

1. For each true statement below, give a proof. For each false statement below, write out its negation, then give a proof of the negation.

- (a) $\forall a, b \in \mathbb{Z}^+$, if $a|b$ and $(a+1)|b$ then $(a+2)|b$.
- (b) $\forall a, b \in \mathbb{Z}^+$, if $a|b$ and $a|(b+1)$ then $a|(b+2)$.
- (c) $\exists a \in \mathbb{Z}^+$ such that $\forall b \in \mathbb{Z}^+$, $a|b$ and $(a+1)|b$.
- (d) $\forall a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+$ such that $a|b$ and $(a+1)|b$.
- (e) $\forall a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+$ such that $a < b$, $a|b$ and $(a+1)|(b+1)$.

(a) This statement is **false**. The negation is

$$\exists a, b \in \mathbb{Z}^+ \text{ such that } a|b \text{ and } (a+1)|b \text{ but } (a+2) \nmid b.$$

An example (or a counterexample to the original statement) is $a = 1$ and $b = 2$. Then $a|b$ since $1|2$, and $(a+1)|b$ since $2|2$, but $(a+2) \nmid b$ since $3 \nmid 2$.

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

Let $a, b \in \mathbb{Z}^+$ be arbitrary so that $a|b$ and $a|(b+1)$. This means that $b = ak$ and $b+1 = a\ell$ for some $k, \ell \in \mathbb{Z}$. Thus $ak + 1 = a\ell$, so

$$a(\ell - k) = a\ell - ak = 1.$$

Since $\ell - k$ is an integer, this says that $a|1$ and so a must be equal to 1 (since $a > 0$). But then it is clear that $a|(b+2)$. This is what we wanted to prove.

(c) This statement is **false**. The negation is

$$\forall a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+ \text{ such that } a \nmid b \text{ or } (a+1) \nmid b.$$

Here is a proof of the negation. Let $a \in \mathbb{Z}^+$ be arbitrary. We choose $b = 1$ (regardless of the value of a). Since $a+1 \geq 2$, $(a+1) \nmid b$. Thus the negation is true, and so the original statement is false..

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

Let $a \in \mathbb{Z}^+$ be arbitrary. Choose $b = a(a+1)$, which is a positive integer. Then $a|b$ (since $a+1 \in \mathbb{Z}$) and $(a+1)|b$ (since $a \in \mathbb{Z}$).

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

Let $a \in \mathbb{Z}^+$ be arbitrary. Choose $b = a(a+2)$, which is a positive integer. Then $a|b$ (since $a+2 \in \mathbb{Z}$) and $(a+1)|(b+1)$ (since $b+1 = a^2 + 2a + 1 = (a+1)^2$ and $a+1 \in \mathbb{Z}$).

But the question is: how could we guess that $b = a(a+2)$? One way is:

1) get data and look for a pattern.

- When $a = 1$, we want $1|b$ and $2|(b+1)$, and the smallest integer $b > 1$ that works is $b = 3$.
- When $a = 2$, we want $2|b$ and $3|(b+1)$, and the smallest integer $b > 2$ that works is $b = 8$.

- When $a = 3$, we want $3|b$ and $4|(b + 1)$, and the smallest integer $b > 3$ that works is $b = 15$.

And so on. Eventually (using more data if you need it) you will see that $3 = 2^2 - 1$, $8 = 3^2 - 1$, and $15 = 4^2 - 1$ (or maybe $3 = 1 \cdot 3$, $8 = 2 \cdot 4$, and $15 = 3 \cdot 5$), so it looks like b should be $(a + 1)^2 - 1 = a(a + 2)$. Or you might:

2) do some algebra to find b . We want $a|b$ and $(a + 1)|(b + 1)$, which says we want integers k and ℓ so that $b = ak$ and $b + 1 = (a + 1)\ell$. Thus $ak + 1 = (a + 1)\ell$, and so

$$\ell = \frac{ak + 1}{a + 1} = k - \frac{k - 1}{a + 1}.$$

Since ℓ and k are both integers, $\frac{k-1}{a+1}$ must be an integer too, so let's try $k - 1 = a + 1$ which says $k = a + 2$. This would mean $b = a(a + 2)$.

2. (a) Prove or disprove the following statement: $\forall a \in \mathbb{R}$, if $\lfloor a \rfloor = 2$ then $\lfloor 2a \rfloor = 4$.
- (b) Write out the contrapositive of the statement in part (a). Is it true or false? Explain.
- (c) Write out the converse of the statement in part (a). Is it true or false? Explain.
- (d) Prove or disprove the following statement: $\forall r \in \mathbb{R}^+ \exists n \in \mathbb{Z}^+$ so that $\lfloor rn \rfloor$ is prime.
- (e) Prove or disprove the following statement: $\exists n \in \mathbb{Z}^+$ so that $\forall r \in \mathbb{R}^+$, $\lfloor rn \rfloor$ is prime.

(a) This statement is **false**. A counterexample is $a = 2.5$. Then $\lfloor a \rfloor = 2$ but $\lfloor 2a \rfloor = \lfloor 5 \rfloor = 5 \neq 4$.

(b) The contrapositive is: $\forall a \in \mathbb{R}$, if $\lfloor 2a \rfloor \neq 4$ then $\lfloor a \rfloor \neq 2$. The contrapositive is false because it is logically equivalent to the original statement which is false.

(c) The converse is: $\forall a \in \mathbb{R}$, if $\lfloor 2a \rfloor = 4$ then $\lfloor a \rfloor = 2$. The converse is **true**. Here is a proof.

Let $a \in \mathbb{R}$ be arbitrary so that $\lfloor 2a \rfloor = 4$. This means that $4 \leq 2a < 5$. Therefore, dividing by 2 we get that $2 \leq a < 2.5$. So certainly $2 \leq a < 3$ which means that $\lfloor a \rfloor = 2$ which is what we want to prove.

(d) This statement is **false**. To show this we will prove that the negation is true. The negation is

$$\exists r \in \mathbb{R}^+ \text{ so that } \forall n \in \mathbb{Z}^+, \lfloor rn \rfloor \text{ is not prime.}$$

An example is $r = 4$. Then for any $n \in \mathbb{Z}^+$, $rn = 4n$ is an integer so $\lfloor rn \rfloor = 4n = 2 \cdot 2n$ which is not prime.

Bonus problem. Try to answer part (d) when “prime” is replaced by “composite”. If you think you have an idea, talk to your professor or TA.

(e) This statement is **false**. To show this we will again prove that the negation is true. The negation is

$$\forall n \in \mathbb{Z}^+ \exists r \in \mathbb{R}^+ \text{ so that } \lfloor rn \rfloor \text{ is not prime.}$$

Let $n \in \mathbb{Z}^+$ be arbitrary. We choose $r = 4$ (regardless of what n is). Then $\lfloor rn \rfloor = 4n = 2 \cdot 2n$ which is not prime.

Another solution would be to choose $r = 1/n$. Then $\lfloor rn \rfloor = 1$ which is not prime.

3. Let N be your student ID number.

- (a) **Use the Euclidean Algorithm** to find $\gcd(N, 271)$.
- (b) Use your answer to part (a) to write $\gcd(N, 271)$ in the form $Na + 271b$ where $a, b \in \mathbb{Z}$.
- (c) [In this part you may use results from §3.1 such as Theorem 3.1.1 on page 133 or exercises 25, 26, 27, 39, 40 or 42 from page 140. If you use any of these results, be sure to say which ones.]
Let's consider all the Math 271 students' answers to part (b). Prove that no student could have correctly given integers a and b which are both even.

- (a) Let's do it for the hypothetical student number $N = 123456$. The Euclidean algorithm gives:

$$\begin{aligned} 123456 &= 455 \cdot 271 + 151 && \text{(so } 151 = 123456 - 455 \cdot 271) \\ 271 &= 1 \cdot 151 + 120 && \text{(so } 120 = 271 - 151) \\ 151 &= 1 \cdot 120 + 31 && \text{(so } 31 = 151 - 120) \\ 120 &= 3 \cdot 31 + 27 && \text{(so } 27 = 120 - 3 \cdot 31) \\ 31 &= 1 \cdot 27 + 4 && \text{(so } 4 = 31 - 27) \\ 27 &= 6 \cdot 4 + 3 && \text{(so } 3 = 27 - 6 \cdot 4) \\ 4 &= 1 \cdot 3 + 1 && \text{(so } 1 = 4 - 3) \\ 3 &= 3 \cdot 1, \end{aligned}$$

so $\gcd(123456, 271) = \mathbf{1}$, the last nonzero remainder.

- (b) Now, starting with the second-last equation above, solving it for the gcd 1, and plugging in the remainders one by one from the earlier equations, we get:

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (27 - 6 \cdot 4) = 7 \cdot 4 - 27 \\ &= 7 \cdot (31 - 27) - 27 = 7 \cdot 31 - 8 \cdot 27 \\ &= 7 \cdot 31 - 8 \cdot (120 - 3 \cdot 31) = 7 \cdot 31 - 8 \cdot 120 + 24 \cdot 31 = 31 \cdot 31 - 8 \cdot 120 \\ &= 31 \cdot (151 - 120) - 8 \cdot 120 = 31 \cdot 151 - 39 \cdot 120 \\ &= 31 \cdot 151 - 39 \cdot (271 - 151) = 70 \cdot 151 - 39 \cdot 271 \\ &= 70 \cdot (123456 - 455 \cdot 271) - 39 \cdot 271 = 70 \cdot 123456 - 31850 \cdot 271 - 39 \cdot 271 \\ &= 70 \cdot 123456 - 31889 \cdot 271. \end{aligned}$$

So $a = 70$ and $b = -31889$ in this case.

- (c) We'll prove this by contradiction. Suppose that some student (with student ID N) found a correct answer where both a and b were even. Suppose that $\gcd(N, 271) = d$. So the student would have obtained the equation $Na + 271b = d$, so d must be even since both a and b are even. (This uses Theorem 3.1.1 on page 133 and exercise 42 (twice) on page 140.) But since 271 is odd and $d|271$ this means that d must be odd. (In fact, 271 is prime which means that d can only be 1 or 271, but we don't need to know that.) This is a contradiction, so a and b cannot both be even.

MATH 271 ASSIGNMENT 2 SOLUTIONS

1. For an integer $n \geq 1$, let $S(n)$ be the statement

$$2 + \frac{1}{24} - \frac{2}{n+1} \leq \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2n-1}{n^3} \leq 3 - \frac{2}{n}.$$

(a) Prove **by induction** (or by well-ordering) that $S(n)$ is true for all integers $n \geq 2$.

(b) Let N be your student ID number. Use (a) to find

$$\left\lfloor \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2N-1}{N^3} \right\rfloor.$$

(a) *Basis step.* When $n = 2$ $S(2)$ is

$$2 + \frac{1}{24} - \frac{2}{3} \leq \frac{1}{1^3} + \frac{3}{2^3} \leq 3 - \frac{2}{2}$$

which is

$$\frac{11}{8} \leq 1 + \frac{3}{8} \leq 2,$$

which is true.

Inductive step. Assume that $S(k)$ holds for some integer $k \geq 2$. We want to prove that $S(k+1)$ holds. So we are assuming that

$$2 + \frac{1}{24} - \frac{2}{k+1} \leq \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2k-1}{k^3} \leq 3 - \frac{2}{k}, \quad (1)$$

and we want to prove that

$$2 + \frac{1}{24} - \frac{2}{k+2} \leq \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2(k+1)-1}{(k+1)^3} \leq 3 - \frac{2}{k+1}. \quad (2)$$

From (1) we get

$$2 + \frac{1}{24} - \frac{2}{k+1} + \frac{2k+1}{(k+1)^3} \leq \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2k-1}{k^3} + \frac{2k+1}{(k+1)^3} \leq 3 - \frac{2}{k} + \frac{2k+1}{(k+1)^3}.$$

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

$$2 + \frac{1}{24} - \frac{2}{k+2} \leq 2 + \frac{1}{24} - \frac{2}{k+1} + \frac{2k+1}{(k+1)^3} \quad (3)$$

and

$$3 - \frac{2}{k} + \frac{2k+1}{(k+1)^3} \leq 3 - \frac{2}{k+1}. \quad (4)$$

Well,

$$\begin{aligned}
 (3) \quad &\iff \frac{2}{k+1} - \frac{2}{k+2} \leq \frac{2k+1}{(k+1)^3} \\
 &\iff \frac{2}{(k+1)(k+2)} \leq \frac{2k+1}{(k+1)^3} \\
 &\iff 2(k+1)^2 \leq (k+2)(2k+1) \\
 &\iff 2k^2 + 4k + 2 \leq 2k^2 + 5k + 2,
 \end{aligned}$$

which is true for all integers $k \geq 2$. Thus (3) is true. Also,

$$\begin{aligned}
 (4) \quad &\iff \frac{2k+1}{(k+1)^3} \leq \frac{2}{k} - \frac{2}{k+1} \\
 &\iff \frac{2k+1}{(k+1)^3} \leq \frac{2}{k(k+1)} \\
 &\iff (2k+1)k \leq 2(k+1)^2 \\
 &\iff 2k^2 + k \leq 2k^2 + 4k + 2,
 \end{aligned}$$

which is also true for all integers $k \geq 2$. Thus (4) is true too. This finishes the proof of the inductive step. Thus $S(n)$ holds for all integers $n \geq 2$.

(b) Since your student ID number N is greater than 47, $\frac{1}{24} > \frac{2}{N+1}$. Thus from (a),

$$2 < 2 + \frac{1}{24} - \frac{2}{N+1} \leq \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2N-1}{N^3} \leq 3 - \frac{2}{N} < 3.$$

Therefore

$$\left\lfloor \frac{1}{1^3} + \frac{3}{2^3} + \frac{5}{3^3} + \cdots + \frac{2N-1}{N^3} \right\rfloor = 2.$$

2. The sequence b_0, b_1, b_2, \dots is defined by: $b_0 = 1$, $b_1 = 1$, $b_2 = 6$, and $b_n = 3b_{n-2} + 2b_{n-3}$ for all integers $n \geq 3$.

(a) Find b_3, b_4 and b_5 .

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

[*Hint*: how far away is b_4 from the *nearest* power of 2? How about b_5 ?]

(c) Use **strong induction** (or well-ordering) to prove your guess.

(a) We get

$$\begin{aligned}
 b_3 &= 3b_1 + 2b_0 = 3 \cdot 1 + 2 \cdot 1 = 5, \\
 b_4 &= 3b_2 + 2b_1 = 3 \cdot 6 + 2 \cdot 1 = 20, \\
 b_5 &= 3b_3 + 2b_2 = 3 \cdot 5 + 2 \cdot 6 = 27.
 \end{aligned}$$

- (b) The nearest power of 2 to $b_4 = 20$ is $2^4 = 16$, which is 4 less than b_4 . The nearest power of 2 to $b_5 = 27$ is $2^5 = 32$, which is 5 more than b_5 . We could also find that $b_6 = 3b_4 + 2b_3 = 3 \cdot 20 + 2 \cdot 5 = 70$, which is 6 more than the nearest power of 2 which is $2^6 = 64$. So we guess that

$$b_n = \begin{cases} 2^n + n & \text{if } n \text{ is even,} \\ 2^n - n & \text{if } n \text{ is odd,} \end{cases}$$

which could also be written as: $b_n = 2^n + (-1)^n n$ for all integers $n \geq 0$.

- (c) *Basis Step.* We must prove that our guessed formula for b_n is true when $n = 0, 1$ and 2 . Note that $2^0 + (-1)^0 0 = 1 + 0 = 1 = b_0$, $2^1 + (-1)^1 1 = 2 - 1 = 1 = b_1$, and $2^2 + (-1)^2 2 = 4 + 2 = 6 = b_2$, so this all checks.

Inductive Step. Assume that the guessed formula is correct for all integers n between 0 and k inclusive, where $k \geq 2$ is some integer. We want to prove that the formula is correct for $n = k + 1$, that is we want to prove that $b_{k+1} = 2^{k+1} + (-1)^{k+1}(k + 1)$. Well,

$$\begin{aligned} b_{k+1} &= 3b_{k-1} + 2b_{k-2} && \text{by the recurrence} \\ &= 3[2^{k-1} + (-1)^{k-1}(k-1)] + 2[2^{k-2} + (-1)^{k-2}(k-2)] && \text{by assumption} \\ &= 3 \cdot 2^{k-1} + 3(-1)^{k-1}(-1)^2(k-1) + 2^{k-1} + 2(-1)^{k-2}(-1)^4(k-2) \\ &= 4 \cdot 2^{k-1} + (-1)^{k+1}[3(k-1) - 2(k-2)] \\ &= 2^{k+1} + (-1)^{k+1}(3k - 3 - 2k + 4) = 2^{k+1} + (-1)^{k+1}(k + 1), \end{aligned}$$

so the formula is correct for $n = k + 1$. Therefore the formula is correct for all integers $n \geq 0$.

3. You are given the following “while” loop:

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

while ($a \neq m$)

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

end while

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

Loop invariant: $I(n)$ is

$$a = n, \quad b = \begin{cases} n & \text{if } n \text{ is even} \\ n - 1 & \text{if } n \text{ is odd} \end{cases}, \quad c = \begin{cases} 2n & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}.$$

- (a) Prove the correctness of this loop with respect to the pre- and post-conditions.
- (b) Suppose the “while” loop is as above, but $c = 1$ in the pre-condition, and statement 2 in the “while” loop is replaced by: $c := 2b - a$. 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 $n = 0$. Since 0 is even, $I(0)$ says $a = 0$, $b = 0$ and $c = 2 \cdot 0 = 0$, and these are all true by the pre-conditions.

So now assume that the loop invariant $I(k)$ holds for some integer $k \geq 0$ where $k < m$. 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

$$a = k, b = k, c = 2k \quad \text{if } k \text{ is even,} \quad a = k, b = k - 1, c = 0 \quad \text{if } k \text{ is odd,}$$

and we now go through the loop.

- Step 1: $b := 2a - b = \begin{cases} 2k - k = k & \text{if } k \text{ is even} \\ 2k - (k - 1) = k + 1 & \text{if } k \text{ is odd} \end{cases}$
 $= \begin{cases} (k + 1) - 1 & \text{if } k + 1 \text{ is odd} \\ k + 1 & \text{if } k + 1 \text{ is even} \end{cases}$.
- Step 2: $c := 2b - c = \begin{cases} 2k - 2k = 0 & \text{if } k \text{ is even} \\ 2(k + 1) - 0 = 2(k + 1) & \text{if } k \text{ is odd} \end{cases}$
 $= \begin{cases} 0 & \text{if } k + 1 \text{ is odd} \\ 2(k + 1) & \text{if } k + 1 \text{ is even} \end{cases}$.
- 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, since m is even, from $I(m)$ we know that $c = 2m$ as required.

(b) If we set the variables to their pre-condition values of $a = 0$, $b = 0$ and $c = 1$, and run through the loop, the new values we get are $b = 2(0) - 0 = 0$, $c = 2(0) - 0 = 0$, $a = 1$. If we continue to run through the loop, and keep track of the variables in a table, here is what we get:

n	0	1	2	3	4	5
b	0	0	2	2	4	4
c	1	0	3	2	5	4
a	0	1	2	3	4	5

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

$$I(n) : \quad a = n, \quad b = \begin{cases} n & \text{if } n \text{ is even} \\ n - 1 & \text{if } n \text{ is odd} \end{cases}, \quad c = \begin{cases} n + 1 & \text{if } n \text{ is even} \\ n - 1 & \text{if } n \text{ is odd} \end{cases},$$

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

$$a = k, b = k, c = k + 1 \quad \text{if } k \text{ is even,} \quad a = k, b = k - 1, c = k - 1 \quad \text{if } k \text{ is odd,}$$

and we now go through the loop.

- Step 1: $b := 2a - b = \begin{cases} 2k - k = k & \text{if } k \text{ is even} \\ 2k - (k - 1) = k + 1 & \text{if } k \text{ is odd} \end{cases}$
 $= \begin{cases} (k + 1) - 1 & \text{if } k + 1 \text{ is odd} \\ k + 1 & \text{if } k + 1 \text{ is even} \end{cases}$.
- Step 2: $c := 2b - a = \begin{cases} 2k - k = k & \text{if } k \text{ is even} \\ 2(k + 1) - k = k + 2 & \text{if } k \text{ is odd} \end{cases}$
 $= \begin{cases} (k + 1) - 1 & \text{if } k + 1 \text{ is odd} \\ (k + 1) + 1 & \text{if } k + 1 \text{ is even} \end{cases}$.
- 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, since m is even, from $I(m)$ we know that $c = m + 1$ as required.

MATH 271 ASSIGNMENT 3 SOLUTIONS

1. Let n be a positive integer. If A_1, A_2, \dots, A_n are sets, we write

$$\mathcal{S}_n = A_1 - (A_2 - (A_3 - (\dots - (A_{n-1} - A_n) \dots))).$$

For example, if $n = 4$ then $\mathcal{S}_4 = A_1 - (A_2 - (A_3 - A_4))$.

(a) Let A be a set, and let $A_i = A$ for all $1 \leq i \leq n$, so that

$$\mathcal{S}_n = A - (A - (A - (\dots - (A - A) \dots))),$$

where there are n A 's. Prove (using induction or well ordering) that

$$\mathcal{S}_n = \begin{cases} A & \text{if } n \text{ is odd} \\ \emptyset & \text{if } n \text{ is even.} \end{cases}$$

- (b) Prove that for all sets A and B , $A - (B - A) = A$. You may use the identities on page 272.
- (c) Let A and B be sets, and let $A_i = \begin{cases} A & \text{if } i \text{ is odd} \\ B & \text{if } i \text{ is even} \end{cases}$. Find a simple formula (something like in part (a)) for \mathcal{S}_n , and prove it using induction or well ordering.

(a) *Basis Step.* If $n = 1$, then $\mathcal{S}_1 = A$, which agrees with what we want since 1 is odd.

Inductive Step. Assume that the formula for \mathcal{S}_k is correct for some positive integer k . Then

$$\begin{aligned} \mathcal{S}_{k+1} &= A - (A - (A - (\dots - (A - A) \dots))) \quad (\text{with } k+1 \text{ } A\text{'s}) \\ &= A - \mathcal{S}_k \\ &= \begin{cases} A - A & \text{if } k \text{ is odd} \\ A - \emptyset & \text{if } k \text{ is even} \end{cases} \quad \text{by assumption} \\ &= \begin{cases} \emptyset & \text{if } k+1 \text{ is even} \\ A & \text{if } k+1 \text{ is odd} \end{cases} \end{aligned}$$

so the formula for \mathcal{S}_{k+1} is correct.

Therefore, by induction, the formula for \mathcal{S}_n is correct for all positive integers n .

(b) Using the identities on page 272,

$$\begin{aligned} A - (B - A) &= A - (B \cap A^c) = A \cap (B \cap A^c)^c \quad (\#12) \\ &= A \cap (B^c \cup (A^c)^c) \quad (\#9) \\ &= A \cap (B^c \cup A) \quad (\#6) \\ &= (A \cap B^c) \cup (A \cap A) \quad (\#3) \\ &= (A \cap B^c) \cup A \quad (\#7) \\ &= A. \quad (\#1, \#10) \end{aligned}$$

You could also prove this using the element method:

To prove $A - (B - A) \subseteq A$: Let $x \in A - (B - A)$ be arbitrary. This implies $x \in A$, so $A - (B - A) \subseteq A$.

To prove $A \subseteq A - (B - A)$: Let $x \in A$ be arbitrary. Then notice that $x \notin B - A$, because if $x \in B - A$ it implies $x \notin A$ which is a contradiction. Since $x \notin B - A$, we get $x \in A - (B - A)$. Thus $A \subseteq A - (B - A)$.

Therefore $A - (B - A) = A$.

- (c) We get $\mathcal{S}_1 = A$, $\mathcal{S}_2 = A - B$, and $\mathcal{S}_3 = A - (B - A)$ which is equal to A by part (b). So we guess that

$$\mathcal{S}_n = \begin{cases} A & \text{if } n \text{ is odd} \\ A - B & \text{if } n \text{ is even,} \end{cases}$$

and we now prove this by induction.

Basis Step. If $n = 1$, then $\mathcal{S}_1 = A$, which agrees with our guess since 1 is odd.

Inductive Step. Assume that our guessed formula for \mathcal{S}_k is correct for some positive integer k . Then

$$\mathcal{S}_{k+1} = \begin{cases} A - (B - (A - (\dots - (B - A)) \dots)) & \text{if } k + 1 \text{ is odd} \\ A - (B - (A - (\dots - (A - B)) \dots)) & \text{if } k + 1 \text{ is even.} \end{cases}$$

Note that the expression $B - (A - (\dots - (B - A)) \dots)$ (or $B - (A - (\dots - (A - B)) \dots)$) inside the outer parentheses is just \mathcal{S}_k with A and B switched. Thus by assumption this expression must be

$$\begin{cases} B & \text{if } k \text{ is odd} \\ B - A & \text{if } k \text{ is even.} \end{cases}$$

Therefore

$$\mathcal{S}_{k+1} = \begin{cases} A - (B - A) = A & \text{if } k + 1 \text{ is odd (again using part (b))} \\ A - B & \text{if } k + 1 \text{ is even,} \end{cases}$$

so the formula for \mathcal{S}_{k+1} is correct.

Therefore, by induction, the formula for \mathcal{S}_n is correct for all positive integers n .

2. There are 5 men and 5 women, of 10 different heights.

- (a) Find the number of ways of arranging the 10 people in a row so that the i th shortest woman is next to the i th shortest man, for all $1 \leq i \leq 5$.
- (b) Find the number of ways of arranging the 10 people in a row so that the women occupy five consecutive spots.
- (c) Find the number of ways of arranging the 10 people in a row so that everyone except the tallest person is next to someone taller.

- (a) Since the i th shortest man and the i th shortest woman must be next to each other for each i , we can think of each couple as being “tied together” and first arrange the five couples. This can be done in $5!$ ways. For each such arrangement, we can put each couple in two orders (MW or WM), which doubles the number of arrangements for each couple. Thus the total number of arrangements is $5! \cdot 2^5 = 120 \cdot 32 = 3840$.
- (b) The five consecutive spots the women occupy could be in 6 different locations: spots 1 to 5, 2 to 6, 3 to 7, 4 to 8, 5 to 9, or 6 to 10. For each of these choices, there are $5!$ ways to arrange the women in these spots, and for each such way of arranging the women there are also $5!$ ways of arranging the men in the five remaining spots. Thus there are $6 \cdot 5! \cdot 5! = 6(120)^2 = 86400$ such arrangements.
- (c) Suppose the people are A_1 to A_{10} from tallest to shortest. To make such an arrangement, start with A_1 . Then A_2 must stand next to A_1 , so there are two choices for where A_2 goes, either to the left or the right of A_1 . Then A_3 must stand next to either A_1 or A_2 , but not in between them, so A_3 must go at one end of the “line” formed by A_1 and A_2 , so there are two choices for where A_3 goes. Then A_4 must go at one end of the line formed by A_1 , A_2 and A_3 , so there are two choices for A_4 . And so on, considering each person in order from tallest to shortest, each person must go at one end of the line formed by all the taller people. Thus each of the 9 people other than the tallest person has two choices for where to be in line, so there are $2^9 = 512$ arrangements altogether.

Another way to do this problem is by induction. First we would need to get a guess for the correct answer for the general problem where there are n people of different heights. In fact we may as well rephrase the problem to be: find the number of arrangements of the numbers $1, 2, \dots, n$ so that each number except n is next to a larger number. We’ll call these “good” arrangements. For small numbers n you can count the good arrangements: for $n = 2$ there are two (12 and 21), for $n = 3$ there are four (123, 132, 231, 321), and so on. Soon we get the guess that there should be 2^{n-1} good arrangements of the numbers $1, 2, \dots, n$, and we now can prove this by induction. We already know the formula is correct for $n = 2$. So suppose that the formula is correct for some integer $n = k$, where $k \geq 2$. So there are 2^{k-1} good arrangements of the numbers $1, 2, \dots, k$. Notice that for each such arrangement, we can stick the number $k + 1$ in on either side of the number k (wherever it is), and we will get a good arrangement of $1, 2, \dots, k + 1$, because now k is next to a larger number, and any number that used to be next to k either still is or else is now next to the even larger number $k + 1$. This gives us $2 \cdot 2^{k-1} = 2^k$ good arrangements of $1, 2, \dots, k + 1$. Moreover each good arrangement of $1, 2, \dots, k + 1$ will get counted this way, because if you take a good arrangement of $1, 2, \dots, k + 1$ and pull out the $k + 1$ (and close up the gap) you will get a good arrangement of $1, 2, \dots, k$, because we know k had to be next to $k + 1$, so any other number ℓ that used to be next to $k + 1$ will now be next to k , and $\ell < k$, so everything is still okay. Thus there are exactly 2^k good arrangements of $1, 2, \dots, k + 1$, which agrees with the formula when $n = k + 1$. This finishes the Inductive Step, and so we know that there are exactly 2^{n-1} good arrangements of $1, 2, \dots, n$ for each integer $n \geq 1$. In particular, there are 2^9 good arrangements when $n = 10$, which answers the question.

3. Find the number of ordered pairs (A, B) of subsets of $\{1, 2, \dots, 10\}$ satisfying:

- (a) $N(A \cap B) = 7$. ($N(X)$ is the number of elements in the set X ; see page 299.)
- (b) $N(A \times B) = 7$.
- (c) $N(\mathcal{P}(A \cup B)) = 7$. ($\mathcal{P}(X)$ is the power set of the set X .)
- (d) $N(\mathcal{P}(A) \cup \mathcal{P}(B)) = 7$.

- (a) We want $A \cap B$ to have exactly 7 elements from the set $\{1, 2, \dots, 10\}$. There are $\binom{10}{7}$ ways to choose these 7 elements. For each such choice, the other three elements in $\{1, 2, \dots, 10\}$ could be in either A or B (or neither), but cannot be in both (or the size of the intersection would be too large). So each of the 3 other elements has three choices: in A , in B , or in neither. This means there are $3^3 = 27$ ways to distribute the 3 elements not in $A \cap B$, for each of the $\binom{10}{7}$ choices for $A \cap B$, so there are $27\binom{10}{7} = 27\binom{10}{3} = \frac{27 \cdot 10 \cdot 9 \cdot 8}{3 \cdot 2} = 3240$ such choices of ordered pairs (A, B) altogether.
- (b) Since $7 = N(A \times B) = N(A) \times N(B)$ and 7 is prime, we would need either $N(A) = 7$ and $N(B) = 1$, or $N(A) = 1$ and $N(B) = 7$. The number of 7-element subsets of $\{1, 2, \dots, 10\}$ is $\binom{10}{7} = \binom{10}{3} = 120$, and the number of 1-element subsets is $\binom{10}{1}$ which of course is 10. So the number of ways to choose A and B with $N(A) = 7$ and $N(B) = 1$ is $120 \times 10 = 1200$, and the number of ways to choose A and B with $N(A) = 1$ and $N(B) = 7$ is also 1200. So there are 2400 such ordered pairs (A, B) altogether.
- (c) For any set X with n elements, its power set $\mathcal{P}(X)$ has 2^n elements. Since 7 is not a power of 2, $\mathcal{P}(A \cup B)$ cannot be equal to 7, so there are 0 (zero) such ordered pairs (A, B) in this case.
- (d) We want $\mathcal{P}(A) \cup \mathcal{P}(B)$ to have exactly 7 elements, where the number of elements in each of $\mathcal{P}(A)$ and $\mathcal{P}(B)$ separately must be a power of 2. If either A or B had three or more elements, then their power set would already have at least 8 elements, which is too big. On the other hand, if say A had only one element, then its power set would have only two elements, while $\mathcal{P}(B)$ would have at most 4 elements, which totals to at most 6 elements, not enough. So each of A and B must have exactly two elements. Then they both have $2^2 = 4$ subsets, but notice that the empty set is a subset of each, which means that $\mathcal{P}(A) \cup \mathcal{P}(B)$ would have at most $4 + 4 - 1 = 7$ elements. If A and B had any elements in common, the number of subsets in $\mathcal{P}(A) \cup \mathcal{P}(B)$ would be even smaller, so it means that what we want to count is the number of ordered pairs (A, B) of disjoint 2-element subsets of $\{1, 2, \dots, 10\}$. The number of choices for A is $\binom{10}{2} = 45$, and for each choice of A the number of choices for B is $\binom{8}{2} = 28$. So the total number of ordered pairs (A, B) is $45 \cdot 28 = 1260$.

You could also do this count by first counting the number of ways to choose the four elements in $A \cup B$ (which is $\binom{10}{4} = 210$), and multiplying by the number of ways to choose two of these four elements to be A (which is $\binom{4}{2} = 6$), getting $210 \cdot 6 = 1260$ ways to choose A and B .

MATH 271 ASSIGNMENT 4 SOLUTIONS

1. If $F : X \rightarrow X$ is a function, define $f^2(x)$ to be $(f \circ f)(x)$, and inductively define $f^k(x) = (f \circ f^{k-1})(x)$ for each integer $k \geq 3$. (So $f^3(x) = (f \circ f^2)(x) = f(f(f(x)))$ for instance.) We also define $f^1(x)$ to be $f(x)$.

Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by: for all $n \in \mathbb{Z}$, $f(n) = \begin{cases} 2 - 2n & \text{if } n \text{ is odd,} \\ 1 - 2n & \text{if } n \text{ is even.} \end{cases}$

- (a) Find $f^2(n)$, $f^3(n)$, and $f^4(n)$.
 (b) Use part (a) (and more data if you need it) to guess a fairly simple formula for $f^k(n)$ for any positive integer k . (You may need to consider k odd and k even separately.)
 (c) Use induction on k (or well ordering) to prove your guess.
- (a) We get

$$\begin{aligned} f^2(n) &= f(f(n)) = \begin{cases} f(2 - 2n) & \text{if } n \text{ is odd,} \\ f(1 - 2n) & \text{if } n \text{ is even.} \end{cases} \\ &= \begin{cases} 1 - 2(2 - 2n) & \text{if } n \text{ is odd (since } 2 - 2n \text{ is even),} \\ 2 - 2(1 - 2n) & \text{if } n \text{ is even (since } 1 - 2n \text{ is odd).} \end{cases} \\ &= \begin{cases} 4n - 3 & \text{if } n \text{ is odd,} \\ 4n & \text{if } n \text{ is even;} \end{cases} \end{aligned}$$

$$\begin{aligned} f^3(n) &= f(f^2(n)) = \begin{cases} f(4n - 3) & \text{if } n \text{ is odd,} \\ f(4n) & \text{if } n \text{ is even.} \end{cases} \\ &= \begin{cases} 2 - 2(4n - 3) & \text{if } n \text{ is odd (since } 4n - 3 \text{ is odd),} \\ 1 - 2(4n) & \text{if } n \text{ is even (since } 4n \text{ is even).} \end{cases} \\ &= \begin{cases} 8 - 8n & \text{if } n \text{ is odd,} \\ 1 - 8n & \text{if } n \text{ is even;} \end{cases} \end{aligned}$$

$$\begin{aligned} f^4(n) &= f(f^3(n)) = \begin{cases} f(8 - 8n) & \text{if } n \text{ is odd,} \\ f(1 - 8n) & \text{if } n \text{ is even.} \end{cases} \\ &= \begin{cases} 1 - 2(8 - 8n) & \text{if } n \text{ is odd (since } 8 - 8n \text{ is even),} \\ 2 - 2(1 - 8n) & \text{if } n \text{ is even (since } 1 - 8n \text{ is odd).} \end{cases} \\ &= \begin{cases} 16n - 15 & \text{if } n \text{ is odd,} \\ 16n & \text{if } n \text{ is even.} \end{cases} \end{aligned}$$

- (b) From part (a) we might guess that if k is odd, then $f^k(n) = \begin{cases} 2^k - 2^k n & \text{if } n \text{ is odd,} \\ 1 - 2^k n & \text{if } n \text{ is even,} \end{cases}$

and if k is even, then $f^k(n) = \begin{cases} 2^k n - 2^k + 1 & \text{if } n \text{ is odd,} \\ 2^k n & \text{if } n \text{ is even.} \end{cases}$

(c) *Basis step.* Our guessed formulas for $f^k(n)$ are true for $k = 1, 2, 3$ and 4 , by part (a).

Inductive step. Assume that our guessed formula is true for some integer $k = \ell \geq 1$. We want to prove that our formula is true when $k = \ell + 1$. We do this in two cases:

Case (i): ℓ is even. So we assume that $f^\ell(n) = \begin{cases} 2^\ell n - 2^\ell + 1 & \text{if } n \text{ is odd,} \\ 2^\ell n & \text{if } n \text{ is even,} \end{cases}$ and we want to prove that $f^{\ell+1}(n) = \begin{cases} 2^{\ell+1} - 2^{\ell+1}n & \text{if } n \text{ is odd,} \\ 1 - 2^{\ell+1}n & \text{if } n \text{ is even.} \end{cases}$

We get

$$\begin{aligned} f^{\ell+1}(n) &= f(f^\ell(n)) = \begin{cases} f(2^\ell n - 2^\ell + 1) & \text{if } n \text{ is odd,} \\ f(2^\ell n) & \text{if } n \text{ is even.} \end{cases} \\ &= \begin{cases} 2 - 2(2^\ell n - 2^\ell + 1) & \text{if } n \text{ is odd (since } 2^\ell n - 2^\ell + 1 \text{ is odd),} \\ 1 - 2(2^\ell n) & \text{if } n \text{ is even (since } 2^\ell n \text{ is even).} \end{cases} \\ &= \begin{cases} 2^{\ell+1} - 2^{\ell+1}n & \text{if } n \text{ is odd,} \\ 1 - 2^{\ell+1}n & \text{if } n \text{ is even,} \end{cases} \end{aligned}$$

so the inductive step works in this case.

Case (ii): ℓ is odd. This time we assume that $f^\ell(n) = \begin{cases} 2^\ell - 2^\ell n & \text{if } n \text{ is odd,} \\ 1 - 2^\ell n & \text{if } n \text{ is even,} \end{cases}$ and we want to prove that $f^{\ell+1}(n) = \begin{cases} 2^{\ell+1}n - 2^{\ell+1} + 1 & \text{if } n \text{ is odd,} \\ 2^{\ell+1}n & \text{if } n \text{ is even.} \end{cases}$

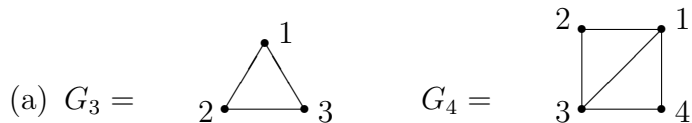
We get

$$\begin{aligned} f^{\ell+1}(n) &= f(f^\ell(n)) = \begin{cases} f(2^\ell - 2^\ell n) & \text{if } n \text{ is odd,} \\ f(1 - 2^\ell n) & \text{if } n \text{ is even.} \end{cases} \\ &= \begin{cases} 1 - 2(2^\ell - 2^\ell n) & \text{if } n \text{ is odd (since } 2^\ell - 2^\ell n \text{ is even),} \\ 2 - 2(1 - 2^\ell n) & \text{if } n \text{ is even (since } 1 - 2^\ell n \text{ is odd).} \end{cases} \\ &= \begin{cases} 2^{\ell+1}n - 2^{\ell+1} + 1 & \text{if } n \text{ is odd,} \\ 2^{\ell+1}n & \text{if } n \text{ is even,} \end{cases} \end{aligned}$$

so the inductive step works in this case too. Therefore the guessed formula is true for all integers $k \geq 1$.

2. For each integer $n \geq 3$, let G_n be the graph with vertex set $V(G_n) = \{1, 2, 3, \dots, n\}$ and where, for all distinct $a, b \in V(G_n)$, ab is an edge if and only if $\gcd(a, b) = 1$.

- (a) Draw G_3 and G_4 .
- (b) Find all integers $n \geq 3$ so that G_n has a Hamiltonian circuit.
- (c) Show that G_n does not have an Euler circuit if $n \bmod 4 \neq 3$ ($n \not\equiv 3 \pmod{4}$). [*Hint:* do even n and odd n separately.]
- (d) Suppose for each integer $n \geq 3$ we define the graph G'_n the same way as for G_n except that $V(G'_n) = \{2, 3, \dots, n\}$. Show (without a computer) that G'_8 does *not* have a Hamiltonian circuit. [*Hint:* start by thinking how 6 could fit into a Hamiltonian circuit.]

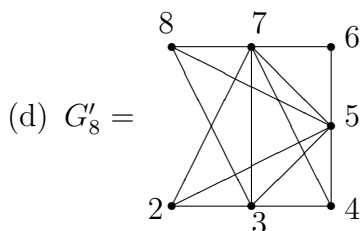


(b) For any integer $n \geq 3$, G_n has the Hamiltonian circuit $(1, 2, 3, \dots, n, 1)$, because $\gcd(k, k+1) = 1$ for any integer k , and also $\gcd(n, 1) = 1$.

(c) Notice that in the graph G_n , vertex 1 is connected to every other vertex, because $\gcd(1, k) = 1$ for every positive integer k . Thus vertex 1 has degree $n - 1$. So if n is even, vertex 1 has odd degree, and therefore G_n does not have an Euler circuit.

Now suppose n is odd. This means that $n \bmod 4 = 1$ or 3 . Suppose that $n \bmod 4 = 1$. This means that $n = 4q + 1$ for some integer q . Look at vertex 2. It is connected to exactly the odd vertices of G_n , because $\gcd(2, k) = 1$ exactly if k is odd. The odd vertices in G_n are $1, 3, 5, \dots, n = 4q + 1$, and there are $2q + 1$ of these. Thus vertex 2 has degree $2q + 1$, which is an odd number. Therefore G_n has no Euler circuit in the case $n \bmod 4 = 1$ either.

Note: Does G_n have an Euler circuit when $n \bmod 4 = 3$? Of course it does when $n = 3$, but it doesn't when $n = 7$. If you figure out whether G_n has an Euler circuit in any other cases ($n = 11, 15, 19, \dots$?) let your professor or TA know.



Suppose that G'_8 had a Hamiltonian circuit. Every vertex of G'_8 must be included in the circuit. Since the degree of vertex 6 is only 2, both of its edges must be in the circuit. So the circuit must contain vertices 5,6,7 in this order. What comes after 7? There are two cases.

Case (i): Suppose 8 comes after 7 in the circuit. Then the circuit contains 5,6,7,8 in this order. The next vertex must then be 3, because 3 is the only vertex adjacent to 8 that is not in the circuit yet. So we have 5,6,7,8,3 in this order, and so the remaining vertices 2 and 4 must go after this and so must be next to each other, which is impossible because they are not adjacent. So no Hamiltonian circuit is possible in this case.

Case (ii): So suppose 8 does not come after 7 in the circuit. This means that 8 must come somewhere else in the circuit, but since we cannot use the edge 78 in the circuit we must use edges 85 and 83, because these are the only other edges containing vertex 8. So the circuit must contain 38567 in this order. But now once again vertices 2 and 4 have to come next, and so must be next to each other, which is impossible. So no Hamiltonian circuit is possible in this case either.

Therefore G'_8 does not have a Hamiltonian circuit.

Note: You can easily show (as in part (b)) that G'_n will have a Hamiltonian circuit whenever n is odd. Does G'_n have a Hamiltonian circuit for any **even** n ? If you get any answers, tell your professor or TA.

3. (a) Find the **total** number of all walks (starting at any vertex, ending at any vertex) of length 271 in the complete graph K_n .
- (b) Find the total number of walks of length 271 in the complete bipartite graph $K_{m,n}$.
- (c) Find the total number of *simple* paths of length $n - 1$ in K_n .
- (d) Find the total number of simple paths of length $m + n - 1$ in $K_{m,n}$. [You may assume that $m \geq n$. You will need to consider a few cases.]
- (a) In K_n we can start at any of the n vertices, then we have $n - 1$ choices for the first step of the walk (to any of the $n - 1$ vertices other than the one we are on), then $n - 1$ choices for the next step, and so on until we have taken 271 steps. So by the multiplication rule there are $n(n - 1)^{271}$ such walks.
- (b) Let the vertices of $K_{m,n}$ be grouped into the two sets M and N , where M has m vertices and N has n vertices. Then all steps must go between M and N . There are two cases.
- Case (i).* If the walk starts at a vertex of M , we have m choices for the starting vertex, then n choices for the first step of the walk (any of the vertices of N), then m choices for the next step of the walk (any of the vertices of M), and so on, alternating between n and m choices until we have taken 271 steps, with the 271st step having n choices. This means that (including the original choice of starting vertex) we will have n choices 136 times and m choices 136 times, so the total number of walks that start at a vertex of M is $n^{136}m^{136} = (nm)^{136}$.
- Case (ii).* If the walk starts at a vertex of N , exactly the same argument will again produce exactly $(nm)^{136}$ walks.
- So the total number of walks is $2(nm)^{136}$.
- (c) A simple path of length $n - 1$ in K_n will have to use each vertex exactly once, and we can use the n vertices in any order we like because all vertices are connected. Thus the total number of such paths is just the number of permutations of the numbers 1 to n , which is $n!$.
- (d) Since $K_{m,n}$ has $m + n$ vertices, any simple path of length $m + n - 1$ will use every vertex exactly once. Again let the vertices of $K_{m,n}$ be grouped into the two sets M and N , where M has m vertices and N has n vertices. Then all steps must go between M and N . Thus the only way to use up every vertex of $K_{m,n}$ with a simple path is if the sizes of M and N are at most one apart. In other words, if $m - n > 1$ then there are **no** such simple paths. We have two cases left.
- Case (i).* Suppose $m = n + 1$. Then all such simple paths must start and end at a vertex of the bigger set M . There are m choices for the starting vertex, then n choices for the first step, then $m - 1$ choices for the next step (any vertex of M except for the starting vertex), then $n - 1$ choices for the next step (any vertex of N except for the second vertex), and so on until we run out of vertices. Thus there are $m \cdot n \cdot (m - 1) \cdot (n - 1) \cdots = m!n! = n!(n + 1)!$ such simple paths in this case.
- Case (ii).* Suppose $m = n$. Then a simple path can start at any vertex. Suppose it starts at a vertex of M (m choices). Then the next step can be any of n choices in N , the next step any of the $m - 1$ remaining vertices in M , the next step any of

the remaining $n - 1$ vertices in N , and so on until we run out of vertices. This gives $m \cdot n \cdot (n - 1) \cdot (n - 2) \cdots = m!n! = (n!)^2$ such paths starting at a vertex of M . But we have the same number of paths starting at a vertex of N . So there are $2(n!)^2$ simple paths altogether in this case.