-2.13 It's easy to convert between one-line and two-line form: If the top line of two-line form is arranged in order $(1, 2, \ldots)$, then the bottom line is the one-line form. Hence we usually omit one or the other of these forms below. (a) For (1,5,7,8)(2,3)(4)(6), the two-line form is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 4 & 7 & 6 & 8 & 1 \end{pmatrix}$. The inverse is (1,8,7,5)(2,3)(4)(6) in cycle form, (8,3,2,4,1,6,5,7) in one-line form.

(b) For $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 7 & 2 & 6 & 4 & 5 & 1 \end{pmatrix}$, the cycle form is (1,8)(2,3,7,5,6,4). The inverse is (1,8)(2,4,6,5,7,3) in cycle form and (8,4,2,6,7,5,3,1) in one-line form

(c) The one-line form (5,4,3,2,1) has the cycle form (1,5)(2,4)(3). The permutation is its own inverse.

(d) The cycle form (5,4,3,2,1) is not in standard form. The standard form in (1,5,4,3,2). Its the one-line form is (5,1,2,3,4). Its inverse is (1,2,3,4,5) in cycle form and (2,3,4,5,1) in one-line form.

SF-2.14 Let $A = \{a_1, a_2, \ldots\}$.

(a) Note that $f(a_1) \in B$, $f(a_2) \in B - \{f(a_1)\}$ and $f(a_1) \in B - \{f(a_1), f(a_2)\}$. Thus there are $|B| = 3$ choices for $f(a_1)$, then $|B| - 1 = 2$ choices for $f(a_2)$ once $f(a_1)$ is chosen, etc. This gives $|S| = 3 \times 2 \times 1 = 6$.

(b) $5 \times 4 \times 3 = 60$ by the reasoning in (a).

(c) If $m > n$ the answer is zero. Otherwise, reasoning as in (a) the answer is

$$\overbrace{n \times (n-1) \times (n-2) \times \cdots \times (n-m+1)}^{m \text{ factors}}$$

This is called the "falling factorial" and written $(n)_m$.
Alternatively, one can choose the m elements of the image in $\binom{n}{m}$ ways and then write those m things in one-line form in $m!$ ways so the answer is $\binom{n}{m}\,m! = (n)_m$.

SF-2.15 (a) Assume $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is onto. Must f and g be onto? The answer is no. Let $X = Y = \{a, b\}$ and let $Z = \{c\}$. Let $f(a) = f(b) = b$ and $g(a) = g(b) = c$. Then $g \circ f : X \to Z$ is onto but f is not onto. In this example, g is onto. That is always the case. To prove that g is onto, we pick any $z \in Z$ and show that there is a $y \in Y$ such that $g(y) = z$. Since $g \circ f$ is onto, there is an $x \in X$ such that $g \circ f(x) = g(f(x)) = z$. Take $y = f(x)$.

(b) In this case, f must be one-to-one, but g need not be. We let you find an example for g. We prove f is one-to-one. Suppose $f(x_1) = f(x_2)$. Then $g(f(x_1)) = g(f(x_2))$. Since $g \circ f$ is one-to-one, $x_1 = x_2$. We have just shown that $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. Hence f is one-to-one.

SF-2.16 We write "iff" for "if and only if."

(a) True. Proof: $y \in f(A \cup B) \quad$ iff $\quad \exists x \in (A \cup B),\ f(x) = y$
iff $\quad \Big(\exists x \in A,\ f(x) = y\Big)$ or $\Big(\exists x \in B,\ f(x) = y\Big)$
iff $\quad y \in f(A)$ or $y \in f(B) \quad$ iff $\quad y \in (f(A) \cup f(B))$.

(b) False. Counterexample: Let $A = \{1\}$, $B = \{2\}$ and $f(1) = f(2) = 3$. Then $f(A \cap B) = f(\emptyset) = \emptyset$ and $f(A) \cap f(B) = \{3\}$.

(c) False. Counterexample: Let $A = \{1\}$, $B = \{2\}$ and $f(1) = f(2) = 3$. Then $f(A - B) = f(A) = \{3\}$ and $f(A) - f(B) = \{3\} - \{3\} = \emptyset$.

(d) True. Proof: $x \in f^{-1}(C \cap D)$ iff $f(x) \in C \cap D$
iff $f(x) \in C$ and $f(x) \in D$ iff $x \in f^{-1}(C)$ and $x \in f^{-1}(D)$
iff $x \in f^{-1}(C) \cap f^{-1}(D)$.

SF-2.17 (a) False. Find the simplest counter example you can!

(b) False. Suppose $X = \{a\}$ and $Y = \{c, d\}$. Let $f(a) = c$ and take the set C of the problem to be Y. Is the statement true for this example? Remember, to show that $P = Q$ for two sets P and Q, you must show that P is a subset of Q and Q is a subset of P.

(c) True. Proof: $x \in (g \circ f)^{-1}(E)$ iff $g(f(x)) \in E$
iff $f(x) \in g^{-1}(E)$ iff $x \in f^{-1}(g^{-1}(E))$.

SF-2.18 (a) Let the elements of the domain be $\{a, b, c\}$ and the elements of the codomain be $\{u, v\}$. We can construct two onto functions f with a given coimage $\{S, T\}$:

- one by taking $S = f^{-1}(u)$ and $T = f^{-1}(v)$,
- one by taking $S = f^{-1}(v)$ and $T = f^{-1}(u)$.

The number of choices for $\{S, T\}$ is the number of partitions of $\{a, b, c\}$ into two blocks. There are three such partitions: $\big\{\{a, b\}, \{c\}\big\}$, $\big\{\{a, c\}, \{b\}\big\}$ and $\big\{\{b, c\}, \{a\}\big\}$. Thus the answer is $2 \times 3 = 6$.

(b) There no onto functions in this case. For an onto function $|\text{Image}(f)| = |\text{Range}(f)|$. For any function, $|\text{Image}(f)| \le |\text{Domain}(f)|$. Thus $|\text{Range}(f)| \le |\text{Domain}(f)|$ for an onto function. In other words $|B| \le |A|$. In this case, that would mean $5 \le 3$, which is not true.

(c) The number of possible coimages is equal to the number of partitions of a set of four elements into two blocks. Each such coimage gives rise to two onto functions, just like in part (a). Rather than list all partitions of four things into two blocks, we note that it is $S(4, 2)$ by definition and use the table in the text to see that $S(4, 2) = 7$. Hence there are $2 \times 7 = 14$ onto functions.

(d) If $m < n$ there are none because of the reasoning in part (b). Suppose that $m \ge n$. We proceed as in (c):

- Given a partition of A, we claim $n!$ onto functions have this partition as coimage. Why is this? Each block must be mapped to a *different* element of B by a function that has this partition as coimage. List the blocks in some order. There are n choices for the image of the first block. This leaves $n - 1$ choices for the image of the second block. This leaves $n - 2$ choices for the image of the third block, and so on. Thus we get $n(n - 1)(n - 2) \cdots = n!$ possible functions.
- Since the number of blocks in the coimage equals the size of the image, you can see that we must partition A into $|B|$ blocks. (Look at the discussion in part (b) if this is unclear.) Thus there are $S(m, n)$ possible partitions.

Since there are $n!$ onto functions for each of the $S(m, n)$ partitions, the answer is $n!\,S(m, n)$.

(e) Since we are dealing with onto functions, $k = n$. Now apply the formula and use the fact that $\binom{n}{n} = 1$.

SF-2.19 One way is to fill in the brief explanation given in the text. Here is another.

- Let $C = \text{Image}(f)$, the image of A. There are $\binom{n}{k}$ possible choices for C since it is a k-subset of B.
- How many functions are there with a given C? They are the onto functions from A to C. We counted them in part (d) of the previous exercise, except now the range is a k-set instead of an n-set. Thus there are $k!\,S(m,k)$ such functions.

Putting the two parts together gives the answer.

Solutions for Equivalence and Order

EO-1.1 Let $a : S \to \mathbb{N} \times \mathbb{N}$ be the function that assigns to each student x, the age of x paired with the years completed. The equivalence class partition is the coimage partition of the function a.

EO-1.2 There are d equivalence classes: $\{x,\ x{+}d,\ x{-}d,\ x{+}2d,\ x{-}2d, \ldots\}$, $x = 0, 1, 2, \ldots, d{-}1$. They form the coimage partition of the function $m(x) = x(\text{mod } d)$.

EO-1.3 Define $t(x)$ to be the truth table of x. The coimage partition of t is the set of equivalence classes. The equivalence classes correspond to sets of equivalent forms in the usual sense that they represent the same Boolean function. How many equivalence classes are there?

EO-1.4 Define a function $f(x) = x^k(\text{mod } d)$. The equivalence classes are the blocks of the Coimage(f). Can you describe the equivalence classes?

EO-1.5 This is a case where it is easy to show that the relation is reflexive, symmetric, and transitive. Defining the function f is not too bad either: $f(x) = x - \lfloor x \rfloor$. That is, $f(x)$ is x minus the least integer in x. We have reached a "cross over" point where proving directly that the relation is reflexive, symmetric, and transitive is easier (barely) than dealing with Coimage(f).

EO-1.6 There are $26 \times 26 = 676$ possible (first,last) letter pairs. Thus at least one block of the coimage of the function f that maps a name to its (first,last) letter pair must have more than one element.

EO-1.7 (a) Yes. The mapping from a set of k integers to remainder mod $k-1$ has $k-1$ blocks in its coimage and k elements in its domain.

(b) No. Take the set of integers to be $\{0,\ 1,\ 2, \ldots,\ k-1\}$. The mapping from integers to integers mod k is the identity mapping.

EO-1.8 Let's look at a particular case, say $n = 9$ so $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Choose $C = \{1, 2, 3, 4, 5\}$. No pair adds up to 10. Now suppose C has 6 elements. We claim there is a pair that adds to 10. To see why, let $f(x)$ be the set $\{x,\ (10 - x)\}$ for $x \in S$. Image(f) has exactly 5 elements and so Coimage(f) has exactly 5 blocks. Now restrict f to C. The domain has 6 elements but the coimage has at most 5 blocks. Therefore there must be two distinct elements x, y in C that have the same value. Thus $\{x, (10{-}x)\} = \{y, (10{-}y)\}$. and, since $x \neq y$, $x = 10{-}y$. Thus $x{+}y = 10$. For general n, $f(x) = \{x,\ (n + 1 - x)\}$ and Coimage(f) has $\lceil n/2 \rceil$ blocks. Thus $k = \lceil n/2 \rceil + 1$.

EO-1.9 This is a more elementary idea than the pigeon-hole principle. Suppose n is even, say $n = 2j$. Note that there are $j + 1$ even and j odd integers in S. To be sure of getting an odd integer you must pick at least $j + 2$ elements of S. To be sure of getting an even integer, you must pick at least $j + 1$. We leave it to you to do the case $n = 2j - 1$.

EO-1.10 The primes between 1 and 50 are $P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$. There are 15 of them. Thus $k = 15$ doesn't work: Take $S = P$. We now show that $k = 16$ works. Define a function f from the set S to P by

$$f(x) = (\text{smallest prime that divides } x).$$

If S has at least 16 elements then one block of the Coimage(f) must contain at least two elements. Say $f(s) = f(t) = p$. Then p is the smallest prime dividing s and also the smallest prime dividing t. Hence p divides $\gcd(s, t)$ and so $\gcd(s, t) > 1$.

EO-1.11 Think about the coimage partition of the function B that maps a person to his/her birth-month. This partition has as most twelve blocks. If each block had less than three elements there would be at most $12 \times 2 = 24$ elements (persons) in the domain of B. Thus, if the domain of B contains more than 24 elements (persons) there must be at least one block in Coimage(B) with more than two elements. In other words, if there are more than 24 in a group of people, there must be at least three with the same birth-month. Thus $k = 25$.

EO-1.12 The table below shows the structure of the possible coimage partitions of f, given that no block has more than three elements. The first row indicates the possible block sizes, 1, 2, or 3. The entries in the other rows indicate how many blocks there are of that size. Thus, in the row with entries 9, 1, 1, there are 9 blocks of size 3, 1 block of size 2, and 1 block of size 1. Our solution given in the statement of the problem corresponds to the first row.

3	2	1
10	0	0
9	1	1
9	0	3
8	3	0
8	2	2
7	4	1
6	6	0

EO-1.13 Let B denote the map from persons to birth ATCs. Coimage(B) can have at most 1461 blocks. If every block had at most 3 elements then the domain of B would be no larger than $3 \times 1461 = 4383$. Thus, if the domain of B has more than 4383 elements there must be at least one block of Coimage(B) with at least 4 elements. Thus $k = 4384$.

EO-1.14 Let f be function from the set of N students to their scores (in the range 27 to 94). The codomain of f has maximum size 65. We have $65 \times 2 = 130$. Thus, $N > 130$ guarantees that 3 students must have the same score.

EO-1.15 You choose x pennies and look at the map f from these pennies to their dates. There can be at most three blocks in the coimage. If each block had three elements, then $x = 9$. Thus, you had better pick more than nine to be sure of getting one block with at least four pennies. If you pick ten pennies, one block must contain at least four pennies. Thus $N_4 = 10$.

To find N_6 a little more care must be taken. There are only four 1971 pennies so $|f^{-1}(1971)| \leq 4$. To choose the most pennies and not get at least 6 with the same date, take all four 1971 pennies, five 1968 pennies, and five 1967 pennies for a total of 14 pennies. Thus, you can choose 14 pennies and still not have six pennies with the same date. One more penny forces you to take at least six pennies of the same date. Thus $N_6 = 15$.

By the same sort of reasoning, $N_8 = 19$. (You can take all the 1968 and 1971 pennies plus 7 of the 1967 pennies without getting eight pennies with the same date.)

EO-1.16 If $n \mid t_k$ for some k, we are done, so assume that n does not divide t_k for any k. Look at the set $R = \{t_k \,\%\, n \mid k = 1, 2, \ldots, n\}$ of remainders mod n. This set has cardinality at most $n-1$, since $0 \notin R$ by assumption. Thus, by the pigeonhole principle, there must be at least two of the integers t_i and t_j that have the same value mod n. Thus, $n \mid (t_i - t_j)$.

EO-1.17 The approach is similar to previous problem. Let

$$S = \Big\{\{0\},\ \{1,\, n-1\},\ \{2,\, n-2\},\ \ldots,\ \{\lfloor n/2 \rfloor,\ \lceil n/2 \rceil\}\Big\},$$

a collection of $\lfloor n/2 \rfloor + 1$ sets, each with two elements except $\{0\}$ and, if n is even, $\{\lfloor n/2 \rfloor,\ \lceil n/2 \rceil\} = \{n/2\}$. Note that if any set in this collection has two elements, then the sum of those two elements is n. Let $R = \{t_i \mid i = 1, 2, \ldots, k\}$ be any collection of k integers and let $f : R \to S$ be a function from R to S. If $k > \lfloor n/2 \rfloor + 1$, then, by the pigeonhole principle, there must be two elements of R that are mapped to the same set of S.

Let $f(t_j)$ to be the set of S that contains the integer $t_j \,\%\, n$. If $f(t_i) = f(t_j)$, there are two possibilities:

(1) $t_i \,\%\, n = t_j \,\%\, n$ or

(2) $t_i + t_j = 0 \pmod{n}$. Thus, either $n \mid (t_i - t_j)$ or $n \mid (t_i + t_j)$. Hence $k \geq \lfloor n/2 \rfloor + 2$ will guarantee the condition of the problem. Why is this bound best possible? (That is, find an example that fails when $k = \lfloor n/2 \rfloor + 1$.)

EO-1.18 Consider an example. Suppose $n = 12$. The numbers are

$$D = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

Factoring out the highest power of two in each case, gives

$$2^0 \times 1,\ 2^1 \times 1,\ 2^0 \times 3,\ 2^2 \times 1,\ 2^0 \times 5,\ 2^3 \times 1,\ 2^0 \times 9,\ 2^1 \times 5,\ 2^0 \times 11,\ 2^2 \times 3,$$

where each number is written as $2^i \times x$ where x is odd. Define $f(2^i \times x) = x$. The function f give the "odd part" of a number. The domain of f is D and the codomain is $R = \{1, 3, 5, 7, 9, 11\}$, the odd integers in D. Note that $|R| = 6 = n/2$. If we take any subset S of D of size at least 7, then, by the pigeonhole principle, there are at least two different integers $p < q$ in S such that $f(p) = f(q)$. If $f(p) = f(q) = x$, we have that $p = 2^i \times x$ and $q = 2^j \times x$ and hence, since $p < q$, we must have $i < j$ and so $p \mid q$. This process works for any n. When n is even $|R| = n/2$ There are slight differences when n is odd, so you should check an odd case, say $n = 11$. When n is odd, $|R| = (n+1)/2$. In general, $|R| = \lfloor (n+1)/2 \rfloor = \lceil n/2 \rceil$. Thus, $m > \lceil n/2 \rceil$ works. Why is this value of m best possible? Look at the set of integers in D that are bigger than $n/2$. This set has $\lceil n/2 \rceil$ elements, and no two divide each other.

EO-1.19 (a) The sequence 1, 2, 3, $\ldots$, ι obviously works.

(b) The sequence 2, 1, 4, 3, $\ldots$, $(2k)$, $(2k-1)$, $\ldots$, (2ι), $(2\iota - 1)$ works. Why? It is clear that the longest decreasing subsequence has length 2. For each $j = 1, \ldots, \iota$, an increasing subsequence can contain at most one of $(2j)$ and $(2j-1)$.

(c) We use the idea in (b). Let S_k be the δ-long decreasing sequence

$$(\delta k),\ (\delta k - 1), \ldots,\ (\delta k - (\delta - 1)).$$

Note that its last term is $\delta(k-1)+1$. Our sequence is $S_1, S_2, \ldots, S_\iota$. A decreasing subsequence must take all of its elements from a single S_k and so has length at most δ. An increasing subsequence can take at most one element from each S_k and so has length at most ι.

EO-1.20 Since $m > q(p-1)$, by Example 11 there is either a $(q+1)$-long increasing subsequence or a p-long decreasing subsequence. We are told that the latter is not present. Thus there is a q-long increasing subsequence.

EO-1.21 (a) Since $(k-1)^2 = n^4 < m$, there must be a k-long monotone subsequence by Example 11.

(b) Since $k > n^2$, there must be an $(n+1)$-long monotone subsequence by Example 11.

(c) By (b) the subsequence of b's is monotone. Since a subsequence of a monotone sequence is monotone, the subsequence $a_{t_1}, \ldots, a_{t_{n+1}}$ is monotone by (a).

EO-1.22 The fact that each client is assigned exactly one lawyer means that the assignment relation is a function $A : \{1, 2, \ldots, 15\} \to \{1, 2, 3, 4, 5\}$. Coimage($A$) has at exactly five blocks and each block has at most four elements. (The first condition is from the fact that each lawyer is to represent at least one client; i.e., A is onto. The second condition part of the statement of the problem.) Forget, for the moment, the question asked in the problem — a pretty good general approach in this type of problem. We need to make a table of possible assignments, without including unnecessary details, so that we can get a feel for the situation.

We consider assignments (functions) A where Coimage(A) has exactly five blocks. We make a "block-size chart" for possible coimages, with the top row given block sizes, from 1 to 4. The remaining four rows show how many blocks of that size can result from various assignments A. Thus, the first row shows 1 block of size 1 (one lawyer, one client), 1 block of size 2 (one lawyer, two clients), no blocks of size 3, and 3 blocks of size 4 (3 lawyers, 4 clients).

1	2	3	4
1	1	0	3
1	0	2	2
0	2	1	2
0	1	3	1
0	0	5	0

Now that we've got a general understanding, let's go back and find out what the question is! It was "Show that if two lawyers are assigned less than three clients, at least two must be assigned four clients." The truth of this is evident from our table. Rows one and two represent the situation where two lawyers are assigned less than three lawyers. In both cases, 2 or more (3 for row 1) are assigned four clients.

We're done but we could use the table to formulate other problems. For example

- Show that if less than two lawyers are assigned less than three clients then at least four lawyers must be assigned more than two clients.

- Show that at least three lawyers must be assigned three or more clients.

Can you do these problems by using the chart? The last question can be answered easily without the chart. Can you do it without the chart?

EO-2.1 (a) This relation is neither reflexive ($2 \not R\ 2$), symmetric ($0\ R\ 3$ and $3 \not R\ 0$), nor transitive ($1\ R\ 0$, $0\ R\ 3$ and $1 \not R\ 3$).

(b) This relation is symmetric, but not reflexive and not transitive.

(c) This relation is transitive, but not reflexive and not symmetric.

(d) This relation is transitive and symmetric, but not reflexive.

(e) This relation is transitive and symmetric, but not reflexive.

EO-2.2 It is not reflexive ($1 \not R\ 1$) and not transitive ($1\ R\ 0$ and $0\ R\ 1$). It is symmetric since $x^2 + y^2 = n^2$ implies that $y^2 + x^2 = n^2$.

EO-2.3 It is reflexive by definition. It is symmetric since $x - y$ is an odd integer if and only if $y - x$ is an odd integer. (One difference is the negative of the other.) It is never satisfies the transitive condition for distinct x, y, z: If $x\ R\ y$ and $y\ R\ z$, then $x - y$ and $y - z$ are both odd integers and so $x - z$ is an **even** integer.

EO-2.4 It is reflexive, symmetric and transitive. One way to prove that it is an equivalence relation is to note that the equivalence classes are the blocks of the coimage partition of the function $f(x) = x^2$.

EO-2.5 It is symmetric since $\gcd(x, y) = \gcd(y, x)$. It fails to be reflexive because $\gcd(1, 1) = 1$. It is not transitive; for example $2\ R\ 10$ and $10\ R\ 5$ but $2 \not R\ 5$.

EO-2.6 It is reflexive and symmetric. (Why?) It is not transitive; for example, consider $\{1\}$, $\{1, 2\}$ and $\{2\}$.

EO-2.7 You should be able to explain why it is reflexive and symmetric. For transitive, consider $\{1\}$, $\{1, 2\}$ and $\{2\}$.

EO-2.8 To specify a relation R, we must make one of two choices (in R or not in R) for each pair (x, y). There are n^2 pairs. Thus there are 2^{n^2} relations —- that's $2^{(n^2)}$, not $(2^n)^2$. (This was done in Example 14.)

A relation R is reflexive if and only if $x\ R\ x$ for all n values of x. Thus we are free to choose for only $n^2 - n$ of the pairs (x, y), namely those with $x \neq y$. Thus there are 2^{n^2-n} reflexive relations. (This was done in Example 14.)

Subtracting the reflexive relations from all relations, we find that $2^{n^2} - 2^{n^2-n}$ relations are not reflexive.

EO-2.9 For a symmetric relation, we can choose freely whether or not $(x, x) \in R$ for all n values of x; however, once we have made a choice for (x, y), we must make the same choice for (y, x). Thus we are free to choose for only half of those (x, y) with $x \neq y$. The number of such pairs is (x, y) is $n^2 - n$. Thus we are free to choose for $n + (n^2 - n)/2$ pairs. This number equals $(n^2 + n)/2 = n(n + 1)/2$. Hence there are $2^{n(n+1)/2}$ symmetric relations. Thus there are $2^{n^2} - 2^{n(n+1)/2}$ which are not symmetric.

EO-2.10 This is exactly the same as the previous exercise with one exception: We must have $(x, x) \in R$ for all R. You should be able to see that the answer is $2^{n(n-1)/2}$.

EO-2.11 The reasoning is exactly the same as in the two previous exercises. Also, half of this problem was done in Example 14.

EO-2.12 Computing the transitive closure "by inspection" of R can be tricky. It's much better to use either the incidence matrix or the directed graph diagram approach. We do the former. With rows and columns in the order 0, 1, 2, 3, the incidence matrix is

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Using Boolean sum and product, we have

$$A^2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad S_2 = A^2 + A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Next, we compute

$$S_3 = S_2\,A + A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \qquad S_4 = S_3\,A + A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Since $S_4 = S_3$, we are done.

EO-2.13 We leave experimentation to you. The results of the matrix calculations are

$$S_1 = A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad S_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad S_3 = S_2.$$

EO-2.14 The covering relation is

$$\bigl\{(4,8),\ (4,12),\ (4,20),\ (6,12),\ (6,18),\ (8,16),\ (9,18),\ (10,20)\bigr\}.$$

The minimal elements are 4, 6, 9, 10, 14 and 15. The maximal elements are 12, 16, 18, 20, 14 and 15. A chain of longest length is $4 \mid 8 \mid 16$. It has length two and is unique.

EO-2.15 The covering relation has cardinality 15 (draw the Hasse diagram). It consists of all pairs $(T, T \cup \{x\})$ where $T \cup \{x\}$ is an allowed subset of S and $x \notin T$. There are 6 chains of length three. The maximal elements are $\{1,3,5\}$, $\{1,4\}$, $\{2,4\}$ and $\{2,5\}$. The minimal element is $\emptyset$. Since there is more than one maximal element, there is no greatest element. Since there is only one minimal element, it is the least element.

EO-2.16 It can be shown that *every* finite poset has at least one maximal element, so your example must be infinite. One example is the integers with the usual order relation. Another example is the rationals (with the usual order relation). Yet another example is the rationals less than 1. Why are the rationals less than or equal to 1 not an example?

EO-2.17 The covering relation is

$$\big\{((0,0),\,(0,1)),\ ((0,0),\,(1,0)),\ ((0,1),\,(1,1)),\ ((1,0),\,(1,1))\big\}.$$

You can see this by drawing the Hasse diagram in the plane $\mathbb{R}^2$, using the elements of S_2 as coordinates. The picture is a square. The covering relation for the subsets of a two-element set under inclusion is essentially the same as this example. The correspondence is given by the isomorphism discussed in Example 17, obtained by using the characteristic function. As noted at the end of the example, the characteristic function provides an isomorphism for n-element sets. You could imagine drawing the Hasse diagram in n dimensions, obtaining an n-dimensional cube. Of course, we can't visualize this for $n > 3$.

EO-2.18 (a) In reverse order since $9 \mid 18$.

(b) In order.

(c) Incomparable since 16 and 6 are incomparable.

EO-2.19 (a) Let S consist of x and the $n-1$ elements $s_2 \prec_C s_3 \prec_C \cdots \prec_C s_n$. There are three possible types of covering relations, depending on which of the s_i equals y.

- If $s_2 = y$, we have the additional relation $x \prec_C s_3$.
- If $s_n = y$, we have the additional relation $s_n \prec_C x$.
- If $s_k = y$ for $2 < k < n$, we have the additional relations $s_{k-1} \prec_C x \prec_C s_{k+1}$.

The Hasse diagram looks like the diagram for a chain except that one element of the chain has been split into two, namely x and y. You should draw the pictures.

(b) Consider two elements (a_1, a_2) and (b_1, b_2) of T. How can they be incomparable?

- We could have a_1 and b_1 incomparable. Thus one of a_1 and b_1 is x and the other is y. Since our pairs are not ordered, we can assume $a_1 = x$ and $b_1 = y$. The values of a_2 and b_2 can be anything. This gives us $n \times n = n^2$ pairs.
- If $a_1 = b_1$, then a_2 and b_2 must be incomparable and so must be x and y in some order. There are n choices for $a_1 = b_1$ and so this gives n pairs.
- If $a_1 \neq b_1$ and they are comparable, then (a_1, a_2) and (b_1, b_2) are also comparable, so this gives us nothing.

Adding up we obtain $n^2 + n$.

EO-2.20 There are 13 configurations. In lex order they are as follows: hhhhhh, hhvvhh, hvhvhh, hvvhhh, hvvvvh, vhhvhh, vhvhhh, vhvvvh, vvhhhh, vvhvvh, vvvhvh, vvvvhh, vvvvvv. You should draw pictures of some of them.

EO-2.21 As in the statement of the problem, we've omitted the commas and parentheses in the lists.

PASS 1
Bucket 1: 321, 441, 221, 311, 111
Bucket 2: 312, 422
Bucket 3: 143
Bucket 4: 214, 234

PASS 2
Bucket 1: 311, 111, 312, 214
Bucket 2: 321, 221, 422
Bucket 3: 234
Bucket 4: 441, 143

PASS 3
Bucket 1: 111, 143
Bucket 2: 214, 221, 234
Bucket 3: 311, 312, 321
Bucket 4: 422, 441

EO-2.22 The topological sort 15, 14, 10, 9, 6, 18, 4, 20, 12, 8, 16 has 26 in-order pairs.

EO-2.23 This poset has a least element, the empty set, and a greatest element, S. Thus every topological sort must start with $\emptyset$ and end with S. The three subsets $\{a\}$, $\{b\}$ and $\{c\}$ can be arranged in any order; that is in any of six ways. What about the three sets $\{a,b\}$, $\{a,c\}$ and $\{b,c\}$?

- They could be arranged in any manner after the three 1-element sets. Combining those six arrangements with the six 1-element set arrangements gives $6 \times 6 = 36$ topological sorts.

- If the one element sets are in the order $\{x\}$, $\{y\}$, $\{z\}$, then the set $\{x,y\}$ can be placed before $\{z\}$ and the other two 2-element sets can be placed after $\{z\}$ in either of two orders. This gives $6 \times 2 = 12$ topological sorts.

Adding the results gives us 48 topological sorts.

Solutions for Induction, Sequences and Series

IS-1.1 There is no single "right" answer. We illustrate this for (a) by giving some possible variations on the answer. In the other cases, we give just one answer.

(a) $\displaystyle\sum_{n=1}^{\infty}(-1)^{n-1}n^2 \quad \text{or} \quad -\sum_{k=1}^{\infty}(-1)^k k^2 \quad \text{or} \quad \sum_{n=0}^{\infty}(-1)^n(n+1)^2$

(b) $\displaystyle\sum_{k=1}^{\infty}(k^3+(-1)^k)$

(c) $\displaystyle\prod_{k=2}^{\infty}(k^2-(-1)^k)$

(d) $\displaystyle\prod_{n=0}^{\infty}(1-r^{2n+1})$

(e) $\displaystyle\sum_{n=2}^{\infty}\frac{n-1}{n!}$

(f) $\displaystyle\sum_{k=0}^{\infty}\frac{n-k}{(k+1)!}$

IS-1.2 (a) For $n \geq 1$, $\frac{}{n} - \frac{1}{n+1}$ — which equals $\frac{1}{n(n+1)}$.

(b) For $n \geq 1$, $\frac{n}{(n+1)^2}$ or, for $n \geq 2$, $\frac{n-1}{n^2}$.

(c) For $n \geq 1$, $\frac{(-1)^{n+1}n}{n+1}$ or, for $n \geq 2$, $\frac{(-1)^n(n-1)}{n}$.

(d) For $n \geq 1$, $n(n+1)$.

(e) For $n \geq 1$, $\lfloor (n-1)/2 \rfloor$ or, for $n \geq 0$, $\lfloor n/2 \rfloor$.

IS-1.3

(a) $\displaystyle\prod_{j=1}^{n}\frac{j^2}{j+1}$

(b) $\displaystyle\sum_{j=0}^{n-2}\frac{j+1}{(n-j-1)^2}$

(c) $\displaystyle\prod_{j=n-1}^{2n-1}\frac{n-j}{j+1}$

(d) $\displaystyle\prod_{j=0}^{n-1}\frac{j+1}{j+2}\prod_{j=0}^{n-1}\frac{j+2}{j+3}$

IS-1.4 Call the claim for n, $\mathcal{A}(n)$.
Base case ($n=1$): $1^2 = 1(1+1)(2+1)/6$ proves it.

Inductive step:

$$\begin{aligned}\sum_{k=1}^{n} k^2 = n^2 + \sum_{k=1}^{n-1} k^2 &= n^2 + \frac{(n-1)n(2(n-1)+1)}{6} && \text{by } \mathcal{A}(n-1)\\ &= \frac{n(6n+(2n^2-3n+1))}{6} = \frac{n(n+1)(2n+1)}{6} && \text{by algebra.}\end{aligned}$$

IS-1.5 By Theorem 2, the sum is a fourth degree polynomial with constant term 0 and lead coefficient 1/4. We could write down three equations for the three other coefficients by setting $n = 1$, $n = 2$ and $n = 3$. It is simpler to just verify that the given polynomial, $\big(n(n+1)/2\big)^2$ is fourth degree with no constant term and lead coefficient 1/4 and that it gives the correct answer for $n = 1$, $n = 2$ and $n = 3$.

For induction, the base case is trivial: $1^3 = (1(1+1)/2)^2$ and the inductive step is $n^3 + ((n-1)n/2)^2 = (n(n+1)/2)^2$, which is easily checked by algebra.

IS-1.6 Call the equation $\mathcal{A}(n)$. The base case ($n = 1$) is simple.
For the inductive step:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{1}{n(n+1)} + \sum_{i=1}^{n-1} \frac{1}{i(i+1)} = \frac{1}{n(n+1)} + \frac{n-1}{n} = \frac{n}{n+1}.$$

IS-1.7 Call the equation $\mathcal{A}(n)$. The base case ($n = 0$) is simple: $1 \times 2^1 = 0 + 2$.
For the inductive step:

$$\begin{aligned}\sum_{i=1}^{n+1} i2^i &= (n+1)2^{n+1} + \sum_{i=1}^{n} i2^i\\ &= (n+1)2^{n+1} + (n-1)2^{n+1} + 2 && \text{by } \mathcal{A}(n-1)\\ &= 2n2^{n+1} + 2 = n2^{n+2} + 2.\end{aligned}$$

IS-1.8 Call the equation $\mathcal{A}(n)$. The base case ($n = 2$) is simple: $1 - 1/2^2 = (2+1)/2^2$.
For the inductive step:

$$\begin{aligned}\prod_{i=2}^{n}\left(1 - \frac{1}{i^2}\right) &= \left(1 - \frac{1}{n^2}\right)\prod_{i=2}^{n-1}\left(1 - \frac{1}{i^2}\right)\\ &= \frac{n^2-1}{n^2}\,\frac{n}{2(n-1)} && \text{by } \mathcal{A}(n-1)\\ &= \frac{n+1}{2n} && \text{by algebra}\end{aligned}$$

IS-1.9 The base case ($n = 1$) is simple. For the inductive step:

$$\sum_{i=1}^{n} i\,i! = n\,n! + \sum_{i=1}^{n-1} i\,i! = n\,n! + n! - 1 = (n+1)! - 1.$$

IS-1.10 The base case ($n = 0$) is simple. For the inductive step:

$$\begin{aligned}\prod_{i=0}^{n} \frac{1}{2i+1}\frac{1}{2i+2} &= \frac{1}{(2n+1)(2n+2)}\prod_{i=0}^{n-1}\frac{1}{2i+1}\frac{1}{2i+2}\\ &= \frac{1}{(2n+1)(2n+2)\,(2n)!} = \frac{1}{(2n+2)!}\end{aligned}$$

IS-1.11 $\sum_{k=1}^{n} 5k = 5\sum_{k=1}^{n} k = 5n(n+1)/2$, by Example 2.

IS-1.12 There are various approaches. Here are some, with details omitted.

- If you know the sum of a geometric: $\sum_{k=0}^{N} Ar^k = \frac{A(r^{N+1}-1)}{r-1}$, you can use it with $A = 1$, $r = a$ and the two values $N = n$ and $N = t-1$. Subtract the two results.
- As in the preceding, but with $A = a^t$, $r = a$ and $N = n - t$.
- Induction with $n = t$ the base case.
- Multiply both sides by $a - 1$ and note that

$$(a-1)\sum_{k=t}^{n} a^k = \sum_{k=t}^{n} a^{k+1} - \sum_{k=t}^{n} a^k = \sum_{j=t+1}^{n+1} a^j - \sum_{k=t}^{n} a^k = a^{n+1} - a^t.$$

IS-1.13 Without induction, one can do arithmetic mod 3. There are two ways to do this:

- $n^3 - 10n + 9 = n^3 - n = (n-1)n(n+1) \bmod 3$. One of the three consecutive integers $n-1$, n and $n+1$ must be a multiple of 3 and so $n^3 - 10n + 9 = 0 \bmod 3$.
- $n \bmod 3$ is either 0, 1 or 2. In all three cases, one can check that $n^3 - 10n + 9 = 0 \bmod 3$.

Without induction, one can write $n^3 - 10n + 9 = (n-1)n(n+1) - 9(n-1)$ and continue; however, this is just a messier version of arithmetic mod 3.

By induction, it's true for $n = 0$. To keep the algebra simple, we prove the case $n + 1$ from the case n. We have

$$(n+1)^3 - 10(n+1) + 9 = n^3 + 3n^2 + 3n + 1 - 10n - 10 + 9 = (n^3 - 10n + 9) + 3(n^2 + n - 3).$$

By the induction assumption, $n^3 - 10n + 9$

IS-1.14 The base case ($n = 1$) is trivial $(x - y) \mid (x^1 - y^1)$.
For the inductive step, we have $(x - y) \mid (x^{n-1} - y^{n-1})$. To get x^n we could multiply by x to conclude that $(x - y) \mid (x^n - xy^{n-1})$. This is not quite right because we want $x^n - y^n$. The difference between what we want and what we have is

$$(x^n - y^n) - (x^n - xy^{n-1}) = (x - y)y^{n-1}.$$

How does this help? If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$. Apply this with $a = x - y$, $b = x^n - xy^{n-1}$ and $c = (x - y)y^{n-1}$ and you are done.

Another way to prove this is by the equation

$$\frac{x^n - y^n}{x - y} = x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-1} + y^n.$$

Again, this can be proved by induction by using $x^n - y^n = x(x^{n-1} - y^{n-1}) - (x-y)y^{n-1}$. You should fill in the proof.

IS-1.15 Modulo 6 we have $n(n^2+5) = n(n^2-1) = (n-1)n(n+1)$, a product of three consecutive integers. One is divisible by 3 and at least one is divisible by 2.
For induction, the base case is trivial. We prove the case $n+1$ using the case n:

$$(n+1)((n+1)^2+5) = (n+1)(n^2+2n+6) = n^3+3n^2+8n+6 = n(n^2+5)+3n(n+1)+6.$$

By induction, $n(n^2+5)$ is divisible by 6. Since $n(n+1)$ is even, $3n(n+1)$ is divisible by 6. Thus we are done.

IS-1.16 The condition $n \neq 3$ looks strange — we haven't had anything like that before. To see what's going on, let's try the inductive step, proving the $n+1$ case. We want $(n+1)^2 \le 2^{n+1}$ and we have $n^2 \le 2^n$. The right sides are double each other, so we could do this if we had something similar for the left sides, namely $(n+1)^2 \le 2n^2$ for then $(n+1)^2 \le 2n^2 \le 2 \times 2^n = 2^{n+1}$. We've reduced the inductive step to proving $(n+1)^2 \le 2n^2$. This is true for $n \ge 3$. There are various ways to see that. Here's one:

$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2,$$

which is nonnegative when $n \ge 3$.

Where are we? We've shown that we can use $n^2 \le 2^n$ to prove $(n+1)^2 \le 2^{n+1}$ provided $n \ge 3$. Thus, we must verify $n = 0$, $n = 1$ and $n = 2$ separately as well as the base case $n = 4$ for the induction. Why $n = 4$ instead of $n = 3$? Because $n = 3$ was excluded in the problem — the inequality is not true when $n = 3$.

IS-1.17 For those who are wondering where this inequality comes from, it was inspired by the Riemann sum approximation to $\int x^{-1/2}\mathrm{d}x$. However, you don't need to know this so we'll omit the details.

The base case ($n = 2$): We want $\sqrt{2} < 1 + 1/\sqrt{2}$, which you can check on a calculator. For the inductive step: We have

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} = \frac{1}{\sqrt{n}} + \sum_{i=1}^{n-1} \frac{1}{\sqrt{i}} > \frac{1}{\sqrt{n}} + \sqrt{n-1},$$

where we used the inequality for $n-1$.

To complete the proof we need to show that

$$\frac{1}{\sqrt{n}} + \sqrt{n-1} \ge \sqrt{n}.$$

The best way to deal with something like this probably to clear of fractions, so we multiply by $\sqrt{n}$ and see that we want to prove

$$1 + \sqrt{n(n-1)} \ge n.$$

If we move the 1 to the other side and square, we get rid of the annoying square root: We want $n(n-1) \geq (n-1)^2$, which is equivalent to $n^2 - n \geq n^2 - 2n + 1$. After some algebra, this is easily seen to be equivalent to $n \geq 1$.

This completes the proof of the inductive step, but it's rather awkward because it's all done backwards. If we reverse the steps, the result is "cleaner," but it looks more like magic. Let's do it.

Since $n > 1$, we have $n + (n^2 - 2n) > 1 + (n^2 - 2n)$. Factoring both sides and taking square roots: $\sqrt{n(n-1)} > n - 1$. Adding 1 to both sides and dividing by $\sqrt{n}$, we have $\sqrt{n-1} + 1/\sqrt{n} > \sqrt{n}$, which is what we needed to prove.

IS-1.18 Let the assertion $\mathcal{A}(n)$ be "$3 \mid f_n$. Clearly $\mathcal{A}(0)$ and $\mathcal{A}(1)$ are true. For $n \geq 2$ we have $f_n = f_{n-2} + f_{n-1}$. By $\mathcal{A}(n-2)$ and $\mathcal{A}(n-1)$, we have $3 \mid f_{n-2}$ and $3 \mid f_{n-1}$. Hence there sum is a multiple of 3 and we are done.

Here's another proof. Let $F_0 = 1$, $F_1 = 2$ and $F_k = F_{k-2} + F_{k-1}$ for $k \geq 2$. Clearly $F_k \in \mathbb{Z}$ for $k \geq 0$. (Strictly speaking, this requires an inductive proof.) By an inductive proof, which we omit, $f_k = 3F_k$.

IS-1.19 We use induction on t. From the recursion $F_2 = 1$ and so the result is true for $t = 0$. For the inductive step:

$$\begin{aligned} F_{3t} &= F_{3t-1} + F_{3t-2} = 1 + 1 = 0 \bmod 2, \\ F_{3t+1} &= F_{3t} + F_{3t-1} = 0 + 1 = 1 \bmod 2, \\ F_{3t+2} &= F_{3t+1} + F_{3t} = 1 + 0 = 1 \bmod 2. \end{aligned}$$

IS-1.20 The base case ($k = 1$) is trivial. For the induction, we need to know the value of $\lfloor k/2 \rfloor$. If k is even, it is $k/2$. If k is odd, it is $(k-1)/2$. Thus, either by $\mathcal{A}(k/2)$ or $\mathcal{A}((k-1)/2)$, we have

$$f_{\lfloor \frac{k}{2} \rfloor} = \begin{cases} k/2, & \text{if } k \text{ is even,} \\ (k-1)/2, & \text{if } k \text{ is odd.} \end{cases}$$

In either case, $2f_{\lfloor \frac{k}{2} \rfloor} \leq k$.

IS-1.21 The general step assumes that there are two nonnegative integers, s and t, less than $k+1$ with $s + t = k + 1$. This does not apply to $k = 0$, the base case. So we must take $k = 1$ as a base case, too, and check if $r^1 = 1$ for all real numbers r. Not so!

IS-1.22 If $p = 1$ and $q = 2$, then $p - 1 = 0$ is not a positive integer.

IS-1.23 To prove these results, we evaluate the functions at n. We've used lots of parentheses to try to make things clearer.

(a) $$(\Delta af)(n) = af(n+1) - af(n) = a\big(f(n+1) - f(n)\big) = a(\Delta f)(n)$$

(b) $$\begin{aligned} (\Delta(f+g))(n) &= (f+g)(n+1) - (f+g)(n) \\ &= f(n+1) + g(n+1) - \big(f(n) + g(n)\big) \\ &= \big(f(n+1) - f(n)\big)\big(g(n+1) - g(n)\big) \\ &= (\Delta f)(n)) + (\Delta g)(n) = (\Delta f + \Delta g)(n) \end{aligned}$$

(c) $$\begin{aligned} (\Delta(fg))(n) &= (fg)(n+1) - (fg)(n) = f(n+1)g(n+1) - f(n)g(n) \\ &= f(n)\big(g(n+1) - g(n)\big) + g(n)\big(f(n+1) - f(n)\big) \\ &\quad + \big(f(n+1) - f(n)\big)\big(g(n+1) - g(n)\big) \\ &= f(n)(\Delta g)(n) + g(n)(\Delta f)(n) + \big((\Delta f)(n)\big)\big((\Delta g)(n)\big) \end{aligned}$$

IS-1.24 We begin with the hint. Using $\binom{n}{i}\frac{n!}{i!\,(n-i)!}$, we have

$$\begin{aligned}\binom{k-1}{j-1}+\binom{k-1}{j} &= \frac{(k-1)!}{(j-1)!\,(k-j)!}+\frac{(k-1)!}{j!\,(k-j-1)!}\\ &= \frac{(k-1)!\,(j+(k-j))}{j!\,(k-j)!} = \frac{k!}{j!\,(k-j)!} = \binom{k}{j}.\end{aligned}$$

Now for the $(\Delta^k f)(n)$ formula. The base case ($k=1$) is the definition of Δ.
We now do the inductive step. If you have difficulty with all the manipulations of sums, try writing it out explicitly for $k=2$ and $k=3$.

$$\begin{aligned}(\Delta^k f)(n) =&(\Delta^{k-1})(\Delta f)(n) = \sum_{i=0}^{k-1}\binom{k-1}{i}(-1)^{k-1-i}(\Delta f)(n+i)\\ =&\sum_{i=0}^{k-1}\binom{k-1}{i}(-1)^{k-1-i}(f(n+i+1)-f(n+i))\\ =&\sum_{i=0}^{k-1}\binom{k-1}{i}(-1)^{k-1-i}f(n+i+1)+\sum_{i=0}^{k-1}\binom{k-1}{i}(-1)^{k-i}f(n+i)\\ =&\sum_{j=1}^{k}\binom{k-1}{j-1}(-1)^{k-j}f(n+j)+\sum_{j=0}^{k-1}\binom{k-1}{j}(-1)^{k-j}f(n+j)\\ =&\sum_{j=1}^{k-1}\left(\binom{k-1}{j-1}+\binom{k-1}{j}\right)(-1)^{k-j}f(n+j)\\ &+\binom{k-1}{k-1}(-1)^{k-k}f(n+k)+\binom{k-1}{0}(-1)^{k-0}f(n+0)\\ =&\sum_{j=1}^{k-1}\binom{k}{j}(-1)^{k-j}f(n+j)+\binom{k}{k}(-1)^{k-k}f(n+k)+\binom{k}{0}(-1)^{k-0}f(n+0)\\ =&\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}f(n+j).\end{aligned}$$

IS-2.1 *Bounded*: Only (f) is bounded.
Monotonic: Only (d) and (e) are not monotonic. You can check (d) and (e) by computing a few values. Perhaps (c) is a bit tricky; however, if you compute a few values you should note that $a_{n+1}=a_n$ whenever n is even and $a_{n+1}=a_n+2$ whenever n is odd.
Eventually monotonic: Since monotonic implies eventually monotonic, we only need to check (d) and (e). After computing a few terms of (d), you should note that $a_{n+1}<a_n$ when n is even and $a_{n+1}>a_n$ when n is odd. Thus it is not eventually monotonic. This leaves only (e). After some computation, it appears that the terms are eventually increasing. In other words $a_{n+1}-a_n$ is eventually non-negative. Compute the difference:

$$a_{n+1}-a_n = \Big(2^{n+1}-10(n+1)\Big)-\Big(2^n-10n\Big) = (2^{n+1}-2^n)-10 = 2^n-10.$$

This is positive for all $n \geq 4$. Thus (e) is eventually monotonic.

IS-2.2 (a) Converges: $\lim_{n\to\infty} \frac{2n^3+3n+1}{3n^3+2} = \lim_{n\to\infty} \frac{2+3/n+1/n^3}{3+2/n^3} = \frac{2}{3}$

(b) Diverges to $-\infty$: $\lim_{n\to\infty} \frac{-n^3+1}{2n^2+3} = \lim_{n\to\infty} \frac{-n+1/n^2}{2+3/n^2}$

(c) Diverges: $\lim_{n\to\infty} \frac{(-n)^n+1}{n^n+1} = \lim_{n\to\infty} \frac{(-1)^n+1/n^n}{1+1/n^n}$

(d) Converges: $\lim_{n\to\infty} \frac{n^n}{(n/2)^{2n}} = \lim_{n\to\infty} \frac{2^{2n}}{n^n} = \lim_{n\to\infty}(4/n)^n = 0$

IS-2.3 (a) Converges: Recall the formula for changing bases in logarithms, namely $\log_a(x) = \log_a(b)\ \log_b(x)$. Thus $\log_2(n) = \log_3(n)\log_2 3$ so $\frac{\log_2(n)}{\log_3(n)} = \log_2 3$

(b) Converges: Think of $\log_2(n)$ as x. Then we have $\frac{\log_2(x)}{x}$, which converges to zero.

IS-3.1 Both series diverge because the terms do not approach zero. (See Theorem 10.) In fact, the terms in (a) diverge to $+\infty$ and those in (b) converge to 1/2.

IS-3.2 In both cases, we apply Theorem 11.

(a) Let $a_n = (4/5)^n$, which gives a geometric series that converges (Example 11). Let $b_n = n^5/4^n$, which is bounded (Example 10).

(b) Let $a_n = 1/n^2$, which gives a convergent general harmonic series (Example 16). Let $b_n = n^2/(n^2 - 150)$, which is bounded.

IS-3.3 In both cases, we apply Theorem 11.

(a) Let $a_n = 1/n^{3/2}$, which gives a convergent general harmonic series (Example 16). Let $b_n = \left(\frac{n^3}{n^3-n^2-1}\right)^{1/2}$, which is bounded.

(b) The problem here is estimating $(n+1)^{1/2} - (n-1)^{1/2}$. If it were a sum instead of a difference, it would be no problem to estimate, so we use a trick:

$$\begin{aligned}(n+1)^{1/2} - (n-1)^{1/2} &= \frac{\big((n+1)^{1/2} - (n-1)^{1/2}\big)\big((n+1)^{1/2} + (n-1)^{1/2}\big)}{\big((n+1)^{1/2} + (n-1)^{1/2}\big)} \\ &= \frac{(n+1)-(n-1)}{\big((n+1)^{1/2} + (n-1)^{1/2}\big)} \\ &= \frac{2}{\big((n+1)^{1/2} + (n-1)^{1/2}\big)}.\end{aligned}$$

Let $a_n = 1/n^{3/2}$ as in (a). Let $b_n = \frac{2n^{1/2}}{\big((n+1)^{1/2}+(n-1)^{1/2}\big)}$, which is bounded.

IS-3.4 These are both alternating series. Calculating some terms seems to indicate that they are monotonic decreasing to zero. How can we prove this? We need to show that a_n goes to zero and $|a_n|$ is eventually monotonic, so we need to estimate the sums in the parentheses somehow. Showing that a_n goes to zero is not too hard, but the monotonicity is a bit tricky.

In (a) we have a partial sum of the generalized harmonic series, which converges. In (b) we have a partial sum H_n of the harmonic series which behaves like $\ln(n)$ by Example 12. Thus $\lim_{n\to\infty} a_n = 0$ in both cases.

Now we need to show that $|a_n|$ is eventually monotonic. Let p_n be the sum in parentheses and call its n^{th} term b_n. We have

$$\left|\frac{a_{n+1}}{a_n}\right| = \frac{(p_n + b_{n+1})/(n+1)}{p_n/n} = \frac{n}{n+1}\,\frac{p_n + b_{n+1}}{p_n} = \frac{1 + b_{n+1}/p_n}{1+1/n}.$$

In both (a) and (b), $b_{n+1} < 1/n$ and $p_n > 1$ so that $1 + b_{n+1}/p_n < 1 + 1/n$ and we are done.

IS-3.5 (a) The only information we have on a series like this is that the series with terms $a_n = (\sin(n))/n$ converges (Example 14). The idea discussed there applies to the series in (a) because the terms $\frac{1}{|n-99.5|}$ are strictly decreasing for $n \geq 100$.

(b) In this case, the idea used in Examples 13 and 14 can be applied because the sequence $a_n = \frac{-9n^2-5}{n^3+1}$ is monotone and converges to zero.