MATH 271 ASSIGNMENT 1 SOLUTIONS

1. Prove or disprove each of the following statements:

   (a) $\forall m \in \mathbf{Z}^+$, $\exists n \in \mathbf{Z}^+$ so that $m + n^3$ is composite.

   (b) $\forall n \in \mathbf{Z}^+$, $\exists m \in \mathbf{Z}^+$ so that $m + n^3$ is composite.

   (c) $\exists m \in \mathbf{Z}^+$ so that $\forall n \in \mathbf{Z}^+$, $m + n^3$ is composite.

   (d) $\exists n \in \mathbf{Z}^+$ so that $\forall m \in \mathbf{Z}^+$, $m + n^3$ is composite.

   (a) This statement is *true*. Here is a proof.

   Let m be an arbitrary positive integer. Let $n = m$. Then $m+n^3 = m+m^3 = m(1+m^2)$, which is composite for all positive integers m except for $m = 1$. So we need to do $m = 1$ separately, and for instance $n = 2$ will work when $m = 1$, because then $m+n^3 = 1+8 = 9 = 3 \cdot 3$ is composite.

   We could also prove this statement by doing the odd and the even cases separately, using some facts from Example 3.2.3 on page 145. If m is odd then let $n = 3$ for example; then $m + n^3 = m + 27$ is even and certainly bigger than 2, so it is composite. On the other hand, if m is even then pick $n = 2$ for example; then $m + n^3 = m + 8$ is again even and bigger than 2, so it is composite.

   (b) This statement is also *true*, and has a similar (but not identical) proof.

   Let n be an arbitrary positive integer. Let $m = n$. Then $m + n^3 = n + n^3 = n(1 + n^2)$, which is composite for all positive integers n except for $n = 1$. So we need to do $n = 1$ separately, and for instance $m = 3$ will work when $n = 1$, because then $m+n^3 = 3+1 = 4 = 2 \cdot 2$ is composite.

   We could also give a proof like the second proof in part (a).

   (c) This statement is *true*. Here is a proof.

   Choose $m = 8$. Then for any positive integer n, $m+n^3 = 8+n^3 = (n+2)(n^2-2n+4)$, which is composite for all positive integers n, since both $n+2$ and $n^2-2n+4 = (n-1)^2+3$ will be greater than 1.

   Note: We could use $m = 27$ or any other perfect cube greater than 1, with the same proof. But we could not use $m = 1$, since although $m+n^3 = 1+n^3 = (n+1)(n^2-n+1)$ will be composite for any positive integer $n > 1$, $1+n^3 = 2$ is not composite when $n = 1$.

   (d) This statement is *false*. Here is a proof by contradiction.

   Suppose that there does exist some positive integer n so that $m + n^3$ is composite for all positive integers m. So this says that all the numbers $n^3 + 1, n^3 + 2, n^3 + 3, \ldots$ are composite. But we also know that there are infinitely many primes (Theorem 3.7.4 on page 183). So there must be some prime (even infinitely many primes) greater than the number n^3, whatever it is. This is a contradiction. Therefore the statement must be false.

2. (a) Disprove each of the following statements:

   (i) For all $r \in \mathbf{R}$ and $n \in \mathbf{Z}$, $\lfloor rn \rfloor = \lfloor r \rfloor \cdot n$.

   (ii) $\forall a, b, c \in \mathbf{Z}^+$, if $a|b$ then $\lfloor a/c \rfloor | \lfloor b/c \rfloor$.

   (iii) $\forall a, b, c \in \mathbf{Z}^+$, if $a|b$ then $\lfloor c/b \rfloor | \lfloor c/a \rfloor$.

   (iv) There exists an integer $c > 1$ so that $\forall a, b \in \mathbf{Z}^+$, if $a|b$ then $\lfloor a/c \rfloor | \lfloor b/c \rfloor$.

   (b) Here is a "proof" of statement (iii). Find the mistake.

   Let a, b, c be positive integers so that $a|b$. This means that $ak = b$ for some integer k. Therefore $\frac{c}{ak} = \frac{c}{b}$. Thus $c/a = ck/b$. Therefore $\lfloor c/a \rfloor = \lfloor ck/b \rfloor = \lfloor c/b \rfloor \cdot k$. Since k is an integer, this proves that $\lfloor c/b \rfloor | \lfloor c/a \rfloor$.

   (a) (i) Here is a counterexample. Let $r = 1/2$ and $n = 2$. Then $\lfloor rn \rfloor = \lfloor (1/2)2 \rfloor = \lfloor 1 \rfloor = 1$ while $\lfloor r \rfloor \cdot n = \lfloor 1/2 \rfloor \cdot 2 = 0 \cdot 2 = 0$.
   Note: If you use addition instead of multiplication, then you get the equation $\lfloor r + n \rfloor = \lfloor r \rfloor + n$, which is true for all $r \in \mathbf{R}$ and $n \in \mathbf{Z}$ (Theorem 3.5.1 on page 167).

   (ii) Here is a counterexample. Let $a = 1$, $b = 2$, $c = 2$. Then $a|b$ since $1|2$, but $\lfloor a/c \rfloor = \lfloor 1/2 \rfloor = 0$ and $\lfloor b/c \rfloor = \lfloor 2/2 \rfloor = 1$, so $\lfloor a/c \rfloor | \lfloor b/c \rfloor$ says $0|1$ which is false.

   (iii) Here is a counterexample. Let $a = 1$, $b = 2$, $c = 1$. Then $a|b$ since $1|2$, but $\lfloor c/b \rfloor = \lfloor 1/2 \rfloor = 0$ and $\lfloor c/a \rfloor = \lfloor 1/1 \rfloor = 1$, so $\lfloor c/b \rfloor | \lfloor c/a \rfloor$ says $0|1$ which is false.

   (iv) To disprove this statement, we will prove its negation. Its negation is:

   For all integers $c > 1$ $\exists a, b \in \mathbf{Z}^+$ so that $a|b$ and $\lfloor a/c \rfloor \not| \lfloor b/c \rfloor$.

   To prove this, let c be an arbitrary integer greater than 1. We need to find $a, b \in \mathbf{Z}^+$ so that $a|b$ and $\lfloor a/c \rfloor \not| \lfloor b/c \rfloor$.

   Try doing $c = 2$ first to see what is going on. Some experimenting might lead you to choose $a = 5$ and $b = 10$. This works since $a|b$ says $5|10$ which is true, but $\lfloor a/c \rfloor = \lfloor 5/2 \rfloor = 2$ and $\lfloor b/c \rfloor = \lfloor 10/2 \rfloor = 5$, so $\lfloor a/c \rfloor | \lfloor b/c \rfloor$ says $2|5$ which is false.

   Now you can try a similar plan for arbitrary c. Choose $a = 2c + 1$; this means that $\lfloor a/c \rfloor = \lfloor (2c + 1)/c \rfloor = \lfloor 2 + (1/c) \rfloor = 2$ as before. Then you can choose $b = ca = c(2c+1)$; this makes sure that $a|b$. But $\lfloor b/c \rfloor = a = 2c+1$, so $\lfloor a/c \rfloor | \lfloor b/c \rfloor$ says $2|(2c + 1)$ which is false since $2c + 1$ is odd.

   (b) The mistake in this "proof" is in the second-last sentence, where it says $\lfloor ck/b \rfloor = \lfloor c/b \rfloor \cdot k$. This uses (i) of part (a) (with $r = c/b$ and $n = k$), which is a false statement and therefore cannot be used.

3. In this question you may use Theorem 3.6.3 on page 174 and Theorem 3.7.1 on page 181, but otherwise use only the definitions of rational and irrational.

   (a) Let $\mathcal{S}$ be the statement

   For all real numbers r, if r is rational and $r \neq 0$ then $r\sqrt{2}$ is irrational.

   Is $\mathcal{S}$ true? Give a proof or counterexample.

   (b) Write out (in good mathematical English) the *contrapositive* of statement $\mathcal{S}$, and give a proof or disproof.

(c) Write out (in good mathematical English) the *converse* of statement $\mathcal{S}$, and give a proof or disproof.

(d) Write out (in good mathematical English) the *negation* of statement $\mathcal{S}$. Is it true? Explain.

(a) $\mathcal{S}$ is true, and here is a proof. Suppose that r is rational and $r \neq 0$. This means that $r = a/b$ for some nonzero integers a and b. We want to prove that $r\sqrt{2}$ is irrational. We will prove this by contradiction. Suppose that $r\sqrt{2}$ is rational. Then $r\sqrt{2} = c/d$ for some integers c and d, where $d \neq 0$. Since $r = a/b$, this means that

$$\frac{a}{b}\sqrt{2} = \frac{c}{d} \ ,$$

which implies that

$$\sqrt{2} = \frac{bc}{ad} \ .$$

But since bc and ad are integers, and $ad \neq 0$ (since a and d are both nonzero), this says that $\sqrt{2}$ is rational which is a contradiction to Theorem 3.7.1 on page 181. Therefore $r\sqrt{2}$ must be irrational.

Note: This problem is a special case of Exercise 10, page 178 (solution on page A-25).

(b) The contrapositive of $\mathcal{S}$ is

For all real numbers r, if $r\sqrt{2}$ is rational, then r is irrational **or** $r = 0$.

The contrapositive is true because it is equivalent to the original statement $\mathcal{S}$ which is true.

(c) The converse of $\mathcal{S}$ is

For all real numbers r, if $r\sqrt{2}$ is irrational, then r is rational and $r \neq 0$.

The converse is *false*. Here is a counterexample. Let $r = \sqrt{2} + 1$. Then $r\sqrt{2} = (\sqrt{2}+1)\sqrt{2} = 2 + \sqrt{2}$, which is irrational by Theorem 3.6.3 on page 174. But r is also irrational by the same theorem. Thus the converse is false.

Another method of proof would be to let $r\sqrt{2}$ be equal to some number that you know is irrational by Theorem 3.6.3, for instance we could let $r\sqrt{2} = \sqrt{2} + 1$. Then solve for r: we get

$$r = \frac{\sqrt{2}+1}{\sqrt{2}} = 1 + \frac{1}{\sqrt{2}} = 1 + \frac{1}{2}\sqrt{2}.$$

By part (a) (which we already know is true!), $(1/2)\sqrt{2}$ is irrational, so by Theorem 3.6.3, $r = 1 + (1/2)\sqrt{2}$ is irrational too, so the converse is false.

(d) The negation is

There exists a real number r such that r is rational and $r \neq 0$, and $r\sqrt{2}$ is also rational.

The negation is *false*, since the original statement $\mathcal{S}$ is true.

MATH 271 ASSIGNMENT 2 SOLUTIONS

1. (a) Prove **by induction** that, for all integers $n \geq 3$,

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \cdots + \frac{2^n}{n!} \leq 8 - \frac{2^n}{n!} \ . \tag{1}$$

(b) Prove that in fact inequality (1) holds for all integers $n \geq 0$.

(c) Find the smallest real number A so that, for all integers $n \geq 0$,

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \cdots + \frac{2^n}{n!} \leq A - \frac{2^n}{n!} \ .$$

(a) *Basis step.* When $n = 3$ inequality (1) is

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \frac{2^3}{3!} \leq 8 - \frac{2^3}{3!}$$

which is

$$1 + 2 + \frac{4}{2} + \frac{8}{6} \leq 8 - \frac{8}{6} \ , \quad \text{that is} \quad \frac{19}{3} \leq \frac{20}{3} \ ,$$

which is true.

Inductive step. Assume that inequality (1) holds for some integer $n = k$, where $k \geq 3$. We want to prove that inequality (1) holds for $n = k + 1$. So we are assuming that

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \cdots + \frac{2^k}{k!} \leq 8 - \frac{2^k}{k!} \ ,$$

and we want to prove that

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \cdots + \frac{2^{k+1}}{(k+1)!} \leq 8 - \frac{2^{k+1}}{(k+1)!} \ . \tag{2}$$

Well,

$$\begin{aligned}
\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \cdots + \frac{2^{k+1}}{(k+1)!} &= \frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \cdots + \frac{2^k}{k!} + \frac{2^{k+1}}{(k+1)!} \\
&\leq 8 - \frac{2^k}{k!} + \frac{2^{k+1}}{(k+1)!} \quad \text{by our assumption} \\
&= 8 - \frac{2^k(k+1)}{k!(k+1)} + \frac{2^k \cdot 2}{(k+1)!} \\
&= 8 - \frac{2^k}{(k+1)!}((k+1) - 2) \\
&= 8 - \frac{2^k(k-1)}{(k+1)!} \ .
\end{aligned}$$

So in order to prove (2), we would like to prove that

$$8 - \frac{2^k(k-1)}{(k+1)!} \leq 8 - \frac{2^{k+1}}{(k+1)!} \ .$$

This is equivalent successively to

$$-\frac{2^k(k-1)}{(k+1)!} \leq -\frac{2^{k+1}}{(k+1)!} \ , \qquad \text{then to} \quad \frac{2^k(k-1)}{(k+1)!} \geq \frac{2^k \cdot 2}{(k+1)!} \ ,$$

and thus to $k-1 \geq 2$, which is true since $k \geq 3$. This finishes the proof of the inductive step. Thus inequality (1) holds for all integers $n \geq 3$.

(b) When $n = 0$, inequality (1) says

$$\frac{2^0}{0!} \leq 8 - \frac{2^0}{0!}$$

which is $1 \leq 8 - 1$ or $1 \leq 7$, which is true. When $n = 1$, inequality (1) says

$$\frac{2^0}{0!} + \frac{2^1}{1!} \leq 8 - \frac{2^1}{1!}$$

which is $1 + 2 \leq 8 - 2$ or $3 \leq 6$, which is true. When $n = 2$, inequality (1) says

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} \leq 8 - \frac{2^2}{2!}$$

which is $1 + 2 + 2 \leq 8 - 2$ or $5 \leq 6$, which is true. Since in part (a) we proved that inequality (1) holds for all integers $n \geq 3$, we now know it holds for all integers $n \geq 0$. Notice that, since the inductive step needed that $k \geq 3$, to prove inequality (1) for all $n \geq 0$ we need all the cases $n = 0, 1, 2$ and 3 in the basis step.

(c) The inductive step in the proof in part (a) works just the same if the 8 right after the inequality sign is replaced with any number A. So the inequality in part (c) will hold for all integers $n \geq 0$ provided that it holds for $n = 0, 1, 2$ and 3, which is the basis step. When $n = 0$ the inequality in (c) says

$$\frac{2^0}{0!} \leq A - \frac{2^0}{0!}$$

which simplifies to $A \geq 1 + 1 = 2$. When $n = 1$ the inequality in (c) says

$$\frac{2^0}{0!} + \frac{2^1}{1!} \leq A - \frac{2^1}{1!}$$

which simplifies to $A \geq 1 + 2 + 2 = 5$. When $n = 2$ the inequality in (c) says

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} \leq A - \frac{2^2}{2!}$$

which simplifies to $A \geq 1 + 2 + 2 + 2 = 7$. When $n = 3$ the inequality in (c) says

$$\frac{2^0}{0!} + \frac{2^1}{1!} + \frac{2^2}{2!} + \frac{2^3}{3!} \leq A - \frac{2^3}{3!}$$

which simplifies to $A \geq 1 + 2 + 2 + 8/6 + 8/6 = 23/3$. We need **all** of these conditions ($A \geq 2$, $A \geq 5$, $A \geq 7$, $A \geq 23/3$) to hold, so the smallest A that will work is $A = \mathbf{23/3}$.

Note. If you have taken calculus, you might recognize the left side of this inequality as being the first $n+1$ terms of the Maclaurin series for e^x when $x = 2$. So as n gets large, the actual value of the left side gets close to $e^2 \approx 7.389$.

2. The sequence $a_0, a_1, a_2, \ldots$ is defined by: $a_0 = 2$, $a_1 = -6$, and $a_n = 2a_{n-1} + 15a_{n-2}$ for all integers $n \geq 2$.

   (a) Find a_2, a_3 and a_4.

   (b) Use part (a) (and more data if you need it) to guess a simple formula for a_n.

   (c) Use **strong induction** to prove your guess.

   (a) We get

$$a_2 = 2a_1 + 15a_0 = 2(-6) + 15(2) = -12 + 30 = \mathbf{18},$$

$$a_3 = 2a_2 + 15a_1 = 2(18) + 15(-6) = 36 - 90 = \mathbf{-54},$$

$$a_4 = 2a_3 + 15a_2 = 2(-54) + 15(18) = -108 + 270 = \mathbf{162}.$$

   (b) Noticing that $a_2 = 2 \cdot 9$, $a_3 = 2 \cdot (-27)$, and $a_4 = 2 \cdot 81$ (and also $a_0 = 2 \cdot 1$ and $a_1 = 2 \cdot (-3)$), we guess that $a_n = 2 \cdot (-3)^n$ for all integers $n \geq 0$.

   (c) *Basis step.* We already checked that the formula $a_n = 2 \cdot (-3)^n$ works when $n = 0, 1, 2$ and 3. Actually for the basis step we only need to check the cases $n = 0$ and $n = 1$, as the inductive step will show.

   Inductive step. Assume that $a_k = 2 \cdot (-3)^k$ for all nonnegative integers k less than n, where $n \geq 2$ is some integer. We want to prove that $a_n = 2 \cdot (-3)^n$. Well,

$$\begin{aligned} a_n &= 2a_{n-1} + 15a_{n-2} \quad (\text{since } n \geq 2) \\ &= 2 \cdot 2 \cdot (-3)^{n-1} + 15 \cdot 2 \cdot (-3)^{n-2} \quad (\text{by assumption}) \\ &= 2 \cdot (-3)^{n-2}\Big[2(-3) + 15\Big] = 2 \cdot (-3)^{n-2} \cdot 9 = 2 \cdot (-3)^{n-2}(-3)^2 = 2 \cdot (-3)^n. \end{aligned}$$

   This proves the inductive step. Therefore $a_n = 2 \cdot (-3)^n$ is true for all integers $n \geq 0$.

3. You are given the following "while" loop:

   [*Pre-condition*: m is a nonnegative integer, $a = 0$, $b = -1$, $c = 0$.]

   while $(a \neq m)$

   1. $b := 2a + 1$
   2. $c := c + b$

3. $a := a + 1$

end while

[*Post-condition*: $c = m^2$.]

Loop invariant: $I(n)$ is "$a = n$, $b = 2n - 1$, $c = n^2$".

(a) Prove the correctness of this loop with respect to the pre- and post-conditions.

(b) Suppose the "while" loop is as above, with the same pre-condition, but statement 2 in the "while" loop is replaced by: $c := c + b + 1$. Find a post-condition that gives the final value of c, and an appropriate loop invariant, and prove the correctness of this loop.

(a) We first need to check that the loop invariant holds when $n = 0$. $I(0)$ says $a = 0$, $b = -1$ and $c = 0$, and these are all true by the pre-conditions.

So now assume that the loop invariant $I(k)$ holds for some integer $k \geq 0$, $k < m$. We want to prove that $I(k + 1)$ holds, that is, that the loop invariant will still hold after one more pass through the loop. So we are assuming that $a = k$, $b = 2k - 1$ and $c = k^2$, and we now go through the loop.

- Step 1: $b := 2a + 1 = 2k + 1 = 2(k + 1) - 1$,
- Step 2: $c := c + b = k^2 + (2k + 1) = (k + 1)^2$,
- Step 3: $a := a + 1 = k + 1$.

This means that $I(k + 1)$ is true, as required.

Finally the loop stops when $a = m$, and we need to check that at that point the post-condition is satisfied. When $a = m$ it means that the loop invariant $I(m)$ must hold, so from $I(m)$ we know that $c = m^2$ as required.

(b) If we set the variables to their pre-condition values of $a = 0$, $b = -1$ and $c = 0$, and run through the loop, the new values we get are $b = 2(0) + 1 = 1$, $c = 0 + 1 + 1 = 2 = 1 \cdot 2$, and $a = 1$. The next time through the loop we will get: $b = 2(1) + 1 = 3$, $c = 2 + 3 + 1 = 6 = 2 \cdot 3$, and $a = 2$. The next time: $b = 2(2) + 1 = 5$, $c = 6 + 5 + 1 = 12 = 3 \cdot 4$, and $a = 3$. From this (or by running through the loop once or twice more to collect more evidence) we can guess that the loop invariant we want will be

$$I(n) : a = n, b = 2n - 1, c = n(n + 1),$$

and the post-condition value of c ought to be $c = m(m+1)$. This choice of $I(n)$ becomes $a = 0$, $b = -1$ and $c = 0$ when $n = 0$, so the pre-condition is satisfied.

So now we assume that the new loop invariant $I(k)$ holds for some integer $k \geq 0$, $k < m$, and we want to prove that $I(k + 1)$ holds. So we are assuming that $a = k$, $b = 2k - 1$ and $c = k(k + 1)$, and we now go through the loop.

- Step 1: $b := 2a + 1 = 2k + 1 = 2(k + 1) - 1$,
- Step 2: $c := c + b + 1 = k(k + 1) + (2k + 1) + 1 = k^2 + 3k + 2 = (k + 1)(k + 2)$,
- Step 3: $a := a + 1 = k + 1$.

This means that $I(k+1)$ is true, as required.

Finally the loop stops when $a = m$, and we need to check that at that point the post-condition is satisfied. When $a = m$ it means that the loop invariant $I(m)$ must hold, so from $I(m)$ we know that $c = m(m+1)$ as required.

MATH 271 ASSIGNMENT 3 SOLUTIONS

1. In this problem you may use exercise 13 on page 281.

   (a) Prove that for all sets A, B, C, $A - C \subseteq (A - B) \cup (B - C)$.

   (b) Prove or disprove: for all sets A, B, C, $A - C = (A - B) \cup (B - C)$.

   (c) Prove the following statement by induction on n: for all integers $n \geq 2$, and for all sets $A_1, A_2, \ldots, A_n$,

$$A_1 - A_n \subseteq (A_1 - A_2) \cup (A_2 - A_3) \cup \cdots \cup (A_{n-1} - A_n).$$

   (a) Let A, B, C be sets and let x be an arbitrary element of $A - C$. We want to prove that $x \in (A - B) \cup (B - C)$. Since $x \in A - C$, we know that $x \in A$ and $x \notin C$. We do two cases:

   Case (i): Suppose that $x \in B$. Then since $x \notin C$, we get that $x \in B - C$, so $x \in (A - B) \cup (B - C)$ as we want.

   Case (ii): Suppose that $x \notin B$. Then since $x \in A$, we get that $x \in A - B$, so again $x \in (A - B) \cup (B - C)$.

   Therefore $x \in (A - B) \cup (B - C)$ in either case, so $A - C \subseteq (A - B) \cup (B - C)$.

   (b) This statement is **false**. A counterexample is $A = \{1\}$, $B = \emptyset$, $C = \{1\}$. Then $A - C = \emptyset$, while $A - B = \{1\}$ and $B - C = \emptyset$ so that $(A - B) \cup (B - C) = \{1\}$.

   (c) *Basis step.* When $n = 2$ the statement is $A_1 - A_2 \subseteq A_1 - A_2$, which is obviously true.

   Inductive step. Let $k \geq 2$ be an integer, and suppose that for any sets $A_1, A_2, \ldots, A_k$,

$$A_1 - A_k \subseteq (A_1 - A_2) \cup (A_2 - A_3) \cup \cdots \cup (A_{k-1} - A_k).$$

   We want to prove that for any sets $A_1, A_2, \ldots, A_{k+1}$,

$$A_1 - A_{k+1} \subseteq (A_1 - A_2) \cup (A_2 - A_3) \cup \cdots \cup (A_k - A_{k+1}).$$

   Well,

$$\begin{aligned}
&(A_1 - A_2) \cup (A_2 - A_3) \cup \cdots \cup (A_k - A_{k+1}) \\
&\quad = \Big[(A_1 - A_2) \cup (A_2 - A_3) \cup \cdots \cup (A_{k-1} - A_k)\Big] \cup (A_k - A_{k+1}) \\
&\quad \supseteq (A_1 - A_k) \cup (A_k - A_{k+1}) \qquad \text{by assumption and exercise 13 p. 281} \\
&\quad \supseteq A_1 - A_{k+1} \qquad \text{by part (a).}
\end{aligned}$$

   This proves the inductive step. Therefore the statement is true for all integers $n \geq 2$.

2. Suppose A and B are finite sets with $N(A) = m$, $N(B) = n$, and $A \subseteq B$. ($N(X)$ denotes the number of elements in a set X: see page 299.)

   (a) How many subsets C of B satisfy $A \cap C = \emptyset$? Explain.

   (b) How many subsets C of B satisfy $A - C = \emptyset$? Explain.

   (c) How many subsets C of B satisfy $C - A = \emptyset$? Explain.

   (d) How many subsets C of B satisfy $A \times C = \emptyset$? Explain.

   (e) How many subsets C of B satisfy $N(C - A) = 1$? Explain.

   (a) To get $C \subseteq B$ and $A \cap C = \emptyset$, C must be any subset of $B - A$. Since $B - A$ has $n - m$ elements, there are exactly $\mathbf{2^{n-m}}$ such subsets C.

   (b) To get $C \subseteq B$ and $A - C = \emptyset$, C must contain all of A and otherwise could contain any other elements of B. So C is just A union any subset of $B - A$, so once again there are exactly $\mathbf{2^{n-m}}$ such subsets C.

   (c) This time, in order that $C - A = \emptyset$ we would need A to contain all of C, so C must be a subset of A. Since A has m elements there are $\mathbf{2^m}$ such subsets C.

   (d) The only way that $A \times C$ can be empty is if either A or C is empty. So we have two possibilities: if $A \neq \emptyset$ (that is, $m > 0$), then C must be the empty set, so there is only **one** such subset C. On the other hand, if $A = \emptyset$ (that is, $m = 0$), then C can be any subset of B, so there are $\mathbf{2^n}$ such subsets C.

   (e) We want exactly one element in $C - A$, so there should be exactly one element x which is in C but not in A. There are $n - m$ elements of B which are not in A, so there are $n - m$ choices for the element x. We could also include in C any elements which are in A, and there are 2^m choices of a subset of A to include in C. Thus by the product rule, there are $\mathbf{(n - m)2^m}$ such subsets C.

3. For any positive integer n, $[n]$ denotes the set $\{1, 2, 3, \ldots, n\}$. Let's say that a subset S of $[n]$ is an *even* set if the sum of all its elements is even, and an *odd* set if the sum of all its elements is odd. For instance, the set $S = \{2, 5, 6\}$ is an odd set because $2 + 5 + 6 = 13$ is odd.

   (a) For each integer $n \geq 2$, find the number of even 2-element subsets of $[n]$, and the number of odd 2-element subsets of $[n]$. Which are more numerous, or are there the same number of each? (Your answer may depend on n.)

   (b) For each integer $n \geq 3$, find the number of even 3-element subsets of $[n]$, and the number of odd 3-element subsets of $[n]$. Which are more numerous, or are there the same number of each? (Your answer may depend on n.)

   (c) How many 271-element subsets S of [2006] are there so that the **product** of all the elements of S is even? Your answer need not be simplified to a definite number (in fact we wish you wouldn't), but it should be expressed using at most two binomial coefficients.

(a) For a 2-element subset $\{a, b\}$ of $[n]$ to be even, we need $a + b$ to be even, so we need either a and b are both even, or a and b are both odd. The number of even numbers in $[n]$ is $\lfloor n/2 \rfloor$ which is $n/2$ if n is even and $(n-1)/2$ if n is odd. The number of ways of choosing two of these numbers is $\binom{\lfloor n/2 \rfloor}{2}$. Similarly the number of odd numbers in $[n]$ is $\lceil n/2 \rceil$ which is $n/2$ if n is even and $(n+1)/2$ if n is odd, and the number of ways of choosing two of these numbers is $\binom{\lceil n/2 \rceil}{2}$. Therefore by the addition rule the number of even 2-element subsets of $[n]$ is

$$\binom{\lfloor n/2 \rfloor}{2} + \binom{\lceil n/2 \rceil}{2}.$$

For a 2-element subset $\{a, b\}$ of $[n]$ to be odd, we need $a + b$ to be odd, so we can suppose that a is even and b is odd. So there are $\lfloor n/2 \rfloor$ choices for a and $\lceil n/2 \rceil$ choices for b. Therefore by the product rule the number of odd 2-element subsets of $[n]$ is

$$\lfloor n/2 \rfloor \cdot \lceil n/2 \rceil.$$

As for which is bigger, we consider n odd and n even separately.

Case (i). If n is *even*, then the number of even 2-element subsets of $[n]$ is

$$\binom{n/2}{2} + \binom{n/2}{2} = 2\binom{n/2(n/2-1)}{2} = \frac{n}{2}\left(\frac{n}{2} - 1\right) = \frac{n(n-2)}{4},$$

and the number of odd 2-element subsets of $[n]$ is

$$\left(\frac{n}{2}\right)\left(\frac{n}{2}\right) = \frac{n^2}{4},$$

so since $n(n-2) = n^2 - 2n < n^2$ for all $n \geq 2$, there are more **odd** 2-element subsets than even 2-element subsets in this case.

Case (ii). If n is *odd*, then the number of even 2-element subsets of $[n]$ is

$$\begin{aligned}
\binom{(n-1)/2}{2} + \binom{(n+1)/2}{2} &= \frac{1}{2}\left(\frac{n-1}{2}\right)\left(\frac{n-1}{2} - 1\right) + \frac{1}{2}\left(\frac{n+1}{2}\right)\left(\frac{n+1}{2} - 1\right) \\
&= \frac{(n-1)(n-3) + (n+1)(n-1)}{8} \\
&= \frac{(n-1)(2n-2)}{8} = \frac{(n-1)^2}{4},
\end{aligned}$$

and the number of odd 2-element subsets of $[n]$ is

$$\left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right) = \frac{(n-1)(n+1)}{4},$$

so since $(n-1)^2 < (n-1)(n+1)$ for all $n \geq 2$, there are more **odd** 2-element subsets than even 2-element subsets in this case too.

Actually, there is an easier way to prove that the number of odd 2-element subsets of $[n]$ is greater than the number of even 2-element subsets of $[n]$, and you don't have to consider n odd and n even separately to do it. Take any even 2-element subset $\{a, b\}$ of $[n]$, where we can assume $a < b$. Since $a + b$ is even, a and b can not be consecutive integers. So you can add 1 to a, and still get two different integers $a + 1$ and b in $[n]$ which will now add to $a + b + 1$ which is an odd number. Thus we can match up every even 2-element subset $a < b$ of $[n]$ with a different odd 2-element subset $a + 1 < b$ of $[n]$. Moreover some odd 2-element subsets of $[n]$, $\{1, 2\}$ for instance, will never get matched up this way. Therefore there must be more odd 2-element subsets of $[n]$ than even 2-element subsets of $[n]$.

(b) For a 3-element subset $\{a, b, c\}$ of $[n]$ to be even, we need $a + b + c$ to be even, so we need either a, b, c are all even, or one of them (say a) is even and b and c are both odd. Using the counts in part (a), the number of ways of choosing three even numbers is $\binom{\lfloor n/2 \rfloor}{3}$, and the number of ways of choosing one even number and two odd numbers is $\lfloor n/2 \rfloor \binom{\lceil n/2 \rceil}{2}$ by the product rule. Therefore by the addition rule the number of even 3-element subsets of $[n]$ is

$$\binom{\lfloor n/2 \rfloor}{3} + \lfloor n/2 \rfloor \binom{\lceil n/2 \rceil}{2}.$$

Similarly, for a 3-element subset $\{a, b, c\}$ of $[n]$ to be odd, we need $a + b + c$ to be odd, so we need either a, b, c are all odd, or one of them is odd and the other two are even. The number of ways of choosing three odd numbers is $\binom{\lceil n/2 \rceil}{3}$, and the number of ways of choosing one odd number and two even numbers is $\lceil n/2 \rceil \binom{\lfloor n/2 \rfloor}{2}$ by the product rule. Therefore by the addition rule the number of odd 3-element subsets of $[n]$ is

$$\binom{\lceil n/2 \rceil}{3} + \lceil n/2 \rceil \binom{\lfloor n/2 \rfloor}{2}.$$

To find out which is bigger, we again consider n odd and n even separately.

Case (i). If n is *even*, then $\lfloor n/2 \rfloor = \lceil n/2 \rceil = n/2$, so the number of even 3-element subsets of $[n]$ is **the same** as the number of odd 3-element subsets of $[n]$. So both must be equal to

$$\frac{1}{2}\binom{n}{3} = \frac{n(n-1)(n-2)}{12}.$$

Case (ii). If n is *odd*, then the number of odd 3-element subsets of $[n]$ is

$$\begin{aligned}
&\binom{(n+1)/2}{3} + \frac{n+1}{2}\binom{(n-1)/2}{2} \\
&= \frac{1}{6}\left(\frac{n+1}{2}\right)\left(\frac{n+1}{2} - 1\right)\left(\frac{n+1}{2} - 2\right) + \frac{n+1}{2} \cdot \frac{1}{2} \cdot \frac{n-1}{2}\left(\frac{n-1}{2} - 1\right) \\
&= \frac{(n+1)(n-1)(n-3)}{48} + \frac{(n+1)(n-1)(n-3)}{16} \\
&= \frac{(n+1)(n-1)(n-3)}{12},
\end{aligned}$$

and so the number of even 3-element subsets of $[n]$ must be

$$\begin{aligned}\binom{n}{3} - \frac{(n+1)(n-1)(n-3)}{12} &= \frac{n(n-1)(n-2)}{6} - \frac{(n+1)(n-1)(n-3)}{12} \\ &= \frac{n-1}{12}\Big[2n(n-2) - (n+1)(n-3)\Big] \\ &= \frac{n-1}{12}\Big[2n^2 - 4n - (n^2 - 2n - 3)\Big] \\ &= \frac{(n-1)(n^2-2n+3)}{12}\,.\end{aligned}$$

Since $(n+1)(n-3) = n^2 - 2n - 3 < n^2 - 2n + 3$ for all $n \geq 3$, there are more **even** 3-element subsets than odd 3-element subsets this time.

Notes. Can you prove either of these facts (that there are more even 3-element subsets of $[n]$ than odd 3-element subsets if n is odd, and the same number if n is even) by matching up subsets as in part (a)? Also, what if you look at 4-element subsets of $[n]$? Which kind of subset (odd or even) is more numerous? What about 5-element subsets and so forth? If you get anywhere with any of these questions tell your professor or TA.

(c) In order for the product of a bunch of integers to be even, we just need that at least one of the integers is even. So it would be better to count the number of 271-element subsets of [2006] whose product is odd, because that would happen exactly if all 271 integers were odd. Since there are $2006/2 = 1003$ odd integers in [2006], the number of ways of choosing 271 of them is $\binom{1003}{271}$. There are $\binom{2006}{271}$ ways of choosing any 271 integers from [2006], so the number of ways of choosing 271 integers from [2006] so as to include at least one even integer is

$$\binom{2006}{271} - \binom{1003}{271}.$$

So this is the answer to our question.

MATH 271 ASSIGNMENT 4 SOLUTIONS

1. Let $X = \{1, 2, \ldots, n\}$, where $n \geq 2$ is an integer. Define the relation $\mathcal{R}$ on the power set $\mathcal{P}(X)$ by: for all $A, B \in \mathcal{P}(X)$, $A\mathcal{R}B$ if and only if $N(A - B) \leq N(B)$.

   (a) Is $\mathcal{R}$ reflexive? Symmetric? Transitive? Explain.

   (b) Find and simplify the number of subsets $A \in \mathcal{P}(X)$ so that $A\mathcal{R}\{1\}$.

   (c) Find and simplify the number of subsets $B \in \mathcal{P}(X)$ so that $\{1, 2\}\mathcal{R}B$.

   (a) **$\mathcal{R}$ is reflexive**. Let $A \in \mathcal{P}(X)$ be arbitrary. Then $A - A = \emptyset$, so $N(A - A) = 0 \leq N(A)$. Thus $A\mathcal{R}A$.

   $\mathcal{R}$ is not symmetric. For example, let $A = \emptyset$ and $B = \{1\}$. Then $A - B = \emptyset$, so $N(A - B) = 0 \leq 1 = N(B)$, and thus $A\mathcal{R}B$. However $B - A = \{1\}$, so $N(B - A) = 1$ while $N(A) = 0$, so $N(B - A) \not\leq N(A)$ and thus $B \not\mathcal{R} A$ (that is, $(B, A) \notin \mathcal{R}$).

   $\mathcal{R}$ is not transitive in general. For example, if $n \geq 3$, let $A = \{1, 2\}$, $B = \{2\}$ and $C = \{3\}$. Then $A - B = \{1\}$ and $B - C = \{2\}$, so $N(A - B) = 1 \leq 1 = N(B)$ and $N(B - C) = 1 \leq 1 = N(C)$, and thus $A\mathcal{R}B$ and $B\mathcal{R}C$. However $A - C = \{1, 2\}$, so $N(A - C) = 2 \not\leq 1 = N(C)$, and thus $A \not\mathcal{R} C$.

   Notes. (i) If $n = 2$, then the relation $\mathcal{R}$ **is** transitive, because for $n = 2$ we get that

   $$\mathcal{R} = \Big\{(\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{2\}), (\{2\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{1, 2\}),$$
   $$(\{1, 2\}, \{1\}), (\{1, 2\}, \{2\})\Big\},$$

   plus all the pairs (A, A), which is a transitive relation.

   (ii) You could discover a counterexample for transitivity by drawing a Venn diagram for the three sets A, B, C and labelling the number of elements in each region of the diagram. See your professor or TA if you want the details.

   (b) $A\mathcal{R}\{1\}$ means $N(A - \{1\}) \leq N(\{1\})$ which means $N(A - \{1\}) \leq 1$. So A must have at most one element, or it could have two elements provided that one of them is the number 1. The number of 1-element subsets of X is n, and the number of 2-element subsets of X that contain 1 is $n - 1$, since the other element can be any of $2, 3, \ldots, n$. Counting $A = \emptyset$ as well, we get that the number of such subsets A is $n + (n - 1) + 1 = 2n$.

   (c) $\{1, 2\}\mathcal{R}B$ means $N(\{1, 2\} - B) \leq N(B)$, which is obviously true whenever $N(B) \geq 2$. The number of subsets B satisfying $N(B) \geq 2$ is the total number of subsets of X minus the number of subsets of size at most 1, which is $2^n - n - 1$. $N(\{1, 2\} - B) \leq N(B)$ is also true for $B = \{1\}$ and $B = \{2\}$, but not for any other 1-element subset (or for the empty set). So the number of such subsets B is $2^n - n - 1 + 2 = 2^n - n + 1$.

2. Let $\mathcal{F}$ be the set of all functions $f : X \to X$, where $X = \{1, 2, 3, 4\}$. Define the relation R on $\mathcal{F}$ by: for all $f, g \in \mathcal{F}$, fRg if and only if $(f \circ g)(x) = (g \circ f)(x)$ for all $x \in X$.

   (a) Is R reflexive? Symmetric? Transitive? Explain.

   (b) Let $g \in \mathcal{F}$ be defined by $g(x) = x$ for all $x \in X$. Find the **number** of functions $f \in \mathcal{F}$ so that fRg.

   (c) Let $h \in \mathcal{F}$ be defined by $h(x) = 1$ for all $x \in X$. Find the **number** of functions $f \in \mathcal{F}$ so that fRh.

   (d) How many of the functions f from part (c) are one-to-one? Explain.

   (a) R **is reflexive**. Let $f \in \mathcal{F}$ be arbitrary. Then $(f \circ f)(x) = (f \circ f)(x)$ for all $x \in X$, so fRf.

   R **is symmetric**. Let $f, g \in \mathcal{F}$ be such that fRg. This means that $(f \circ g)(x) = (g \circ f)(x)$ for all $x \in X$. Thus (obviously) $(g \circ f)(x) = (f \circ g)(x)$ for all $x \in X$, so gRf.

   R **is not transitive**. Let $f, g, h \in \mathcal{F}$ be defined by: $f(1) = 2$, $f(x) = x$ for $x = 2, 3, 4$; $g(x) = x$ for all $x \in X$; and $h(1) = 3$, $h(x) = x$ for $x = 2, 3, 4$. Then

$$(f \circ g)(x) = f(g(x)) = f(x) \qquad \text{for all } x \in X$$

   and

$$(g \circ f)(x) = g(f(x)) = f(x) \qquad \text{for all } x \in X,$$

   so $(f \circ g)(x) = (g \circ f)(x)$ for all $x \in X$ and thus fRg. Similarly,

$$(g \circ h)(x) = g(h(x)) = h(x) \qquad \text{for all } x \in X$$

   and

$$(h \circ g)(x) = h(g(x)) = h(x) \qquad \text{for all } x \in X,$$

   so $(g \circ h)(x) = (h \circ g)(x)$ for all $x \in X$ and thus gRh. But $(f \circ h)(1) = f(h(1)) = f(3) = 3$ while $(h \circ f)(1) = h(f(1)) = h(2) = 2$, so $(f \circ h)(1) \neq (h \circ f)(1)$ and thus $f \not R\, h$.

   (b) In order that fRg, we need $(f \circ g)(x) = (g \circ f)(x)$ for all $x \in X$. But

$$(f \circ g)(x) = f(g(x)) = f(x) \qquad \text{for all } x \in X$$

   and

$$(g \circ f)(x) = g(f(x)) = f(x) \qquad \text{for all } x \in X,$$

   so $(f \circ g)(x) = (g \circ f)(x)$ for all $x \in X$, and thus fRg, *regardless* of what f is. Thus f can be **any** function from X to X. The number of such functions is $4^4 = 256$, since there are 4 choices for $f(1)$, 4 choices for $f(2)$, 4 choices for $f(3)$, and 4 choices for $f(4)$.

   Note. g is called the *identity function* on the set X (see example 7.1.5 on page 394). The fact that it is related by R to every function follows from Theorem 7.4.1 on page 434. This property made it convenient to use in part (a) in showing that R is not transitive.

(c) This time

$$(f \circ h)(x) = f(h(x)) = f(1) \qquad \text{for all } x \in X$$

and

$$(h \circ f)(x) = h(f(x)) = 1 \qquad \text{for all } x \in X,$$

so $(f \circ h)(x) = (h \circ f)(x)$ for all $x \in X$ (and thus fRh) happens exactly if $f(1) = 1$. The number of functions $f \in \mathcal{F}$ which satisfy $f(1) = 1$ is just the number of ways of choosing the values of $f(2), f(3)$ and $f(4)$, which is $4^3 = 64$.

Note. h is a *constant function* (see page 392).

(d) For a function f in part (c) to be one-to-one, there are three choices for $f(2)$ (any of the numbers 2, 3 or 4), then two choices for $f(3)$, and finally only one choice for $f(4)$, so there are $3 \times 2 \times 1 = 6$ such functions altogether.

3. Let $\mathcal{B}_{\leq 10}$ be the set of all binary strings (0-1 sequences) of length at most 10. Define a relation R on $\mathcal{B}_{\leq 10}$ by: for all $s, t \in \mathcal{B}_{\leq 10}$, sRt if and only if the largest number of consecutive 1's in s is equal to the largest number of consecutive 1's in t. For example, when $s = 11011$ and $t = 001101$ we have sRt because in both s and t the largest number of consecutive 1's is 2.

(a) Prove that R is an equivalence relation.

(b) How many distinct equivalence classes does R have? Explain.

(c) How many elements are there in the equivalence class [000]? Explain.

(d) Find an element in the equivalence class [1110] with the largest possible total number of 1's.

(e) Let k be an integer between 3 and 10. Find (in terms of k) the number of elements in the equivalence class [100] which have length k and have exactly two 1's. Your answer should be a single binomial coefficient. Give a *combinatorial* proof that your answer is correct.

(a) R **is reflexive**. Let $s \in \mathcal{B}_{\leq 10}$ be arbitrary. Then the largest number of consecutive 1's in s is equal to the largest number of consecutive 1's in s, so sRs.

R **is symmetric**. Let s and t be elements of $\mathcal{B}_{\leq 10}$ so that sRt. This means that the largest number of consecutive 1's in s is equal to the largest number of consecutive 1's in t. But then the largest number of consecutive 1's in t is equal to the largest number of consecutive 1's in s, so tRs.

R **is transitive**. Let s, t and u be elements of $\mathcal{B}_{\leq 10}$ so that sRt and tRu. This means that the largest number of consecutive 1's in s is equal to the largest number of consecutive 1's in t, and the largest number of consecutive 1's in t is equal to the largest number of consecutive 1's in u. But then the largest number of consecutive 1's in s is equal to the largest number of consecutive 1's in u, so sRu.

Since R is reflexive, symmetric and transitive, R is an equivalence relation.

(b) There are 11 different possible values for the largest number of consecutive 1's in an element of $\mathcal{B}_{\leq 10}$, namely all the integers from 0 to 10. Thus there are 11 different equivalence classes of R.

(c) The equivalence class [000] contains all elements of $\mathcal{B}_{\leq 10}$ where the largest number of consecutive 1's is zero, that is, all binary strings of length at most 10 consisting only of 0's. There are 11 such strings (including the empty string ϵ), so [000] has 11 elements. They are:

$$[000] = \{\epsilon, 0, 00, 000, \ldots, 0000000000\}.$$

(d) We need a string in $\mathcal{B}_{\leq 10}$ with as many 1's as possible and with three 1's in a row but not four 1's in a row. So of course we make it length 10, and one example is 1110111011. The only other example is 1101110111.

(e) We want all binary strings of length k with exactly two 1's (and therefore $k-2$ 0's), where the two 1's are *not* consecutive. So we could write down a row of $k-2$ 0's, then choose two of the $k-1$ gaps between the 0's (counting the two ends as well) to be where we put the 1's. So there are $\binom{k-1}{2}$ such strings.

Another way to count these strings is to count the *bad* strings of length k, and subtract. There are $\binom{k}{2}$ binary strings of length k with exactly two 1's. The number of these where the two 1's are consecutive is just the number of ways of arranging $k-2$ 0's and *one* symbol 11, which is $k-1$. Thus the number of strings we want is $\binom{k}{2} - (k-1) = \binom{k-1}{2}$ by algebra or by Pascal's formula (page 360).

Note. You might try to find the **total** number of elements in [100] of lengths 1, 2, 3, 4 and so on. Do you notice a pattern? (*Hint*: add 1 from each number.) If you think you see a pattern, show it to your professor or TA.