Problem of the Month

Problem 0: What's my card?

September 2024

Some friends are playing a game involving ten cards numbered 1 through 10. In part (a), Adina, Budi, and Dewei are the players. In parts (b) and (c), Adina, Budi, Charlie, and Dewei are the players. To play the game, each player other than Dewei chooses a card and shows it to all other players, but no player looks at their own card. The game consists of a dialogue with the goal being for all players holding a card to deduce the integer on their own card. In each part of this question, the dialogue is given in the order the statements/questions occurred. **No player is allowed to ask a question to which they already know the answer**.

(a) Given the dialogue below, determine the integers on Adina's and Budi's cards.

1. (Adina) Is the integer on my card larger than the integer on Budi's card?
2. (Dewei) No.
3. (Budi) I know the integer on my card.
4. (Adina) I know the integer on my card.

(b) After the dialogue below, Adina, Budi, and Charlie each know the integer on their own card. Determine all possibilities for the integers on their cards.

1. (Adina) Is the sum of the integers on the cards a perfect square?
2. (Dewei) Yes.

(c) Given the dialogue below, determine all possibilities for the integers on the cards.

1. (Adina) Are the integers on any of the cards prime?
2. (Dewei) No.
3. (Budi) Is the sum of the integers on the cards prime?
4. (Dewei) Yes.
5. The three statements below occur simultaneously.
   - (Adina) I do not know what integer is on my card.
   - (Budi) I do not know what integer is on my card.
   - (Charlie) I know what integer is on my card.
6. The two statements below occur simultaneously
   - (Adina) I still do not know what integer is on my card.
   - (Budi) I now know what integer is on my card.
7. (Adina) I now know what integer is on my card.

Problem of the Month

Problem 0: What's my card?

September 2024

Hint

(a) Would this dialogue be possible if Adina saw a 3 on Budi's card? Make sure you keep in mind that no player will ever ask a question to which they already know the answer!

(b) To narrow the search for the answer, determine all possible sets of three distinct integers between 1 and 10 inclusive that have a sum equal to a perfect square. Going from there, you might want to explore what would happen for some particular configurations of the cards. For instance, if the integers are 1, 2, and 6, would it be possible for all players to determine the integer on their card from the dialogue given?

(c) The general strategy for this problem is similar to that in (b), but you will need to carefully examine how the players would be able to eliminate possibilities based on what the other players are able to infer. Experimenting with various configurations of the cards will likely be helpful.

Problem of the Month

Solution to Problem 0: What's my card?

September 2024

(a) Denote the integer on Adina's card by a and the integer on Budi's card by b.

If $b = 1$ or $b = 10$, then Adina would know the answer to the question in the first line and hence would not have asked it. Therefore, $b \neq 1$ and $b \neq 10$. Budi deduces this information from the fact that Adina asked the question in the first line.

After Dewei answers "No" in the second line, Budi knows the following information: the value of a, that $b \neq 1$, that $b \neq 10$, and that $a < b$. According to the third line of the dialogue, Budi is able to determine the value of b from this information.

Since $a < b$ and $b < 10$, it must be that $a \leq 8$. If $a < 8$, then there is no way for Budi to deduce the value of b from the information in the previous paragraph. Therefore, $a = 8$ and $b = 9$.

Although we have already deduced the integers on the two cards, it is worth pointing out that the final line of the dialogue makes sense. Indeed, the fact that Budi determined the value of b immediately after Adina's question was answered tells Adina that $a = 8$. Otherwise, as discussed in the previous paragraph, there is no way that Budi could have determined the value of b after line 2 in the dialogue.

(b) The smallest possible sum of three different integers from 1 to 10 inclusive is $1+2+3 = 6$ and the largest is $8 + 9 + 10 = 27$. Therefore, 9, 16, and 25 are the only possible perfect squares that can be equal to the sum of the integers on the cards. It is not difficult to deduce that there are exactly 15 sets of three distinct integers from 1 to 10 having a sum equal to a perfect square. One way to approach this is to examine possibilities by considering the largest integer in the set. For instance, if 10 is the largest integer, then we seek distinct positive integers x and y such that $x + y + 10$ is a perfect square. Since $10 > 9$, $x+y+10 > 9$, and so 16 and 25 are the only possibilities for this sum. This means either $x + y = 6$ or $x + y = 15$. In the former case, x and y could be 1 and 5 or 2 and 4 in either order (x and y need to be different, so $x = y = 3$ is not possible). In the latter case, x and y equal to 6 and 9 or 7 and 8. Therefore, four of the sets of three distinct positive integers are $\{1, 5, 10\}$, $\{2, 4, 10\}$, $\{6, 9, 10\}$, and $\{7, 8, 10\}$. Moreover, these four are the only such sets that contain 10. All fifteen sets are listed below.

$$\{1, 2, 6\}, \{1, 3, 5\}, \{1, 5, 10\}, \{1, 6, 9\}, \{1, 7, 8\}, \{2, 3, 4\}, \{2, 4, 10\}, \{2, 5, 9\},$$

$$\{2, 6, 8\}, \{3, 4, 9\}, \{3, 5, 8\}, \{3, 6, 7\}, \{4, 5, 7\}, \{6, 9, 10\}, \{7, 8, 10\}$$

After the dialogue, each player knows that the sum of the integers on the three cards is a perfect square. Each player can see two cards. If a player sees the integers 1 and 6, then the integer on their own card could be 2 or 9, but they will not be able to tell which since in either case the sum would be a perfect square. Since every player is able to deduce the integer on their card once they learn that the sum is a perfect square, it is not possible for

1 and 6 to be two of the integers on the cards. Therefore, the sets $\{1,2,6\}$ and $\{1,6,9\}$ can be eliminated as possibilities for the integers on the three cards.

$$\cancel{\{1,2,6\}}, \{1,3,5\}, \{1,5,10\}, \cancel{\{1,6,9\}}, \{1,7,8\}, \{2,3,4\}, \{2,4,10\}, \{2,5,9\},$$

$$\{2,6,8\}, \{3,4,9\}, \{3,5,8\}, \{3,6,7\}, \{4,5,7\}, \{6,9,10\}, \{7,8,10\}$$

If a player sees the integers 1 and 5, then the integer on their card could be 3 or 10, but they cannot determine which of the two. Therefore, the three cards cannot be $\{1,3,5\}$ or $\{1,5,10\}$.

Continuing with this sort of reasoning, all possibilities except $\{2,5,9\}$, $\{3,6,7\}$, and $\{4,5,7\}$ can be eliminated from the list above.

If the integers are 2, 5, and 9, then one of the players sees the cards 2 and 5. The only way for the sum to be a perfect square is for the integer on their card to be 9 (remember, there is only one of each card, so they cannot be holding a card with a 2 since they see a 2). Therefore, they know the integer on their card. The player who sees 2 and 9 knows their card must have 5 on it since there is no other integer that can be added to $2+9=11$ to get a perfect square. Finally, the player who sees 2 and 5 knows their card must have 9 on it by the same reasoning. Therefore, if the cards have 2, 5, and 9 on them (in any order), then all three players will know the integer on their card as soon as they learn that the sum is a perfect square.

By similar reasoning, if the integers are 3, 6, and 7 in any order, then each player will know the integer on their card once they learn that the sum is a square. Similar reasoning applies if the integers are 4, 5, and 7 in any order.

This gives a total of $3 \times 6 = 18$ configurations of the cards because there are 6 ways to distribute the three cards among the three players for each of the three possible sets of cards. However, it is possible that some of these configurations would lead to Adina knowing the answer to her question immediately from the cards she can see. To finish the argument, we will show that in any of these 18 configurations of the cards, Adina could not possibly know just from the cards that she sees that the sum is or is not a perfect square.

The possible pairs of integers that Adina can see are $\{2,5\}$, $\{2,9\}$, $\{5,9\}$, $\{3,6\}$, $\{3,7\}$, $\{6,7\}$, $\{4,5\}$, $\{4,7\}$, or $\{5,7\}$. These are the two-element subsets of the three possible sets of integers on the cards. In each of these nine cases, there is at least one possibility for the integer on her card that would make the sum a perfect square. As well, in each of these nine cases, if the integer on her card were 1, then the sum would not be a perfect square. Therefore, if Adina sees any of these nine pairs of integers, there is no way for her to know whether the sum is a perfect square. Therefore, all 18 configurations described above are possible.

(c) Since none of the cards have a prime number on them, the possibilities for the integers on the cards are 1, 4, 6, 8, 9, and 10. As well, the sum of the three integers is prime, which rules out many possibilities. By carefully checking, one finds that there are exactly seven sets of three distinct integers from the list 1, 4, 6, 8, 10 that have a prime sum. They are listed below.

$$\{1,4,6\}, \ \{1,4,8\}, \ \{1,6,10\}, \ \{1,8,10\}, \ \{4,6,9\}, \ \{4,9,10\}, \ \{6,8,9\}$$

The first column in the table below contains the fifteen pairs of two distinct integers selected from 1, 4, 6, 8, 9, and 10, which are the possible pairs of cards that a player can see. The right column contains the corresponding number of three-element sets from the list above of which the given two-element set is a subset. For example, the number 2 occurs to the right of $\{1,4\}$ because $\{1,4\}$ is a subset of $\{1,4,6\}$ and $\{1,4,8\}$ and none of the other sets.

$\{1,4\}$	2
$\{4,6\}$	2
$\{6,9\}$	2
$\{1,6\}$	2
$\{4,8\}$	1
$\{6,10\}$	1
$\{1,8\}$	2
$\{4,9\}$	2
$\{8,9\}$	1
$\{1,9\}$	0
$\{4,10\}$	1
$\{8,10\}$	1
$\{1,10\}$	2
$\{6,8\}$	1
$\{9,10\}$	1

If a pair in the table above has a 1 next to it, then a player who sees those two integers will know the integer on their card after the first four lines of dialogue. For instance, if a player sees 4 and 8, they will know that their card is 1 since $\{1,4,8\}$ is the only one of the seven sets above that contains 4 and 8. On the other hand, if there is a 2 next to a set in the table above, then a player who sees those two integers will not be able to determine the integer on their card after the first four lines of dialogue. For instance, if a player sees 1 and 4, then the set of integers is either $\{1,4,6\}$ or $\{1,4,8\}$, so a player who sees 1 and 4 knows that their card is 6 or 8, but cannot determine which.

We know that after the first four lines of dialogue, exactly one player is able to determine the integer on their card. Suppose the set of integers on the cards is $\{4,9,10\}$. The two-element subsets of this set are $\{4,9\}$, $\{4,10\}$, and $\{9,10\}$. Both $\{4,10\}$ and $\{9,10\}$ have a 1 next to them in the table above, so this means that if the set of integers is $\{4,9,10\}$, then two players would know the integer on their card after the first four lines of dialogue. Therefore, the set of integers on the cards is not $\{4,9,10\}$. For similar reasons, the integers cannot be $\{6,8,9\}$.

The two-element subsets of $\{1,4,6\}$ all have a 2 next to them in the table above, which means that if the set of integers is $\{1,4,6\}$, then *none* of the players would know the integer on their card after the first four lines of dialogue. Therefore, the set of integers is not $\{1,4,6\}$, and for the same reason, it is not $\{4,6,9\}$.

The three players will also deduce this information as soon as the statements in line 5 of the dialogue are spoken. Thus, after these statements are made, all three players know that the only possibilities for the set of integers on the cards are those below:

$$\{1,4,8\},\ \{1,6,10\},\ \{1,8,10\}$$

Furthermore, in each of these three cases, the integer on Charlie's card must be 1 since only the player with 1 on their card is able to deduce the integer on their card after the first 5 lines of dialogue. For instance, if the cards are 1, 4, and 8, then the players who have 4 and 8 on their card see the pairs of integers $\{1, 8\}$ and $\{1, 4\}$ respectively. Since these sets each have a 2 next to them in the table above, these players cannot deduce the integer on their card from the first five lines of dialogue. However, the player whose card has a 1 on it sees the set $\{4, 8\}$, which has a 1 next to it in the table above, so they can deduce the integer on their card from the first five lines. By similar reasoning, if the cards are $\{1, 6, 10\}$ or $\{1, 8, 10\}$, then the player who is able to deduce the integer on their card must be holding the card with 1 on it. Therefore, the integer on Charlie's card is 1.

We have now narrowed down to 6 possibilities for how the cards are distributed:

Adina	Budi	Charlie
4	8	1
8	4	1
6	10	1
10	6	1
8	10	1
10	8	1

Since Charlie's card has 1 on it, Adina and Budi each see a 1 and one of 4, 6, 8, and 10. If Adina or Budi sees 1 and 4, then they know that the integer on their card is 8 since $\{1, 4, 8\}$ is the only possible remaining set that contains both 1 and 4. Similarly, if one of them sees 1 and 6, then they know the integer on their card is 10. If they see 1 and 8, then the integer on their card could be either 4 or 10, and if they see 1 and 10, then the integer on their card could be either 6 or 8.

In the sixth line of dialogue, we find out that after line 5, Adina does not know the integer on her card and Budi does know the integer on his card. This means Adina sees either 1 and 8 or 1 and 10, and Budi sees either 1 and 4 or 1 and 6. Of the six possibilities in the table above, the only two that satisfy both of these conditions are

Adina	Budi	Charlie
4	8	1
6	10	1

Therefore, Charlie is holding the card with 1 on it, and either Adina's card has 4 on it and Budi's has 8 on it, or Adina's card has 6 on it and Budi's has 10 on it.

In fact, both of these are possible. Denote by a the integer on Adina's card, by b the integer on Budi's card, and by c the integer on Charlie's card. We will verify that when $a = 4$, $b = 8$, and $c = 1$ the dialogue makes sense. Verifying the case when $a = 6$, $b = 10$, and $c = 1$ can be done similarly. Therefore, we assume that $a = 4$, $b = 8$, and $c = 1$.

1. Adina sees 8 and 1, neither of which is prime, so she can ask the question in line 1 since she does not know its answer.

3. Budi sees that $c = 1$ and $a = 4$ and knows that b is not prime. If $b = 8$, then $a+b+c$ is prime. If $b = 10$, then $a + b + c$ is not prime. Therefore, Budi cannot know the answer to the question in the third line before he asks it.

5. - Adina sees that $b = 8$ and $c = 1$, knows that $a+b+c = a+9$ is prime, and knows a is not prime. Therefore, she knows that either $a = 4$ or $a = 10$, but cannot tell which.
   - Budi sees that $a = 4$ and $c = 1$, knows that b is not prime, and knows that $a + b + c = 5 + b$ is prime. Therefore, he knows that $b = 6$ or $b = 8$, but cannot tell which.
   - Charlie sees $a = 4$ and $b = 8$, knows that c is one of 1, 6, 9, and 10, and knows that $a+b+c = 12+c$ is prime. Since $12+6 = 18$, $12+9 = 21$, and $12+10 = 22$ are all composite, Charlie knows at this point that $c = 1$.
6. - Budi knew that either $b = 6$ or $b = 8$ after he learned that $a + b + c$ was prime. He knows that Charlie knows the values of both a and b. If $b = 6$, then Charlie would not have been able to determine whether $c = 1$ or $c = 9$ since the sums $a + b + c = 4 + 6 + 1$ and $a + b + c = 4 + 6 + 9$ are both prime. Therefore, Budi concludes that $b = 8$.
   - Adina knows that $a = 4$ or $a = 10$ and she knows that Charlie knows that $b = 8$. She also knows that Charlie is able to deduce the value of c from the information revealed in the first four lines of dialogue. If $a = 10$, then Charlie could see an 8 and a 10 and would know that c was one of 1, 4, 6, and 9. The sum $8+10+1 = 19$ is prime, but $8+10+4$, $8+10+6$, and $8+10+9$ are all composite. This means Charlie would be able to deduce that $c = 1$ if $a = 10$. Similarly (as previously argued), if $a = 4$, then Charlie would be able to deduce that $c = 1$. Therefore, Charlie's ability to deduce the value of c after the first five lines does not tell Adina the value of a. As well, whether Adina is holding 4 or 10, Budi would not be able to tell whether he is holding 6 or 8 after the first five lines. This is because $4 + 1 + 6$, $4 + 1 + 8$, $10 + 1 + 6$, and $10 + 1 + 8$ are all prime. Therefore, Budi's inability to determine the value of b after the first five lines of dialogue does not tell Adina the value of a.
7. If $a = 10$ and $b = 6$ or $b = 8$, then Charlie would still be able to deduce that $c = 1$ after the first four lines of dialogue. However, Budi would not be able to deduce the value of b after the first five lines of dialogue. Both of these facts follow from reasoning similar to that which is above. Therefore, once Budi announces that he has deduced the integer on his card, Adina knows that $a \neq 10$, so she knows that $a = 4$.

In conclusion, the complete set of possibilities for the integers on the cards are that Adina's card has 4, Budi's card has 8, and Charlie's card has 1, or Adina's card has 6, Budi's card has 10, and Charlie's card has 1.

Problem of the Month

Problem 1: A bit of binary

October 2024

When we ordinarily write an integer, we write it in base-10, using digits from the set

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

For example, when we write 743 what we mean is

$$743 = 7 \times 10^2 + 4 \times 10^1 + 3 \times 10^0.$$

However, there is nothing special about 10, and we can use other numbers as a base! Integers can also be written in base-2, and we call this writing an integer in *binary*. When writing an integer in binary, we use powers of 2 instead of powers of 10, and we use the "digits" from the set $\{0, 1\}$ ("digits" is in scare quotes because binary digits are called *bits*). We are going to explore some problems related to writing numbers in binary.

How do we write a number, say 121, in binary? Well, it's not that different to writing it in base-10. First, find the largest power of 2 which is less than or equal to 121, which is $2^6 = 64$. Subtracting this power gives us $121 - 64 = 57$. Then we repeat with 57, and continue this way until we are left with only a power of 2. With 121 this process looks like this:

$$\begin{aligned} 121 &= 2^6 + 57 \\ 57 &= 2^5 + 25 \\ 25 &= 2^4 + 9 \\ 9 &= 2^3 + 1 \\ 1 &= 2^0 \end{aligned}$$

Once we are done with this process, we conclude that $121 = 2^6 + 2^5 + 2^4 + 2^3 + 2^0$. To be completely explicit,

$$121 = 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0.$$

More compactly, we write this as $121 = [1111001]_2$.

This process works great for natural numbers, but it also works great for all real numbers! Typically, we write real numbers in base-10. For example, $\pi = 3.1415\ldots$ means

$$\pi = 3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2} + 1 \times 10^{-3} + 5 \times 10^{-4} + \cdots.$$

To write π in binary, we follow the procedure above: find the highest power of 2 less than or equal to π, subtract it, and repeat. The first few steps look like this:

$$\begin{aligned} \pi &= 2^1 + (\pi - 2) \\ \pi - 2 &= 2^0 + (\pi - 3) \\ \pi - 3 &= 2^{-3} + \left(\pi - \frac{25}{8}\right) \end{aligned}$$

Therefore, $\pi = 1 \times 2^1 + 1 \times 2^0 + 0 \times 2^{-1} + 0 \times 2^{-2} + 1 \times 2^{-3} + \cdots$ or more succinctly, $\pi = [11.001\ldots]_2$ (take a moment and prove that these calculations are correct, that is, for example, that 2^{-3} is indeed the largest power of 2 less than or equal to $\pi - 3$).

Before we get started on the questions, here are a couple of important facts you can take for granted without proof.

Fact 1: The binary expansions $[0.a_1a_2\cdots a_k0\overline{1}]_2$ and $[0.a_1a_2\cdots a_k1]_2$ represent the same number. This is due to the fact that $\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = 1$. As a result, we never write a binary number ending in an infinite string of 1's. This is analogous to the fact that the decimal expansions $0.\overline{9}$ and 1 are decimal expansions of the same number (that number being the number 1).

Fact 2: With Fact 1 taken care of, every real number has a unique binary expansion.

Problems

1. (a) Compute the binary expansion of 279.
   (b) Let k be a positive integer. Compute the binary expansion of $2^k - 1$.
   (c) Let $\sqrt{3} = [a_0.a_1a_2a_3a_4\ldots]_2$. Compute a_0, a_1, a_2, a_3, and a_4.
2. In base-10, $\frac{1}{7} = 0.\overline{142857}$. In this question we will find the binary expansion of $\frac{1}{7}$, which will also be repeating.
   (a) Find a pair of positive integers k and n so that $2^k \cdot \frac{1}{7} = \frac{1}{7} + n$.
   (b) Let $\frac{1}{7} = [0.a_1a_2a_3\ldots]_2$ (why is the only thing to the left of the decimal point a 0?). Using your values for k and n from part (a), write down binary expansions of $2^k \cdot \frac{1}{7}$ and $\frac{1}{7} + n$ in terms of the a_i.
   (c) Compute the binary expansion of $\frac{1}{7}$. It should look like $[0.\overline{a_1a_2\cdots a_t}]$ for some t.
   (d) Compute the binary expansion of $\frac{3}{11}$.
3. Let p be a prime. Prove that when $\sqrt{p}$ is written in binary, there are infinitely many 1's and infinitely many 0's.
4. The *floor* of a real number x is denoted $\lfloor x \rfloor$, and is the largest integer n so that $n \leq x$. Prove that the sequence
$$\lfloor\sqrt{2}\rfloor, \lfloor 2\sqrt{2}\rfloor, \lfloor 3\sqrt{2}\rfloor, \lfloor 4\sqrt{2}\rfloor, \lfloor 5\sqrt{2}\rfloor \ldots$$
contains infinitely many powers of 2.

Problem of the Month
Problem 1: A bit of binary
October 2024

Hint

1. (b) Compute the binary expansion of $2^3 - 1$, $2^4 - 1$, and $2^5 - 1$. Do you notice any pattern? To prove the pattern always holds, first note that for integer $k > 1$, $2^k > 2^k - 1 > 2^{k-1}$. Then simplify $2^k - 1 - 2^{k-1}$.
   (c) Recall that $\sqrt{3} > \frac{p}{q}$ if and only if $3 > \frac{p^2}{q^2}$ (and the same is true of the reverse inequality).
2. (a) Try searching through different options for k, starting at $k = 1$ and increasing k.
   (b) What happens to the decimal expansion of a number when you multiply it by 10^k? What happens to the decimal expansion of a number of the form $0.a_1a_2a_3\ldots$ when you add an integer to it? Do the same things hold true in the world of binary expansions?
   (c) From part (b) you have two different binary expansions for the same number. By Fact 2 at the beginning of the list of problems, these two binary expansions must be identical. Compare these expressions to each other.
   (d) Start by finding integers k and n so that $2^k \cdot \frac{3}{11} = \frac{3}{11} + n$. Such integers do exist. Keep searching for them!
3. The square root of a positive integer that is not a perfect square is always irrational. You can use this fact without proof.
4. To find a power of 2 in the sequence, we are seeking integers m and k satisfying
$$2^k < m\sqrt{2} < 1 + 2^k.$$
Dividing by $\sqrt{2}$ gives
$$2^{k-1}\sqrt{2} < m < 2^{k-1}\sqrt{2} + \frac{1}{\sqrt{2}}.$$
The first inequality tells us that we should think about multiplying $\sqrt{2}$ by a power of two. The second inequality has the troublesome $\frac{1}{\sqrt{2}}$ term, which is secretly just $2^{-1}\sqrt{2}$. Think about what happens to the binary expansion of $\sqrt{2}$ when you multiply it by a power of 2.

Problem of the Month

Solution to Problem 1: A bit of binary

October 2024

1. (a) $279 = [100010111]_2$ since $279 = 2^8 + 2^4 + 2^2 + 2^1 + 2^0$.

   (b) The binary expansion of $2^k - 1$ is simply a string of k 1's. That is, $2^k - 1 = [\overbrace{11\cdots 1}^{k}]_2$. Let's prove this. First note that $2^k - 1 = 2^{k-1} + (2^k - 1 - 2^{k-1})$. Some simplifying gives $2^k - 1 - 2^{k-1} = 2^{k-1} - 1$. Therefore, our procedure for computing the binary expansion of $2^k - 1$ looks like this:

$$\begin{aligned}
2^k - 1 &= 2^{k-1} + (2^{k-1} - 1) \\
2^{k-1} - 1 &= 2^{k-2} + (2^{k-2} - 1) \\
&\vdots \\
2^2 - 1 &= 2^1 + (2^1 - 1) \\
2^1 - 1 &= 2^0
\end{aligned}$$

   Therefore $2^k - 1 = 2^{k-1} + 2^{k-2} + \cdots + 2^1 + 2^0$ so $2^k - 1 = [\overbrace{11\cdots 1}^{k}]_2$.

   (c) We could just solve this problem by letting our calculator deal with the decimal approximation of $\sqrt{3}$, but we can't really be sure it wouldn't make some rounding errors. Let's compute this, proving we have the correct binary digits along the way.

   First, since $2^2 > 3 > 1^2$, we know $2^1 > \sqrt{3} > 2^0$. Therefore, our first step in computing the binary expansion is $\sqrt{3} = 2^0 + (\sqrt{3} - 1)$ and $a_0 = 1$. To decide whether $a_1 = 0$ or $a_1 = 1$, we need to decide whether $\sqrt{3} - 1 < 2^{-1}$ or $\sqrt{3} - 1 > 2^{-1}$. We have

$$(1 + 2^{-1})^2 = \frac{9}{4} < 3$$

   so $1 + 2^{-1} < \sqrt{3}$ and $2^{-1} < \sqrt{3} - 1$. Therefore $a_1 = 1$. For the next binary digit we need to compare $\sqrt{3} - 1 - \frac{1}{2}$ with $\frac{1}{4}$. Similar to the previous computation we have

$$(1 + 2^{-1} + 2^{-2})^2 = \frac{49}{16} > 3.$$

   We then conclude $\sqrt{3} - 2^0 - 2^{-1} < 2^{-2}$ and $a_2 = 0$. To compute a_3 we need to compare $\sqrt{3} - 2^0 - 2^{-1}$ to 2^{-3}. We have

$$(1 + 2^{-1} + 2^{-3})^2 = \frac{169}{64} < 3$$

   so $\sqrt{3} - 2^0 - 2^{-1} > 2^{-3}$ and $a_3 = 1$. Once more, to compute a_4 we have

$$(1 + 2^{-1} + 2^{-3} + 2^{-4})^2 = \frac{729}{256} < 3$$

so $\sqrt{3} - 2^0 - 2^{-1} - 2^{-3} > 2^{-4}$ and $a_4 = 1$. Therefore

$$a_0 = 1, \quad a_1 = 1, \quad a_2 = 0, \quad a_3 = 1, \quad \text{and} \quad a_4 = 1$$

and $\sqrt{3} = [1.1011\ldots]_2$.

2. (a) $k = 3$ and $n = 1$ works since $2^3\frac{1}{7} = \frac{8}{7} = \frac{1}{7} + 1$. There are infinitely many other correct answers ($k = 6$ and $n = 9$ is another example), but we will use $k = 3$ and $n = 1$ going forward.

   (b) Adding 1 to the number $[0.a_1a_2\ldots]_2$ changes the expansion to $[1.a_1a_2\ldots]_2$. Just like how multiplying by 10^3 moves the decimal point three places to the right, multiplying by 2^3 moves the point in a binary expansion three places to the right (convince yourself this is true!). Therefore,

$$2^3\frac{1}{7} = [a_1a_2a_3.a_4a_5\ldots]_2 \quad \text{and} \quad \frac{1}{7} + 1 = [1.a_1a_2a_3\ldots]_2.$$

   (c) From the previous part we have two different binary expressions for the same number:

$$[a_1a_2a_3.a_4a_5\ldots]_2 = 2^3\frac{1}{7} = \frac{1}{7} + 1 = [1.a_1a_2a_3\ldots]_2.$$

   Since binary expansions are unique (see Fact 2 from above the statement of the problem on the problem sheet), these two binary expansions must be exactly the same! Comparing the bits (remember, bits are the binary digits) of these two expansions gives

$$a_1 = a_2 = 0, \quad a_3 = 1, \quad \text{and} \quad a_k = a_{k+3}$$

   for all natural numbers k. Therefore $\frac{1}{7} = [0.\overline{001}]_2$.

   (d) We will follow the same procedure as we did for computing the binary expansion of $\frac{1}{7}$ in the first three parts of this question.

   First, we wish to find integers k and n so that $2^k\frac{3}{11} = \frac{3}{11} + n$. At this point, we don't even know if such integers exist, but let's start looking anyway. If such a k and n exist, we would have

$$\frac{3 \cdot 2^k}{11} = \frac{3 + 11n}{11}$$

   so $3 \cdot 2^k = 3 + 11n$. We can now search through values of k, hoping that $3 \cdot 2^k - 3$ is a multiple of 11. Let's do exactly this.

k	$3 \cdot 2^k - 3$	multiple of 11?
1	3	no
2	9	no
3	21	no
4	45	no
5	93	no
6	189	no
7	381	no
8	765	no
9	1533	no
10	3069	YES!

Great! So $2^{10}\frac{3}{11} = \frac{3}{11} + \frac{3069}{11} = \frac{3}{11} + 279$. Now let $\frac{3}{11} = [0.a_1a_2a_3\ldots]_2$ (note that since $\frac{3}{11} < 1$, the only binary digit to the left of the point is 0). By the solution to $1(a)$ above we have

$$\frac{3}{11} + 279 = [100010111.a_1a_2a_3\ldots]_2.$$

Since multiplying by 2^{10} shifts the point 10 places to the right we have

$$2^{10}\frac{3}{11} = [a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}.a_{11}a_{12}a_{13}\ldots]_2.$$

Comparing these two expansions gives us

$$\begin{aligned} a_1 &= 0 \\ a_2 &= 1 \\ a_3 &= 0 \\ a_4 &= 0 \\ a_5 &= 0 \\ a_6 &= 1 \\ a_7 &= 0 \\ a_8 &= 1 \\ a_9 &= 1 \\ a_{10} &= 1, \text{ and} \\ a_t &= a_{t+10} \end{aligned}$$

for all integers $t \geq 1$. Therefore $\frac{3}{11} = [0.\overline{0100010111}]_2$.

3. The key observation here is that $\sqrt{p}$ is not rational. Let $\sqrt{p} = [a_na_{n-1}\cdots a_1a_0.a_{-1}a_{-2}a_{-3}\cdots]_2$. Suppose there are only finitely many 1's. Then there is some k so that a_{-k} is the very last 1 that appears. Then

$$\sqrt{p} = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \cdots + a_1 \cdot 2 + a_0 + \frac{a_{-1}}{2} + \frac{a_{-2}}{2^2} + \cdots + \frac{a_{-k}}{2^k}$$

which is a rational number, contradicting the fact that $\sqrt{p}$ is irrational. Therefore, the binary expansion of $\sqrt{p}$ must have infinitely many 1's.

Now suppose that there are only finitely many 0's. If there are only finitely many 1's, then the above argument shows $\sqrt{p}$ is rational, so we must have infinitely many 1's. Then the binary expansion must take the form

$$\sqrt{p} = [a_na_{n-1}\cdots a_1a_0.a_{-1}a_{-2}\cdots a_{-k}0\overline{1}]_2$$

that is, the binary expansion eventually becomes just a string of 1's. However (by Fact 1 at the beginning of the questions in the problem document), we know such a binary expansion is equal to the binary expansion

$$\sqrt{p} = [a_na_{n-1}\cdots a_1a_0.a_{-1}a_{-2}\cdots a_{-k}1]_2$$

and we again have only finitely many 0's (by assumption) and finitely many 1's (as we have just shown), contradicting the fact $\sqrt{p}$ is irrational. Alas, we are forced to conclude that the binary expansion of $\sqrt{p}$ has infinitely many 0's and infinitely many 1's.

4. Let $\sqrt{2} = [1.a_1a_2a_3\ldots]_2$. Choose k so that $a_k = 1$ (such a k exists since there are infinitely many 1's in the binary expansion of $\sqrt{2}$ by Question 3). Then

$$2^{k-1}\sqrt{2} = [1a_1a_2\cdots a_{k-1}.1a_{k+1}a_{k+2}\cdots]_2$$

so

$$\lfloor 2^{k-1}\sqrt{2}\rfloor = [1a_1a_2\cdots a_{k-1}]_2 \quad \text{and} \quad 2^{k-1}\sqrt{2} - \lfloor 2^{k-1}\sqrt{2}\rfloor = [0.1a_{k+1}a_{k+2}\cdots]_2.$$

Since there are infinitely many 1's in the binary expansion of $\sqrt{2}$, $[0.0a_{k+1}a_{k+2}\cdots]_2 > 0$. Therefore,

$$2^{k-1}\sqrt{2} - \lfloor 2^{k-1}\sqrt{2}\rfloor = [0.1]_2 + [0.0a_{k+1}a_{k+2}\cdots]_2 > [0.1]_2 = \frac{1}{2}.$$

By the definition of the floor function, $1 > 2^{k-1}\sqrt{2} - \lfloor 2^{k-1}\sqrt{2}\rfloor$. Combining the two inequalities gives

$$1 > 2^{k-1}\sqrt{2} - \lfloor 2^{k-1}\sqrt{2}\rfloor > \frac{1}{2}.$$

Some manipulation of the inequalities gives

$$2^{k-1}\sqrt{2} - 1 < \lfloor 2^{k-1}\sqrt{2}\rfloor < 2^{k-1}\sqrt{2} - \frac{1}{2}.$$

Multiplying all sides of the inequalities by $\sqrt{2}$ and then adding $\sqrt{2}$ gives

$$2^k < (\lfloor 2^{k-1}\sqrt{2}\rfloor + 1)\sqrt{2} < 2^k + \frac{\sqrt{2}}{2}.$$

Let $m = \lfloor 2^{k-1}\sqrt{2}\rfloor + 1$, which is a positive integer. Since $\frac{\sqrt{2}}{2} < 1$ we have

$$2^k < m\sqrt{2} < 2^k + 1$$

and therefore $\lfloor m\sqrt{2}\rfloor = 2^k$. Since there are infinitely many k so that $a_k = 1$, there are infinitely many elements of the sequence

$$\lfloor\sqrt{2}\rfloor, \lfloor 2\sqrt{2}\rfloor, \lfloor 3\sqrt{2}\rfloor, \lfloor 4\sqrt{2}\rfloor, \lfloor 5\sqrt{2}\rfloor, \ldots$$

that are powers of 2.

Problem of the Month

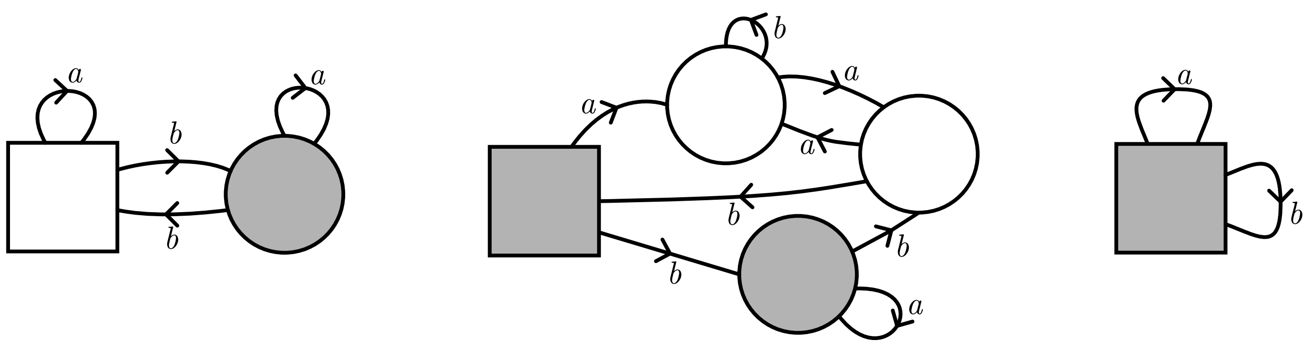
Problem 2: Manuals for Robots

Nov 2024

A *course* for a robot is a finite set of places (denoted by circles or squares) with arrows labelled a and b between places, satisfying the following conditions:

1. For every place s, there is exactly one arrow labelled a and one arrow labelled b which starts at s.
2. There is exactly one place called the *starting* place, denoted by a square.
3. Some positive number of places are called *finishing* places, and they are denoted by being shaded. The starting place can be a finishing place.
4. The course is *connected*. That is, there is a way to get from the starting place to any other place by following (possibly several) arrows.

While there is exactly one arrow labelled a and one arrow labelled b starting at every place, there may be multiple arrows labelled a ending at a particular place, or none at all! Take a moment to check that the following three examples are indeed courses.



Course 1 Course 2 Course 3

For a particular course, we can give a robot instructions as to how to move from place to place in the form of a string. A *string* is a finite sequence of a's and b's (for example, $abaa$).

For each string, the robot begins at the starting place, and follows the arrows in the order they appear in the string (reading from left to right), moving from place to place.

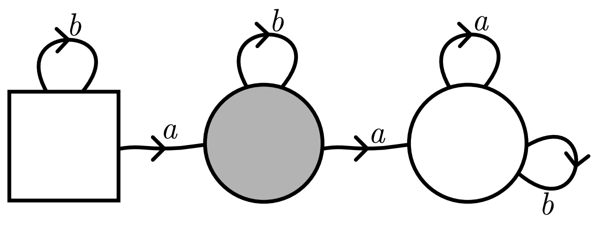
If the robot ends at a finishing place, then the string is *accepted*. Otherwise, the string is *rejected*. Notice that by Condition 1 in the definition of a course, the string completely determines which places the robot visits.

The set of accepted strings is the *manual* for that course. For example, the manual for Course 3 above is the set of all strings. Convince yourself that the manual for Course 1 is the set of strings with an odd number of b's.

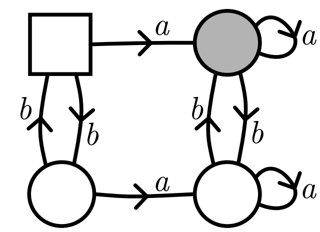
Problems

1. Decide which of the following strings belong to the manual for Course 2 from the first page: abb, aab, $baaaa$, $abba$.

2. Describe the manuals for the following courses:



(a)



(b)

3. (a) Construct a course whose manual is the set of three strings $\{a, ab, bbb\}$.

   (b) Construct a course whose manual is the set of all strings where the number of a's in the string is a multiple of 3.

4. For this problem we need to introduce some language and notation.

   The *length* of a string is the number of characters in the string. For example, $aaba$ has length 4. The string of length 0 is called the *empty string* and we denote it by e.

   If x and y are strings, then xy is the *concatenation* of the two strings. The string x^n is x concatonated with itself n times. For example, if $x = bab$, $y = ba$, and $z = aab$, then $xy^3z = babbababaaab$. Define x^0 to be the empty string e.

   A *substring* of a string x is a string consisting of consecutive letters from x. For example, ab, ba, e, and $baba$ are all substrings of $baba$. The string bba is not a substring of $baba$.

   (a) Suppose a course has k places, and let w be a string in its manual of length at least k. Show that there is a substring y of w with length at least 1 and at most k so that when it is deleted from w, the remaining word is also in the manual.

   (b) Suppose a course has k places, and let w be a string in its manual of length at least k. Show that you can write $w = xyz$ with the property that $y \neq e$, the length of y is at most k, and for all natural numbers n, xy^nz is also in the manual.

   (c) Prove that the manual for a course cannot be the set of all strings with length equal to a perfect square.

   (d) Prove that the manual for a course cannot be the set of all strings that are palindromes. (A *palindrome* is a string that is the same when written backwards. The strings $abba$ and aaa are palindromes, but ba is not.)

Problem of the Month

Problem 2: Manuals for Robots

November 2024

Hint

1. Put your finger on the starting place (the square) and pretend you are the robot, following the arrows as they appear in each string. If you end at a finishing place (a shaded shape), the string is in the manual. If you don't end at a finishing place, the string is not in the manual.

2. (a) Decide whether or not the following strings are in the manual:

$$bbb, bbabb, bbabba, bbbbbabbbbb, bbbbbabbbabb.$$

What do you notice?

(b) Think about what it takes to move from the top row of places to the bottom row of places, and from the bottom row to the top row. Think about what it takes to move from the left column to the right column, and what it takes to move from the right column to the left column.

3. (a) First draw in the arrows and places corresponding to the desired finite set of words. Create another place that acts as a disposal site for the rest of the words. Make sure that once the robot is in that place, it can never get out!

(b) Think carefully about Course 1 from the first page of the problem, except pretend that the square is shaded instead of the circle.

4. (a) Suppose a string has length 3. As the robot is travelling according to the instructions from the string, how many different places can the robot visit? What about if the string has length 1? What if the string has length k?

(b) If a substring of a string returns the robot to a place it has already visited, what happens if you repeat that substring again?

(c) Use Part (b), and pay close attention to the lengths of the words xy^nz.

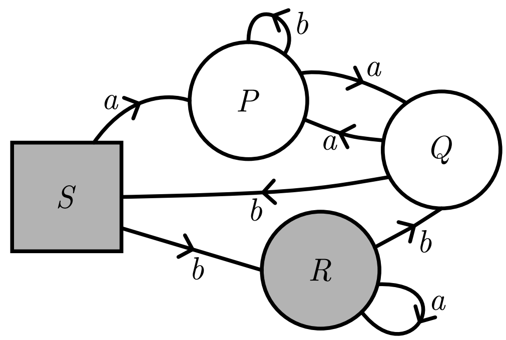
(d) Suppose there are k places in a course, and w is a string in the manual of length at most k. By Part (b), $w = xyz$. Can you put any restrictions on the length of x? If you can, see if you can cleverly select a palindrome w so that when you write $w = xyz$ as in Part (b), xy^2z is not a palindrome.

Problem of the Month

Solution to Problem 2: Manuals for Robots

November 2024

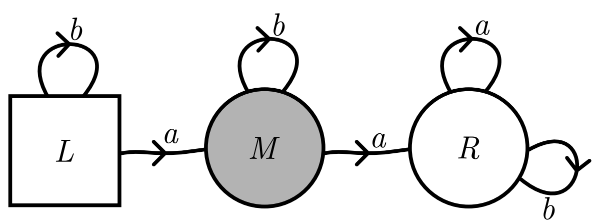
1. Here is Course 2, with some labels on the places.



The string abb ends at place P. The string aab ends at place S. The string $baaaa$ ends at place R. The string $abba$ ends at place Q.

The finishing places of the course are S and R. Therefore aab and $baaaa$ are in the manual, and abb and $abba$ are not in the manual.

2. (a) The manual for this course is the set of strings with exactly one a.



To justify this statement, name the places L, M, R (for left, middle, and right) from left to right respectively, as above. Note that L is the starting place, and M is the only finishing place.

There are a few important properties to notice about this course.

- The only way to move from place L to place M is through the a arrow.
- The only way to move from place M to place R is through the a arrow.
- There is no way to move to place L from another place.
- There is no way to move from place R to any other place.

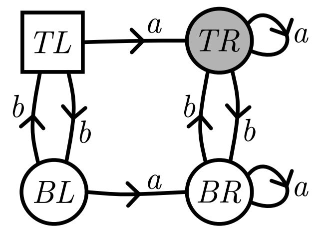
Suppose now that a string contains zero a's. Then the robot ends at place L so the string is not in the manual.

Suppose a string contains at least two a's. After the first two a's, the robot is at place R. Since there is no way to move from place R, the robot stays at place R until the string is completed. Therefore the string is not in the manual.

Finally, suppose a string contains exactly 1 a. Until the robot encounters the a, it stays at place L. The a moves the robot to place M. The rest of the string consists only of b's, so the robot ends at place M. We can conclude the string is part of the manual.

Therefore the manual consists precisely of those strings with exactly one a.

(b) The manual is the set of strings that has at least one a and an even number of b's.



Let's justify this. Label the places TL, TR, BL, BR for top left, top right, bottom left, and bottom right as above. The starting place is TL and the only finishing place is TR. Here are the important properties of this course.

i. If the robot is in the top row (TL or TR), then moving along an arrow labelled b moves the robot to the bottom row (BL or BR). This is the only way to move from the top row to the bottom row.

ii. If the robot is in the bottom row, then moving along an arrow labelled b moves the robot to the top row. This is the only way to move from the bottom row to the top row.

iii. If the robot is in the left column (TL or BL), then moving along an arrow labelled a moves the robot to the right column (TR or BR). Further, this is the only way to move from the left column to the right column.

iv. Once the robot is in the right column, it stays in the right column.

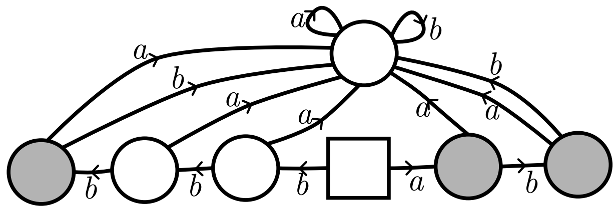
Suppose we have a string in the manual. Since the robot starts in the left column and finishes in the right column, the string must contain at least one a by Properties (iii) and (iv). Since the robot starts and ends in the top row, by Properties (i) and (ii), there must be an even number of b's in the string.

On the other hand, suppose there is a string with an even number of b's and at least one a. By Properties (i) and (ii), the robot must move between the top and bottom rows an even number of times. Since it starts at the top row, it must end at the top row. By Properties (iii) and (iv), since the robot has traversed at least one arrow labelled a, it must end up in the right column. We conclude that the robot ends in the place TR, and therefore the string belongs to the manual.

Therefore the manual consists exactly of those strings with at least one a and an even number of b's.

3. There are many possible correct courses for this question. We will give one correct answer for each part.

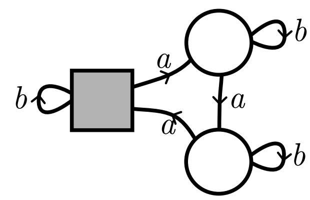
(a) Here is such a course:



Let's justify ourselves. There are three finishing places, and for each one there is only one way to get from the starting place to that finishing place. The three paths are a, ab, and bbb. Therefore the manual for this course is the set of three strings $\{a, ab, bbb\}$.

Notice how there is a place above which acts as a kind of garbage can for strings that don't belong to the desired manual. We can imitate this construction in general to construct a course with any finite set of strings as its manual!

(b) Here is such a course:



To see why this is the case, notice that every time an a appears in a string, the robot moves one place clockwise. Since there are 3 places, the robot returns to the starting place (which is also the only finishing place) exactly when there has been a multiple of 3 a's in the string.

Of course, there is nothing special about the number 3 here. Fix a positive integer k. We can imitate this construction to build a course whose manual is the set of all strings with a multiple of k appearances of the letter a.

4. (a) Notice that if a string has length 1, then the robot will visit two, not necessarily distinct, places - the starting place and some other place. If a string has length 2, then the robot will visit three, not necessarily distinct, places on its journey. If a string has length k, then the robot will visit $k + 1$ not necessarily distinct places on its journey. Since there are k places in our course, if a robot follows the instructions of a string of length at least k, then there must be some place which the robot visits twice (by the pigeonhole principle).

Let w be a string of length at least k in the manual. Let's call the first place that is visited twice p. Let's split w up into three substrings. The first substring, x, will be the string that takes the robot from the starting place to p for the first time. Note that x may be empty if p is the starting place. Then there is some substring y that takes the robot from p back to p for the second time. Note that $y \neq e$ since we are waiting for the robot to visit p again. Let z be the rest of the string w, which takes the robot from p (which has now been visited twice by the robot) to one of the finishing places. Note that z may be empty. While travelling along the course according to the instructions in z, the robot may visit p again, but we don't care!

We now have that $w = xyz$, where $y \neq e$ and y takes the robot from p to p. The string x takes the robot from the starting place to p, and the string z takes the robot from p to a finishing place. Therefore the string xz takes the robot from the starting place to a finishing place. Alas, xz is also in the manual!

(b) Let $w = xyz$, where x, y, and z are constructed as in the solution to part (a). Notice that since y takes the robot from place p to place p, then y^n also takes the robot from place p to place p. It simply repeats the path n times.

Consider now the string xy^nz for any natural number n. The string x takes the robot from the starting place to p, the string y^n takes the robot from p to p, and the string z takes the robot from p to a finishing place. Therefore a robot following the instructions given by the string xy^nz travels from the starting place to a finishing place, so xy^nz is in the manual.

(c) Suppose the set of strings of perfect-square length is the manual for some course, and suppose that course has k places. Choose any string w of length k^2. Since the length of w is a perfect square, it is in the manual. Since $k^2 \geq k$, by part (b) we can write $w = xyz$ for some substring $y \neq e$ so that xy^nz is in the manual for every natural number n. Let l be the length of w and let $d \geq 1$ be the length of y. Then the sequence of words in the manual

$$xyz, xy^2z, xy^3z, \ldots$$

have lengths

$$l, l+d, l+2d, \ldots$$

respectively. Said another way, the lengths of the words $xyz, xy^2z, xy^3z, \ldots$ form an arithmetic sequence. Therefore, in order to complete the problem, we have to prove the following fact:

Fact: In an arithmetic sequence, there is at least one number that is not a perfect square.

Proof. Let l and d be integers with $d \geq 1$, and consider the arithmetic sequence $l, l+d, l+2d, \ldots$. Let $t \geq d$ be an integer. Then

$$(t+1)^2 - t^2 = 2t + 1 \geq 2d + 1 > d.$$

Exactly one of every d consecutive numbers greater than l is in the arithmetic sequence. Choose t to be any integer satisfying $t \geq d$ and $t^2 \geq l$. Since the difference between $(t+1)^2$ and t^2 is greater than d, there must be some number in the arithmetic sequence strictly between t^2 and $(t+1)^2$. However, there are no perfect squares between t^2 and $(t+1)^2$, completing the proof. $\square$

Great! We have just shown that at least one of the lengths of $xyz, xy^2z, xy^3z, \ldots$ is not a perfect square, but they are all in the manual. Therefore, there is no course whose manual consists exactly of all strings with perfect square lengths.

(d) As above, suppose there is a course with manual consisting exactly of all palindromes, and suppose the course has k places. Then the string $w = a^kba^k$ is in the manual and has length $2k + 1 > k$. By Part (b), we can write $w = xyz$ with $y \neq e$ and xy^nz in the manual for all natural numbers n.

By the construction of x, y, and z in the solution to Part (a), the substring xy takes the robot from the starting place to the second occurrence of some place. By the pigeonhole principle, this has to happen within the robot visiting $k+1$ places, which happens after moving across k arrows. It follows that xy has length at most k.

Therefore to write $a^kba^k = xyz$ with $y \neq e$ and the length of xy at most k, we must have that $x = a^t$ and $y = a^s$ with $s \geq 1$ and $s + t \leq k$. This is because any substring at the beginning of the string a^kba^k of length at most k must just be a string of a's. It follows that $z = a^{k-s-t}ba^k$.

Now $xy^2z = a^ta^{2s}a^{k-s-t}ba^k$. Since $t + 2s + k - s - t = s + k > k$, xy^2z is not a palindrome but it is in the manual. We have a contradiction and can conclude that there is no course whose manual is the set of all palindromes.

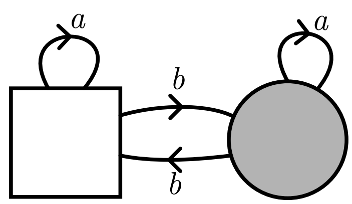
Problem of the Month

Curious Context for Problem 2: Manuals for Robots

November 2024

Regular languages.

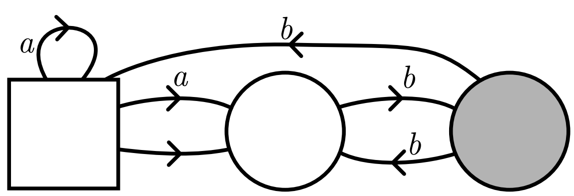
In November's problem you were asked to study the set of strings that form the manual for a particular course. In computer science, these courses are called *Deterministic Finite Automata*, or DFAs. A set of strings which arises as the manual for a DFA is called a *regular language*. For example, the manual for the DFA below is the set L of all strings with an odd number of bs. So L is an example of a regular language.



In Problem 4 you showed that the set of strings with length equal to a perfect square, and the set of palindromes, are both not regular languages. The tool used to prove that these are not regular languages is presented in Problem 4(b), and is known as the *pumping lemma*. The pumping lemma was first proved in 1959 by Michael Rabin and Dana Scott [1]. They used the pumping lemma to prove that the set of all strings of the form $a^n b a^n$, where n is a natural number, is not a regular language.

Nondeterministic finite automata.

In the definition of a DFA, we could relax the condition on the arrows, and allow any number of arrows labelled a, and any number of arrows labelled b to leave from any place (instead of exactly one of each). We can even have some arrows without a label at all, allowing you to move between places without using a letter. Such courses are called *Nondeterministic finite automata*, or NFAs. Notice that in a DFA, once you have a string, your path through the arrows is completely determined. In an NFA, you may have some choices. Here is an example of an NFA:



On first glance, it appears that NFAs allow you to have much more interesting languages (or "manuals" in the language of the POTM). Remarkably, this is not the case! In the same paper that introduced the pumping lemma, Rabin and Scott proved that any language attained from an NFA can be attained from a DFA. Said another way, if a set of strings is the manual for some NFA, then it's the manual for some DFA and is therefore a regular language.

Regular expressions.

Regular expressions are a tool used in computer programming to search through a list of words and find those which satisfy some condition. For example, you can use regular expressions to search through a list of words and return those which start and end with the letter 'c'. Regular expressions are a great tool to study patterns in written pieces of work, or to get a computer to solve a crossword by brute force! When you instruct a computer to use a regular expression, the computer creates an NFA and runs each word in your list through the NFA, checking if it's part of the manual.

Chomsky hierarchy.
In linguistics, there is a notion of computational complexity of a particular language, captured by something called the *Chomsky hierarchy*. Roughly, it measures how much computational power is needed to parse a sentence in that language. There are four types of grammars in the hierarchy, and regular languages are the simplest type (what is referred to as Type-3). The other types of grammars, in increasing order of complexity, are called context-free, context-sensitive, and recursively enumerable.

References

[1] Rabin, M. O. and Scott, D. *Finite automata and their decision problems.* IBM J. Res. Develop. 3 (1959), pp. 114-125.

Problem of the Month
Problem 3: Three-sign sums

December 2024

This month's problem is an extension of Question B3 from the 2024 Canadian Intermediate Mathematics Contest, which was run by the CEMC in November 2024. The question that appeared on the contest is on its own page at the end of this problem. As a warm up, try the problem yourself and pay attention to the differences between the contest problem and this Problem of the Month.

Given an increasing list of integers $L = \{a_1, a_2, \ldots, a_k\}$, the *3-sign sum* of the list L, denoted $\mu(L)$, is the sum of the integers in the list, in order, except that every third integer is subtracted instead of added. For example, if $L = \{3, 4, 5, 8, 10, 11, 13\}$, then $\mu(L) = 3 + 4 - 5 + 8 + 10 - 11 + 13 = 22$.

Let n be a positive integer, and consider the list $\{1, 2, 3, \ldots, n\}$. We define the integer f_n to be the sum of all 3-sign sums of all increasing sublists of $\{1, 2, 3, \ldots, n\}$. For example,

$$f_3 = \mu(\{1\}) + \mu(\{2\}) + \mu(\{3\}) + \mu(\{1, 2\}) + \mu(\{1, 3\}) + \mu(\{2, 3\}) + \mu(\{1, 2, 3\}).$$

The problems below use binomial coefficients and the binomial theorem. If you are unfamiliar with, or need a refresher for, these concepts, please see this Problem of the Month lesson.

1. (a) Compute f_3, f_4, and f_5.

   (b) Verify that $f_5 = 2f_4 + 5\left(\binom{4}{0} + \binom{4}{1} - \binom{4}{2} + \binom{4}{3} + \binom{4}{4}\right)$.

2. For all integers $n \geq 2$, prove that $f_{n+1} = 2f_n + (n+1)\left(b_0\binom{n}{0} + b_1\binom{n}{1} + b_2\binom{n}{2} + \cdots + b_n\binom{n}{n}\right)$ where

$$b_t = \begin{cases} 1 & \text{if } t+1 \text{ is not a multiple of 3} \\ -1 & \text{if } t+1 \text{ is a multiple of 3.} \end{cases}$$

For the remainder of the problems, our goal is to work out how to compute the expression

$$b_0\binom{n}{0} + b_1\binom{n}{1} + b_2\binom{n}{2} + \cdots + b_n\binom{n}{n}.$$

With that in mind, let α be a number that satisfies $\alpha^2 + \alpha = -1$.

It turns out that there is no real number α with this property (see if you can prove this!), but we can still work with α as a number. We simply treat α like a variable, with the added flexibility that we can replace $\alpha^2 + \alpha$ with -1.

It's very likely that you already have experience doing something like this. For example, when we write $\sqrt{2}$, it's not important that $\sqrt{2} \approx 1.41$. The important thing is that the number satisfies $(\sqrt{2})^2 = 2$. So, when working with $\sqrt{2}$, we simply treat it like a variable with the added bonus that we can replace $(\sqrt{2})^2$ with 2. Similarly, when we write a fraction like $\frac{5}{3}$, while it's true that this number is equal to $1.\overline{6}$, the important thing is that when you multiply $\frac{5}{3}$ by 3, you get 5.

3. Evaluate the following expressions (they should all be integers!).

(a) α^3

(b) $\alpha^8 + \alpha^4 + \alpha^9$

(c) $(1+\alpha) - (1+\alpha)^2$

4. Let $n \geq 1$ be an integer. Let $g_n(x) = (1+x)^n$.

(a) Find numbers A, B, and C in terms of α such that

$$b_0\binom{n}{0} + b_1\binom{n}{1} + b_2\binom{n}{2} + \cdots + b_n\binom{n}{n} = Ag_n(1) + Bg_n(\alpha) + Cg_n(\alpha^2).$$

[Note: The binomial theorem will be essential here.]

(b) Using the values you found in part (a), Let $d_n = Ag_n(1) + Bg_n(\alpha) + Cg_n(\alpha^2)$. Evaluate d_n (it is always an integer!). Keep in mind that the value of d_n may depend on n.

5. Evaluate $f_6, f_7, f_8, f_9, f_{10}, f_{11}$, and f_{12}.

Here is Question B3 from the 2024 Canadian Intermediate Mathematics Contest.

Given an increasing list of consecutive integers, the *3-sign sum* of the list is the sum of the integers in the list, in order, except that every third integer is subtracted instead of added. For example, the 3-sign sum of the list 3, 4, 5, 6, 7, 8, 9 is $3 + 4 - 5 + 6 + 7 - 8 + 9 = 16$.

(a) Determine the 3-sign sum of 8, 9, 10, 11, 12, 13, 14, 15.

For a positive integer n, a *slice* of the list 1, 2, 3, $\ldots$, $n-1$, n is an increasing list of at least 1 and at most n consecutive integers, each of which is between 1 and n inclusive. For example, 1, 2 and 2, 3, 4 are both slices of the list 1, 2, 3, 4, 5. As another example, the list 1, 2, 3 has a total of six slices. They are given in the left column of the table below with their 3-sign sums in the right column.

Slice	3-sign sum
1, 2, 3	$1+2-3=0$
1, 2	$1+2=3$
2, 3	$2+3=5$
1	1
2	2
3	3

For a positive integer n, the *Ghimire number* of n, denoted G_n, is the sum of the 3-sign sums of all slices of 1, 2, 3, $\ldots$, $n-1$, n. For example, using the information from the table above, $G_3 = 0 + 3 + 5 + 1 + 2 + 3 = 14$.

(b) For each integer $n \geq 1$, show that $\dfrac{G_{3n} - 2G_{3n-1} + G_{3n-2}}{3}$ is a perfect square.

(c) Determine the remainder when $G_{2025} - G_{2024}$ is divided by 27.

Problem of the Month

Problem 3: Three-sign sums

December 2024

Hint

1. Ignoring the empty sublist, there are fifteen sublists of $\{1, 2, 3, 4\}$. However, seven of those are sublists of $\{1, 2, 3\}$. So, when computing f_4, you have already done almost half the work when you computed f_3! For the remaining half of the work, notice that $\mu(\{a, b, c\}) = \mu(\{a, b\}) - c$ and $\mu(\{a, b, c, d\}) = \mu(\{a, b, c\}) + d$.

   See if you can then use your work for f_4 to reduce the work required for you to compute f_5. Alternatively, ignoring the empty sublist, there are thirty-one sublists of $\{1, 2, 3, 4, 5\}$, you can just roll up your sleeves and compute the 3-sign sums of all of them!

2. Split up your computation of f_{n+1} into adding up the 3-sign sums of those sublists of $\{1, \ldots, n+1\}$ that contain $n+1$, and those that do not contain $n+1$. When adding up the 3-sign sums of those sublists that contain $n+1$, notice that $\mu(\{a, b, n+1\}) = \mu(\{a, b\}) - (n+1)$ and $\mu(\{a, b, c, n+1\}) = \mu(\{a, b, c\}) + (n+1)$.

3. We have $\alpha^2 + \alpha = -1$. Rearranging we get

   $$-\alpha = 1 + \alpha^2, \quad -\alpha^2 = 1 + \alpha, \quad \text{and} \quad \alpha^2 + \alpha + 1 = 0.$$

   Also, remember that $\alpha^4 = \alpha(\alpha^3)$.

4. (a) Use the binomial theorem to expand $g_n(1)$, $g_n(\alpha)$ and $g_n(\alpha^2)$, keeping in mind your answer from 3(a). What happens if you multiply $g_n(\alpha)$ and $g_n(\alpha^2)$ by powers of α?

   Compute $g_n(1) + g_n(\alpha) + g_n(\alpha^2)$. This isn't quite what you want, but can you adjust the terms somehow to get what you want?

   (b) You should find that d_n involves powers of (-1) in terms of n, and powers of α in terms of n. Powers of (-1) depend on what the remainder of the power is when divided by 2. How do powers of α behave? You may have to split your computation of d_n up into 6 cases.

5. Combine your answers from 1(a), 2, and 4(b).

Problem of the Month

Solution to Problem 3: Three-sign sums

December 2024

1. (a) We have

$$\begin{aligned} f_3 &= \mu(\{1\}) + \mu(\{2\}) + \mu(\{3\}) + \mu(\{1,2\}) + \mu(\{1,3\}) + \mu(\{2,3\}) + \mu(\{1,2,3\}) \\ &= 1 + 2 + 3 + (1+2) + (1+3) + (2+3) + (1+2-3) \\ &= 18. \end{aligned}$$

For f_4, we will organise ourselves a little differently to make computing f_5 a little easier. Notice that if a sublist of $\{1,2,3,4\}$ does not contain 4, then it is a sublist of $\{1,2,3\}$. Therefore we have

$$\begin{aligned} f_4 &= f_3 + \mu(\{4\}) + \mu(\{1,4\}) + \mu(\{2,4\}) + \mu(\{3,4\}) \\ &\qquad + \mu(\{1,2,4\}) + \mu(\{1,3,4\}) + \mu(\{2,3,4\}) + \mu(\{1,2,3,4\}) \\ &= 18 + 4 + (1+4) + (2+4) + (3+4) \\ &\qquad + (1+2-4) + (1+3-4) + (2+3-4) + (1+2-3+4) \\ &= 44. \end{aligned}$$

When computing f_4, notice that if we ignore all the 4s that showed up in the sum, what is left over is again a copy of f_3. With this in mind, for f_5 we have

$$\begin{aligned} f_5 &= f_4 + 5 + (1+5) + (2+5) + (3+5) + (4+5) \\ &\qquad + (1+2-5) + (1+3-5) + (1+4-5) \\ &\qquad + (2+3-5) + (2+4-5) + (3+4-5) \\ &\qquad + (1+2-3+5) + (1+2-4+5) + (1+3-4+5) + (2+3-4+5) \\ &\qquad + (1+2-3+4+5) \\ &= f_4 + f_4 + (5) + (5+5+5+5) - (5+5+5+5+5+5) + (5+5+5+5) + (5) \\ &= 44 + 44 + 5(1+4-6+4+1) \\ &= 108. \end{aligned}$$

The 5s in the third-last line are grouped by whether they come from computing $\mu(L)$ for a list L of length 1, 2, 3, 4, or 5.

(b) We have $\binom{4}{0} = \binom{4}{4} = 1$, $\binom{4}{1} = \binom{4}{3} = 4$, and $\binom{4}{2} = 6$. Then

$$2f_4 + 5\left(\binom{4}{0} + \binom{4}{1} - \binom{4}{2} + \binom{4}{3} + \binom{4}{4}\right) = 2(44) + 5(1+4-6+4+1) = 108$$

which is the value we obtained for f_5.

2. Our computation of f_5 in Problem 1(a) above gives us some hints as to how to prove this result. Let's pay close attention to this situation first before embarking on the general proof.

In the solution to 1(a) we arrived at the expression

$$f_5 = 2f_4 + (5) + (5+5+5+5) - (5+5+5+5+5+5) + (5+5+5+5) + (5).$$

The number of 5s in the first set of parentheses is the number of sublists of $\{1,2,3,4,5\}$ of length 1 that contain 5. There is only one such list, namely $\{5\}$.

The number of 5s in the second set of parentheses is the number of sublists of $\{1,2,3,4,5\}$ of length 2 that contain 5. Every such list is of the form $\{k,5\}$, where $1 \le a \le 4$. There are $4 = \binom{4}{1}$ ways to choose an element a from $\{1,2,3,4\}$, so there are four sublists of length 2 that contain 5.

There are six 5s in the third set of parentheses. This is the number of sublists of $\{1,2,3,4,5\}$ of length 3 that contain 5. Every such sublist is of the form $\{a,b,5\}$ where $a < b$ and a and b belong to the set $\{1,2,3,4\}$. The number of ways we can choose two distinct elements a and b from $\{1,2,3,4\}$ is precisely the binomial coefficient $\binom{4}{2} = 6$.

Similarly, there are four 5s in the fourth set of parentheses because there are $\binom{4}{3} = 4$ ways to select three elements a,b,c from $\{1,2,3,4\}$ to create a sublist $\{a,b,c,5\}$ of length 4.

Finally there is $\binom{4}{4} = 1$ way to choose four elements from $\{1,2,3,4\}$ to create a list of length 5 containing 5, which is the list $\{1,2,3,4,5\}$.

Notice that the third set of parentheses is negated, and all the others are left as they are. Let's look at this a little more closely. Here is what the 3-sign sum of lists containing a 5 look like, for lists of length 1, 2, 3, 4, and 5 respectively:

$$\begin{aligned}
\mu(\{5\}) &= 5\\
\mu(\{a,5\}) &= a+5\\
\mu(\{a,b,5\}) &= a+b-5\\
\mu(\{a,b,c,5\}) &= a+b-c+5\\
\mu(\{a,b,c,d,5\}) &= a+b-c+d+5.
\end{aligned}$$

The only time the 5 appears negated is when computing the 3-sign sum of a list of length 3.

Great! Let's look at the general case now. We wish to relate f_{n+1} to f_n. We can split up the computation of f_{n+1} into summing up the 3-sign sums of sublists of $\{1,\ldots,n+1\}$ that contain $n+1$, and those that do not contain $n+1$.

The sum of all the $\mu(L)$ where $n+1$ is not in L is simply summing up $\mu(L)$ for L a sublist of $\{1,\ldots,n\}$, which is precisely f_n. Therefore we can write

$$f_{n+1} = f_n + S$$

where S is the sum of all 3-sign sums of sublists that contain $n+1$. Let's look at an arbitrary term from the sum S. For what follows, we must allow the empty list $\emptyset$ to be a sublist of $\{1,\ldots,n\}$ to be a sublist, and we define $\mu(\emptyset) = 0$.

A sublist of length k that contains $n+1$ is of the form $\{a_1,a_2,\ldots,a_{k-1},n+1\}$ where $\{a_1,a_2,\ldots,a_{k-1}\}$ is a sublist of $\{1,\ldots,n\}$. So

$$\mu(\{a_1,a_2,\ldots,a_{k-1},n+1\}) = \begin{cases} \mu(\{a_1,a_2,\ldots,a_{k-1}\}) - (n+1) & \text{if } k \text{ is a multiple of 3,}\\ \mu(\{a_1,a_2,\ldots,a_{k-1}\}) + (n+1) & \text{if } k \text{ is not a multiple of 3.}\end{cases}$$

Observe that $\mu(\{a_1, a_2, \ldots, a_{k-1}\})$ is the 3-sign sum of a sublist of $\{1, \ldots, n\}$.

Every sublist of $\{1, \ldots, n+1\}$ that contains $n+1$ gives rise to a sublist of $\{1, \ldots, n\}$ by removing $n+1$ from the list. Furthermore, every sublist of $\{1, \ldots, n\}$ gives rise to a sublist of $\{1, \ldots, n+1\}$ containing $n+1$ by simply appending $n+1$ on to the end of the list. Therefore, when computing the sum of all 3-sign sums of sublists of $\{1, \ldots, n+1\}$ containing $n+1$, we are left with the sum of all 3-sign sums of sublists of $\{1, \ldots, n\}$ plus some number of $(n+1)$s. More formally we have

$$S = f_n + M(n+1)$$

for some integer M. To figure out the value of M, we must pay attention to the length of each sublist. Sublists of $\{1, \ldots, n+1\}$ containing $n+1$ with length a multiple of three contribute -1 to the value of M, and sublists of $\{1, \ldots, n+1\}$ containing $n+1$ whose length is not a multiple of three contribute $+1$. So, in order to figure out what M is, we must count the number of sublists containing $n+1$ of each length.

The number of sublists of $\{1, \ldots, n+1\}$ of length k containing $n+1$ is equal to the number of sublists of $\{1, \ldots, n\}$ of length $k-1$. The number of sublists of $\{1, \ldots, n\}$ of length $k-1$ is the binomial coefficient $\binom{n}{k-1}$. To write down an expression for M, we must first introduce the integer b_t. Let t be an integer and define

$$b_t = \begin{cases} 1 & \text{if } t+1 \text{ is not a multiple of } 3 \\ -1 & \text{if } t+1 \text{ is a multiple of } 3. \end{cases}$$

Let C_k be the number of sublists of $\{1, \ldots, n+1\}$ of length k that contain $n+1$. Then

$$M = b_0 C_1 + b_1 C_2 + \cdots + b_n C_{n+1}.$$

But from our discussion above we have $C_k = \binom{n}{k-1}$. Therefore,

$$M = b_0 \binom{n}{0} + b_1 \binom{n}{1} + \cdots + b_n \binom{n}{n}.$$

Putting all of this together we have

$$\begin{aligned} f_{n+1} &= f_n + f_n + M(n+1) \\ &= 2f_n + (n+1)\left(b_0 \binom{n}{0} + b_1 \binom{n}{1} + \cdots + b_n \binom{n}{n}\right) \end{aligned}$$

completing the proof.

3. (a) We have

$$\begin{aligned} \alpha^3 &= (\alpha^2)\alpha \\ &= (-1-\alpha)\alpha \\ &= -\alpha - \alpha^2 \\ &= 1. \end{aligned}$$

(b) Using the fact that $\alpha^3 = 1$ we have

$$\begin{aligned}\alpha^8 + \alpha^4 + \alpha^9 &= (\alpha^3)(\alpha^3)(\alpha^2) + (\alpha^3)(\alpha) + (\alpha^3)^3\\ &= \alpha^2 + \alpha + 1\\ &= -1 + 1\\ &= 0.\end{aligned}$$

(c)

$$\begin{aligned}(1+\alpha) - (1+\alpha)^2 &= (1+\alpha) - (-\alpha^2)^2\\ &= (1+\alpha) - (\alpha^4)\\ &= 1 + \alpha - \alpha && \text{since } \alpha^3 = 1\\ &= 1.\end{aligned}$$

4. (a) Using the binomial theorem we have

$$\begin{aligned}g_n(1) &= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}\\ g_n(\alpha) &= \binom{n}{0} + \binom{n}{1}\alpha + \binom{n}{2}\alpha^2 + \cdots + \binom{n}{n}\alpha^n\\ g_n(\alpha^2) &= \binom{n}{0} + \binom{n}{1}\alpha^2 + \binom{n}{2}\alpha^4 + \cdots + \binom{n}{n}\alpha^{2n}.\end{aligned}$$

Since $\alpha^3 = 1$ we can rewrite the second and third expressions as

$$\begin{aligned}g_n(\alpha) &= \binom{n}{0} + \binom{n}{1}\alpha + \binom{n}{2}\alpha^2 + \binom{n}{3} + \binom{n}{4}\alpha + \binom{n}{5}\alpha^2 + \binom{n}{6} + \cdots\\ g_n(\alpha^2) &= \binom{n}{0} + \binom{n}{1}\alpha^2 + \binom{n}{2}\alpha + \binom{n}{3} + \binom{n}{4}\alpha^2 + \binom{n}{5}\alpha + \binom{n}{6} + \cdots.\end{aligned}$$

It is tempting to just take the sum of these two expressions. This would give every third term a coefficient of 2, and every other term a coefficient of $\alpha^2 + \alpha = -1$. A promising development! After all, we want a sum of binomial coefficients where every third term is different from the other two. However, if we simply sum $g_n(\alpha)$ and $g_n(\alpha^2)$, the (approximately) one-third of terms that are different from the rest are in the wrong spot! To remedy this, let's shift where the α and α^2 appear by multiplying each equation by an appropriate power of α. We have

$$\begin{aligned}\alpha g_n(\alpha) &= \binom{n}{0}\alpha + \binom{n}{1}\alpha^2 + \binom{n}{2} + \binom{n}{3}\alpha + \binom{n}{4}\alpha^2 + \binom{n}{5} + \binom{n}{6}\alpha + \cdots\\ \alpha^2 g_n(\alpha^2) &= \binom{n}{0}\alpha^2 + \binom{n}{1}\alpha + \binom{n}{2} + \binom{n}{3}\alpha^2 + \binom{n}{4}\alpha + \binom{n}{5} + \binom{n}{6}\alpha^2 + \cdots.\end{aligned}$$

Much better! Taking the sum we get

$$\begin{aligned}\alpha g_n(\alpha) + \alpha^2 g_n(\alpha^2) &= \binom{n}{0}(\alpha + \alpha^2) + \binom{n}{1}(\alpha^2 + \alpha) + 2\binom{n}{2}\\ &\quad + \binom{n}{3}(\alpha + \alpha^2) + \binom{n}{4}(\alpha^2 + \alpha) + 2\binom{n}{5} + \cdots\\ &= -\binom{n}{0} - \binom{n}{1} + 2\binom{n}{2} - \binom{n}{3} - \binom{n}{4} + 2\binom{n}{5} + \cdots.\end{aligned}$$

Adding $g_n(1)$ to this gives

$$g_n(1) + \alpha g_n(\alpha) + \alpha^2 g_n(\alpha^2) = 3\binom{n}{2} + 3\binom{n}{5} + 3\binom{n}{8} + \cdots .$$

We can now start with $g_n(1)$ and subtract an appropriate multiple of $g_n(1)+\alpha g_n(\alpha)+\alpha^2 g_n(\alpha^2)$ to get what we want.

$$\begin{aligned}
&g_n(1) - \frac{2}{3}\left(g_n(1) + \alpha g_n(\alpha) + \alpha^2 g_n(\alpha^2)\right) \\
&= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} \\
&\qquad - 2\left(\binom{n}{2} + \binom{n}{5} + \binom{n}{8} + \cdots\right) \\
&= \binom{n}{0} + \binom{n}{1} - \binom{n}{2} + \binom{n}{3} + \binom{n}{4} - \binom{n}{5} + \binom{n}{6} + \cdots \\
&= b_0\binom{n}{0} + b_1\binom{n}{1} + \cdots + b_n\binom{n}{n}.
\end{aligned}$$

We can now finally conclude that

$$\begin{aligned}
A &= \frac{1}{3} \\
B &= -\frac{2}{3}\alpha \\
C &= -\frac{2}{3}\alpha^2.
\end{aligned}$$

(b) We have

$$\begin{aligned}
d_n &= \frac{1}{3}g_n(1) - \frac{2}{3}\alpha g_n(\alpha) - \frac{2}{3}\alpha^2 g_n(\alpha^2) \\
&= \frac{1}{3}(2^n) - \frac{2}{3}\alpha(1+\alpha)^n - \frac{2}{3}\alpha^2(1+\alpha^2)^n \qquad \text{since } g_n(x) = (1+x)^n \\
&= \frac{1}{3}(2^n) - \frac{2}{3}\alpha(-\alpha^2)^n - \frac{2}{3}\alpha^2(-\alpha)^n \\
&= \frac{1}{3}\left(2^n + 2\alpha^{2n+1}(-1)^{n+1} + 2\alpha^{2+n}(-1)^{n+1}\right) \\
&= \frac{2}{3}\left(2^{n-1} + (-1)^{n+1}(\alpha^{2n+1} + \alpha^{2+n})\right).
\end{aligned}$$

Let $r_n = (-1)^{n+1}(\alpha^{2n+1}+\alpha^{2+n})$. The behaviour of $(-1)^{n+1}$ depends on the remainder of n when divided by 2. The behaviour of powers of α depends on the remainder of the power when divided by 3. With this in mind, let's analyse the behaviour of r_n for different remainders of n when divided by $2 \times 3 = 6$.

When $n = 6k$ for some integer k we have

$$\begin{aligned}
r_{6k} &= (-1)^{6k+1}(\alpha^{12k+1} + \alpha^{6k+2}) \\
&= -(\alpha + \alpha^2) \\
&= 1.
\end{aligned}$$

When $n = 6k+1$ we have

$$\begin{aligned} r_{6k+1} &= (-1)^{6k+2}(\alpha^{12k+3} + \alpha^{6k+3}) \\ &= 2. \end{aligned}$$

For $n = 6k+2$,

$$\begin{aligned} r_{6k+2} &= (-1)^{6k+3}(\alpha^{12k+5} + \alpha^{6k+4}) \\ &= -(\alpha^2 + \alpha) \\ &= 1. \end{aligned}$$

The remaining cases are given by

$$\begin{aligned} r_{6k+3} &= (-1)^{6k+4}(\alpha^{12k+7} + \alpha^{6k+5}) = \alpha + \alpha^2 = -1 \\ r_{6k+4} &= (-1)^{6k+5}(\alpha^{12k+9} + \alpha^{6k+6}) = -(1+1) = -2 \\ r_{6k+5} &= (-1)^{6k+6}(\alpha^{12k+11} + \alpha^{6k+7}) = \alpha^2 + \alpha = -1. \end{aligned}$$

So, $d_n = \frac{2}{3}(2^{n-1} + r_n)$, where r_n is given by the following table:

n	r_n
$6k$	1
$6k+1$	2
$6k+2$	1
$6k+3$	-1
$6k+4$	-2
$6k+5$	-1

5. Putting all the parts together we have the recursive formula

$$f_{n+1} = 2f_n + \frac{2(n+1)}{3}(2^{n-1} + r_n)$$

where r_n is given by the table above. From 1(a) we know $f_5 = 108$. Applying the recursive formula repeatedly gives

$$\begin{aligned} f_6 &= 2f_5 + \frac{2(6)}{3}(2^4 + r_5) = 2(108) + \frac{2(6)}{3}(2^4 + (-1)) = 276. \\ f_7 &= 2f_6 + \frac{2(7)}{3}(2^5 + r_6) = 2(276) + \frac{2(7)}{3}(2^5 + 1) = 706. \\ f_8 &= 2f_7 + \frac{2(8)}{3}(2^6 + r_7) = 2(706) + \frac{2(8)}{3}(2^6 + 2) = 1\,764. \\ f_9 &= 2f_8 + \frac{2(9)}{3}(2^7 + r_8) = 2(1\,764) + \frac{2(9)}{3}(2^7 + 1) = 4\,302. \\ f_{10} &= 2f_9 + \frac{2(10)}{3}(2^8 + r_9) = 2(4\,302) + \frac{2(10)}{3}(2^8 + (-1)) = 10\,304. \\ f_{11} &= 2f_{10} + \frac{2(11)}{3}(2^9 + r_{10}) = 2(10\,304) + \frac{2(11)}{3}(2^9 + (-2)) = 24\,348. \\ f_{12} &= 2f_{11} + \frac{2(12)}{3}(2^{10} + r_{11}) = 2(24\,348) + \frac{2(12)}{3}(2^{10} + (-1)) = 56\,880. \end{aligned}$$

If you were to compute f_{12} directly from the definition, you would have had to compute the 3-sign sum of 4 096 lists. What we have done in this Problem of the Month is much less work, especially if you wanted to compute something larger like f_{30}. If you were to compute f_{30} directly from the definition, you would need to compute over 1 billion 3-sign sums! That's a lot of sums.

Problem of the Month

Problem 4: A Polynomial Sandwich

January 2025

Let a, b, c, and d be rational numbers and $f(x) = ax^3 + bx^2 + cx + d$. Suppose $f(n)$ is an integer whenever n is an integer and that

$$\frac{1}{3}n^3 - n - \frac{2}{3} \leq f(n) \leq \frac{1}{3}n^3 + n^2 + 2n + \frac{4}{3}$$

for every integer n with the possible exception of $n = -2$.

1. Show that $a = \dfrac{1}{3}$.
2. Find $f(10^{2025}) - f(10^{2025} - 1)$.

Problem of the Month
Problem 4: A Polynomial Sandwich

January 2025

Hint

1. The graphs of the polynomials $y = \frac{1}{3}x^3 - x - \frac{2}{3}$ and $y = \frac{1}{3}x^3 + x^2 + 2x + \frac{4}{3}$ look quite different near the origin. However, since they have the same leading term, they look nearly identical if you zoom out. Try graphing these two cubics on the same axes using graphing software. The function $f(x)$ lies between these two cubic functions (at least on integer inputs), so it should have the same overall "shape". This suggests that $a = \frac{1}{3}$. There are short arguments to justify this using limits, but there are also more elementary approaches. One thing you might try is to subtract $\frac{1}{3}n^3$ from each of the three expressions in the chain of inequalities. If $a \neq \frac{1}{3}$, you will have a cubic that is trapped between two quadratics, which should make you suspicious. Remember, the inequalities hold for all integers, especially really, really, really, really big ones.

2. If you substitute $n = 0$ into the inequality, you should find that $-\frac{2}{3} \leq f(0) \leq \frac{4}{3}$. Since $f(0)$ is an integer, this means either $f(0) = 0$ or $f(0) = 1$. It is possible to find b, c, and d by gathering and using similar information.

Problem of the Month

Solution to Problem 4: A Polynomial Sandwich

January 2025

1. We present two solutions to Problem 1. In both solutions, we will use the so called *triangle inequality*. This frequently useful fact says that if u and v are real numbers, then

$$|u+v| \leq |u| + |v|$$

where $|x|$ represents the absolute value of the real number x. The triangle inequality can be applied twice to get that $|u+v+w| \leq |u|+|v|+|w|$ for any real numbers u, v, and w. If you are unfamiliar with the triangle inequality or even with absolute values, this might be a good time for an internet search!

Solution 1: We will prove the following fact: If $p(x) = Ax^3 + Bx^2 + Cx + D$ with real numbers A, B, C, and D and $A \neq 0$, then there are infinitely many integers n such that $p(n) > 0$ and infinitely many integers m such that $p(m) < 0$.

Then $a = \dfrac{1}{3}$ can be deduced from this fact. To see this, consider the polynomial

$$\begin{aligned} q(x) &= f(x) - \left(\frac{1}{3}x^3 + x^2 + 2x + \frac{4}{3}\right) \\ &= \left(a - \frac{1}{3}\right)x^3 + (b-1)x^2 + (c-2)x + \left(d - \frac{4}{3}\right). \end{aligned}$$

Using the given information, $q(n) \leq 0$ for every integer n with the possible exception of $n = -2$. This means $q(n) > 0$ for at most one integer. By the fact above, if $a - \dfrac{1}{3}$ were different from 0, then there would be infinitely many integers n with $q(n) > 0$. This means we must have $a - \dfrac{1}{3} = 0$.

Interestingly, we have only used one of the two inequalities given in the problem. To understand why we can only use one of the inequalities, you may want to reread the hint for this problem and think about what the inequalities say when n is negative versus when n is positive.

To prove the fact above, set $M = \max\{|B|, |C|, |D|\}$. In particular, this means M is at least as large as each of $|B|, |C|$, and $|D|$.

If $B = C = D = 0$, then $p(n) > 0$ when $n > 0$ and $p(m) < 0$ when $m < 0$ or vice versa, depending on the sign of A. For the rest of the proof, we assume not all of B, C, and D are zero, which means $M > 0$.

For any nonzero integer n, using the triangle inequality and the fact that $1 \leq |n| \leq |n|^2 \leq$

$|n|^3$ we get that

$$\begin{aligned}
|Bn^2 + Cn + D| &\leq |Bn^2| + |Cn| + |D| \\
&= |B||n|^2 + |C||n| + |D| \\
&\leq |B||n|^2 + |C||n|^2 + |D||n|^2 \\
&\leq M|n|^2 + M|n|^2 + M|n|^2 \\
&= 3M|n|^2.
\end{aligned}$$

If u and v are real numbers with v positive, the inequality $|u| \leq v$ is really saying that $-v \leq u \leq v$. Since $3M|n|^2$ is positive, the chain of inequalities above implies that

$$-3M|n|^2 \leq Bn^2 + Cn + D \leq 3M|n|^2.$$

Adding An^3 to this chain of inequalities gives

$$An^3 - 3M|n|^2 \leq p(n) \leq An^3 + 3M|n|^2 \tag{$*$}$$

for all nonzero integers n.

We will use these inequalities to show that as long as $A \neq 0$, there are infinitely many integers n with $p(n) > 0$ and infinitely many integers m with $p(m) < 0$.

First, suppose $A > 0$. In this case, choose any positive integer $n > \dfrac{3M}{A}$. There are infinitely many such n since M and A are constants. Noting that $0 < n^2 = |n|^2$, this implies $n^3 > \dfrac{3M}{A}|n|^2$. Since $A > 0$, we can multiply both sides by A and rearrange to get $0 < An^3 - 3M|n|^2$. Combining with $(*)$, this implies $p(n) > 0$ for any positive integer $n > \dfrac{3M}{A}$.

Now choose any negative integer $m < \dfrac{-3M}{A}$. As in the previous paragraph, $0 < m^2 = |m|^2$, which implies $m^3 < -\dfrac{3M}{A}|m|^2$, which can be rearranged to $Am^3 + 3M|m|^2 < 0$. Combining with $(*)$, gives $p(m) < 0$ for any negative integer $m < \dfrac{-3M}{A}$, and there are infinitely many such m.

In a similar manner we can deal with the case of $A < 0$, proving the fact is true for all $A \neq 0$.

Solution 2: We will assume that $a \neq \dfrac{1}{3}$ and deduce a contradiction. First, assume $a > \dfrac{1}{3}$. By rearranging the inequality

$$an^3 + bn^2 + cn + d \leq \frac{1}{3}n^3 + n^2 + 2n + \frac{4}{3},$$

which holds for all integers except possibly $n = -2$, we get

$$\left(a - \frac{1}{3}\right) n^3 \leq (1-b)n^2 + (2-c)n + \frac{4}{3} - d.$$

Multiplying through by 3 gives

$$(3a-1)n^3 \le 3(1-b)n^2 + 3(2-c)n + 4 - 3d.$$

Dividing through by n^3 gives

$$3a-1 \le \frac{3(1-b)}{n} + \frac{3(2-c)}{n^2} + \frac{(4-3d)}{n^3},$$

but we are only guaranteed that this inequality holds for positive integers n since the original inequality may fail at $n=-2$, and dividing by a negative integer n would have reversed the inequality.

For any real number u, we have $u \le |u|$, which means

$$3a-1 \le \left|\frac{3(1-b)}{n}\right| + \left|\frac{3(2-c)}{n^2}\right| + \left|\frac{(4-3d)}{n^3}\right|.$$

Noting that $\frac{1}{n^2} < \frac{1}{n}$ and $\frac{1}{n^3} < \frac{1}{n}$ for all integers $n > 1$, we get

$$\begin{aligned} 3a-1 &\le \left|\frac{3(1-b)}{n}\right| + \left|\frac{3(2-c)}{n^2}\right| + \left|\frac{(4-3d)}{n^3}\right| \\ &= |3(1-b)|\frac{1}{n} + |3(2-c)|\frac{1}{n^2} + |(4-3d)|\frac{1}{n^3} \\ &< |3(1-b)|\frac{1}{n} + |3(2-c)|\frac{1}{n} + |(4-3d)|\frac{1}{n} \\ &= \frac{1}{n}\left(|3(1-b)| + |3(2-c)| + |(4-3d)|\right) \end{aligned}$$

and so

$$3a-1 < \frac{1}{n}\left(|3(1-b)| + |3(2-c)| + |(4-3d)|\right) \qquad (**)$$

for every integer $n > 1$. Recall that $a > \frac{1}{3}$ which implies $3a-1 > 0$. If $|3(1-b)| + |3(2-c)| + |(4-3d)|$ is equal to 0, then $(**)$ says that something positive is less than 0, which can never happen. Otherwise, the quantity $|3(1-b)|+|3(2-c)|+|(4-3d)|$ is some positive number, which means that by taking n large enough, we can force

$$\frac{1}{n}\left(|3(1-b)| + |3(2-c)| + |(4-3d)|\right) < 3a-1$$

which violates $(**)$ as well. In other words, $(**)$ can only hold for finitely many positive integers n. However, the assumption $a > \frac{1}{3}$ implies that $(**)$ holds for all positive integers. This means it must not be the case that $a > \frac{1}{3}$ so we conclude that $a \le \frac{1}{3}$.

Similarly, if we assume $a < \frac{1}{3}$, we can use the other inequality to derive a contradiction. When doing this, one would need to be careful to take $n < -2$ since the assumed inequality is not guaranteed to hold for $n = -2$.

If you have learned a bit about *limits* in a calculus course, you might want to think about how this relates to the *Squeeze Theorem*. In fact, the Squeeze Theorem can be used to give a very short proof that $a = \frac{1}{3}$.

2. Since
$$\frac{1}{3}n^3 - n - \frac{2}{3} \le f(n) \le \frac{1}{3}n^3 + n^2 + 2n + \frac{4}{3},$$
for all integers (except possibly $n = -2$), this chain of inequalities provides an interval in which $f(n)$ lies for each integer $n \neq -2$. Since $f(n)$ is an integer, this will give a finite number of possible values of $f(n)$. By finding integers n for which there are a small number of possibilities for $f(n)$, we will be able to find a finite list of possibilities for $f(x)$. To help with this, consider the polynomial

$$h(x) = \left(\frac{1}{3}x^3 + x^2 + 2x + \frac{4}{3}\right) - \left(\frac{1}{3}x^3 - x - \frac{2}{3}\right) = x^2 + 3x + 2.$$

For an integer n, $h(n)$ is the length of the interval containing $f(n)$. Integers n where $h(n)$ is small will have a small number of possibilities for the value of $f(n)$.

Notice that $h(x) = (x+1)(x+2)$, so we expect $h(n)$ to be smallest when n is either equal to or near -1 and -2. We are not guaranteed that the inequalities hold for $n = -2$. Therefore, we will substitute $n = -1$, $n = 0$, and $n = -3$.

When $n = -1$,

$$\begin{array}{rcccl} \frac{1}{3}(-1)^3 - (-1) - \frac{2}{3} & \le & f(-1) & \le & \frac{1}{3}(-1)^3 + (-1)^2 + 2(-1) + \frac{4}{3} \\ 0 & \le & f(-1) & \le & 0 \end{array}$$

which means $f(-1) = 0$.

When $n = 0$, we have

$$\begin{array}{rcccl} \frac{1}{3}(0)^3 - (0) - \frac{2}{3} & \le & f(0) & \le & \frac{1}{3}(0)^3 + (0)^2 + 2(0) + \frac{4}{3} \\ -\frac{2}{3} & \le & f(0) & \le & \frac{4}{3} \end{array}$$

and since $f(0)$ is an integer, this means $f(0) = 0$ or $f(0) = 1$.

Finally, with $n = -3$, we get

$$\begin{array}{rcccl} \frac{1}{3}(-3)^3 - (-3) - \frac{2}{3} & \le & f(-3) & \le & \frac{1}{3}(-3)^3 + (-3)^2 + 2(-3) + \frac{4}{3} \\ -\frac{20}{3} & \le & f(-3) & \le & -\frac{14}{3} \end{array}$$

and since $f(-3)$ must be an integer, we get that $f(-3)$ is either -6 or -5.

We can translate this into information about the unknown coefficients, b, c, and d of $f(n)$. From $f(-1) = 0$, we get

$$0 = \frac{1}{3}(-1)^3 + b(-1)^2 + c(-1) + d = -\frac{1}{3} + b - c + d$$

or $b - c + d = \dfrac{1}{3}$.

Substituting $n = 0$, we have that $f(0) = d$, which implies $d = 0$ or $d = 1$.

Since $f(-3) = -5$ or $f(-3) = -6$ and

$$f(-3) = \frac{1}{3}(-3)^3 + b(-3)^2 + c(-3) + d = -9 + 9b - 3c + d.$$

it must be that $9b - 3c + d = 4$ or $9b - 3c + d = 3$. This means b, c, and d satisfy one of the following four systems of equations:

$$\begin{cases} b - c + d = \frac{1}{3} \\ 9b - 3c + d = 3 \\ d = 0 \end{cases} \qquad \begin{cases} b - c + d = \frac{1}{3} \\ 9b - 3c + d = 3 \\ d = 1 \end{cases}$$

$$\begin{cases} b - c + d = \frac{1}{3} \\ 9b - 3c + d = 4 \\ d = 0 \end{cases} \qquad \begin{cases} b - c + d = \frac{1}{3} \\ 9b - 3c + d = 4 \\ d = 1 \end{cases}$$

Consider the system on the top-left. If $d = 0$ is substituted into the first two equations, they simplify to $b - c = \frac{1}{3}$ and $9b - 3c = 3$. Multiplying the first of these resulting equations by 3 gives $3b - 3c = 1$, which can be subtracted from $9b - 3c = 3$ to get $6b = 2$ or $b = \frac{1}{3}$. Since $b - c = \frac{1}{3}$, this means $c = 0$. Therefore, one possibility for the polynomial $f(x)$ is $f(x) = \frac{1}{3}x^3 + \frac{1}{3}x^2$.

The other three systems can be solved in a similar way. This gives a total of four possibilities for $f(x)$ which are listed below in factored form:

$$\begin{aligned} \frac{1}{3}x^3 + \frac{1}{3}x^2 &= \frac{1}{3}x^2(x+1) \\ \frac{1}{3}x^3 + \frac{2}{3}x^2 + \frac{4}{3}x + 1 &= \frac{1}{3}(x+1)(x^2+x+3) \\ \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x &= \frac{1}{6}x(x+1)(2x+1) \\ \frac{1}{3}x^3 + \frac{5}{6}x^2 + \frac{3}{2}x + 1 &= \frac{1}{6}(x+1)(2x^2+3x+6) \end{aligned}$$

When $n = 1$ is substituted into the first, second, and fourth polynomials, the outputs are $\frac{2}{3}$, $\frac{10}{3}$, and $\frac{11}{3}$, respectively. None of these are integers, which means $f(x)$ cannot be any of these three polynomials since $f(n)$ must be an integer when n is an integer. Therefore, the only possibility is that

$$f(x) = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x = \frac{x(x+1)(2x+1)}{6}.$$

We now verify that $f(x)$ has the properties claimed in the question.

To see that $f(n)$ is an integer for every integer n, we will show that $n(n+1)(2n+1)$, the numerator of $f(n)$, must be a multiple of 6. Since n and $n+1$ are consecutive integers, one of them must be even. This means $n(n+1)(2n+1)$ is even. If either n or $n+1$ is a multiple of 3, then $n(n+1)(2n+1)$ is a multiple of 3. If neither n nor $n+1$ is a multiple of 3, then n must be 1 more than a multiple of 3. That is, there is some integer k so that $n = 3k+1$. Then $2n+1 = 2(3k+1)+1 = 6k+3 = 3(2k+1)$, so $2n+1$ is a multiple of 3. This shows that $n(n+1)(2n+1)$ must be a multiple of 3. Therefore,

$$f(n) = \frac{n(n+1)(2n+1)}{6}$$

is an integer for every integer n. You may recognize that $f(n) = 1^2 + 2^2 + 3^2 + \cdots + n^2$, which immediately implies $f(n)$ is an integer.

Next, we will show that $\frac{1}{3}n^3 - n - \frac{2}{3} \leq f(n)$ or

$$\frac{1}{3}n^3 - n - \frac{2}{3} \leq \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

for all integers n with the possible exception of $n = -2$. After rearranging, this inequality is equivalent to

$$0 \leq \frac{1}{2}n^2 + \frac{7}{6}n + \frac{2}{3}.$$

Since 6 is positive, the inequality is also equivalent to

$$0 \leq 6\left(\frac{1}{2}n^2 + \frac{7}{6}n + \frac{2}{3}\right) = 3n^2 + 7n + 4 = (3n+4)(n+1).$$

The polynomial $(3x+4)(x+1)$ is quadratic and has roots $x = -1$ and $x = -\frac{4}{3}$. The leading coefficient is positive, which means it can only take negative values strictly between $-\frac{4}{3}$ and -1. There are no integers in this range, which means $(3n+4)(n+1) \geq 0$ for all integers n. Thus, the original inequality also holds for all integers n including $n = -2$.

Now consider the polynomial $(x+1)(3x+8)$ which has roots $x = -\frac{8}{3}$ and $x = -1$. The only integer n for which $(n+1)(3n+8)$ is negative is $n = -2$ since -2 is the only integer between $-\frac{8}{3}$ and -1. Therefore, for all integers $n \neq -2$, we have

$$0 \leq (n+1)(3n+8)$$

which we expand and divide by 6 to get

$$0 \leq \frac{1}{2}n^2 + \frac{11}{6}n + \frac{4}{3}.$$

After rearranging and adding $\frac{1}{3}n^3$ to both sides, we have that

$$f(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n \leq \frac{1}{3}n^3 + n^2 + 2n + \frac{4}{3}$$

for all integers $n \neq -2$. Combining this with the other inequality, we have now shown that

$$\frac{1}{3}n^3 - n - \frac{2}{3} \leq f(n) \leq \frac{1}{3}n^3 + n^2 + 2n + \frac{4}{3}$$

for all integers $n \neq -2$.

Finally, let's compute $f(10^{2025}) - f(10^{2025} - 1)$. To do this, we will work out $f(n) - f(n-1)$ for general n and substitute $n = 10^{2025}$ into the resulting expression.

$$\begin{aligned} f(n) - f(n-1) &= \frac{n(n+1)(2n+1)}{6} - \frac{(n-1)[(n-1)+1][2(n-1)+1]}{6} \\ &= \frac{n[(n+1)(2n+1) - (n-1)(2n-1)]}{6} \\ &= \frac{n(2n^2 + n + 2n + 1 - 2n^2 + n + 2n - 1)}{6} \\ &= \frac{n(6n)}{6} \\ &= n^2 \end{aligned}$$

Therefore, $f(10^{2025}) - f(10^{2025} - 1) = (10^{2025})^2 = 10^{4050}$. As mentioned earlier, the polynomial $f(x)$ has the special property that $f(n) = 1^2 + 2^2 + 3^2 + \cdots + n^2$ for every $n \geq 1$. It follows from this property that $f(n) - f(n-1) = n^2$.

Notice that we used the fact that $n \neq -2$ to prove the inequality $f(n) \leq \frac{1}{3}n^3 + n^2 + 2n + \frac{4}{3}$. It is worth thinking about what happens at $n = -2$, and seeing if you can figure out why we had to exclude $n = -2$.

Problem of the Month

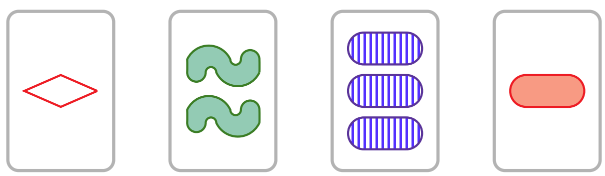
Problem 5: SET!

February 2025

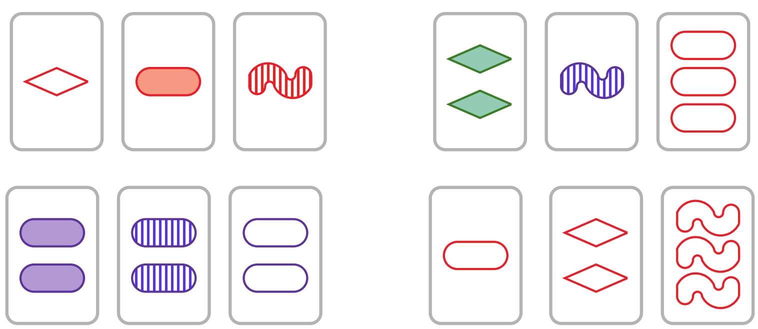
This month's problem is about the card game SET!. Each card in the game SET! has four properties, and each property has three options as follows:

- **Number**: 1, 2, or 3.
- **Colour**: Red, green, or purple.
- **Shading**: Solid, striped, or open.
- **Shape**: Squiggle, diamond, or oval.

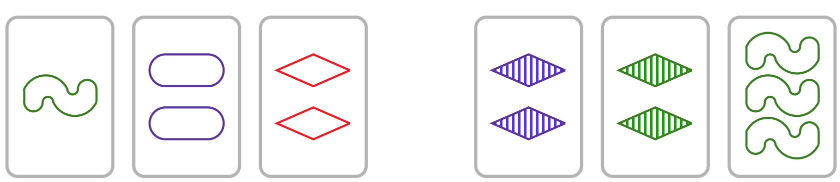
For example, below are some cards from a SET! deck. From left to right we have a card with 1 red open diamond, a card with 2 green solid squiggles, a card with 3 purple striped ovals, and a card with 1 red solid oval.



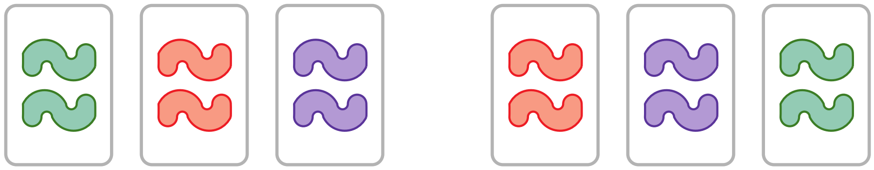
A *set* is a group of three cards such that for each of the four properties, all three cards have the same option, or all three cards have different options. For example, the following four collections of three cards are sets:



However, the following two collections of three cards are not sets:

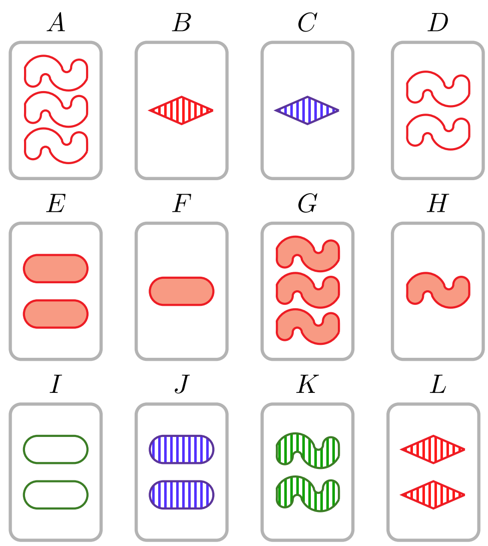


The order of the cards doesn't matter, so the two collections of three cards



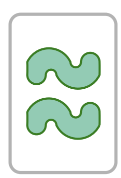
are considered to be the same set. Note that the same card could appear in two distinct sets.

1. Find six distinct sets in the following collection of twelve cards:



2. A SET! deck consists of exactly one of every possible card. How many cards are in a SET! deck?

3. How many distinct sets contain the following card?



4. How many different sets exist in a SET! deck?

5. In a game of SET!, first, a full deck is shuffled. Then twelve cards are dealt on the table, and the players try to find sets. If a player finds a set, they shout "set", and pick up the three cards that form the set. Those three cards are removed from the game (to be counted at the end), and three more cards from the deck are dealt to replace them. The game continues until all the cards from the deck are dealt and there are no more sets among the cards remaining on the table.

   Suppose that during a game of SET!, there are three cards remaining on the table. That is, every card in the deck besides the three on the table has been collected as part of a set. Show that the remaining three cards must form a set.

Problem of the Month
Problem 5: SET!

February 2025

Hint

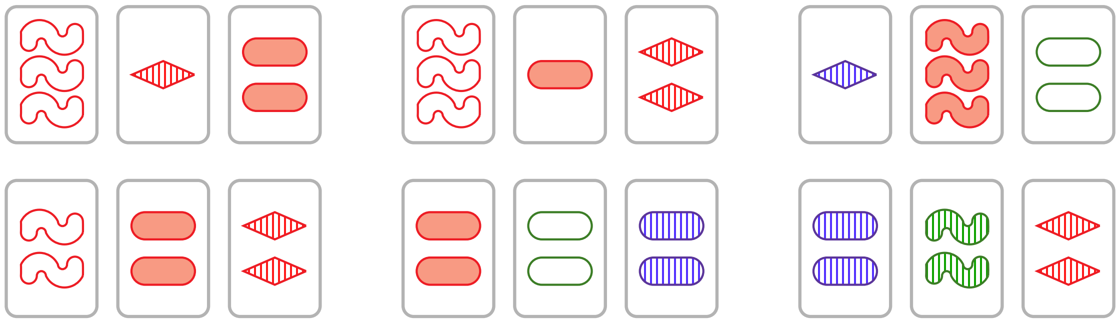
1. Three of the six sets consist entirely of red cards.
2. First count the red cards with solid squiggles. Then count all the red cards with squiggles. Then count all the red cards.
3. Choose any two SET! cards. How many other cards go with those two to form a set?
4. See the previous hint.
5. Try encoding the cards as 4-tuples (p, q, r, s), where each coordinate represents a property, and each entry in each coordinate can be either 1, 2, or 3 corresponding to the three different options for each property. Can you identify when three 4-tuples correspond to cards that form a set?

Problem of the Month

Solution to Problem 5: SET!

February 2025

1. The six sets are:



   Going by the labels in the statement of the problem, the six sets are

$$\{A, B, E\}, \{A, F, L\}, \{C, G, I\}, \{D, E, L\}, \{E, I, J\}, \{J, K, L\}.$$

2. Since each property has three options, and there are four properties, there are

$$3 \times 3 \times 3 \times 3 = 81$$

   cards in a SET! deck.

For the next two questions, we first make the following observation: Given any two cards A and B, there is a unique third card C so that the three cards A, B, and C form a set. Let's see why this is true.

For each property, if the options on A and B are the same, then the option for that property on card C must also be the same as it is for A and B. If the options are not the same for A and B, then C must have the third option for that property.

For example, if A and B are both shaded solid, then C must be shaded solid. On the other hand, if the shading of A is striped and the shading of B is solid, then the shading of C must be open.

3. With the observation above in mind, to create a set that contains the given card, we just have to choose any other card. Then the given card with our choice of second card uniquely determines a third card that forms a set.

   There are 80 choices for a second card. However this counts every set twice! To see why, call the card we are given in the question A. Suppose we choose a card B, and the unique third card that forms a set is C. If instead we choose C as the second card, then B is the unique card that forms a set with A and C. So choosing B as the second card results in the same set as choosing C as the second card.

   Therefore the answer is $\frac{80}{2} = 40$.

4. **Solution 1:** We again rely on the observation above that once we have chosen two cards as part of a set, the third is determined.

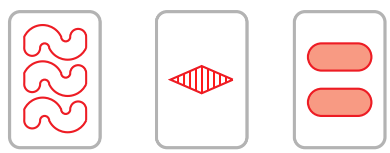
   There are 81 ways to choose the first card in our set, and 80 ways to choose the second. However, since there are $3! = 6$ ways to order the three cards in a set, the number 81×80 counts each set six times. Therefore the number of different sets in a SET! deck is $\frac{81\times 80}{6} = 1080$.

   Solution 2: Using Question 3, we know each card appears in 40 sets. Since there are 81 cards in a full deck, and 3 cards in a set, there are $\frac{40\times 81}{3} = 1080$ sets in a SET! deck.

5. For this question, we will need to introduce a different way of thinking about the cards. We can encode each card by a 4-tuple (q, r, s, t), where each entry q, r, s, t is either 1, 2, or 3 as in the following table:

Entry in the 4-tuple	Number	Shading	Colour	Shape
1	1	open	red	diamond
2	2	striped	green	oval
3	3	solid	purple	squiggle

   For example, consider the cards from one of the sets from Problem 1 above:



   These cards are encoded by the tuples $(3, 1, 1, 3)$, $(1, 2, 1, 1)$, and $(2, 3, 1, 2)$ respectively.

   Let's think about what it takes for three 4-tuples to form a set. Each coordinate in the tuple (ie, the first, second, third, or fourth entry) corresponds to one of the properties (number, shading, colour, and shape, in that order).

   The condition that a property has the same option across the three cards translates to the entry in the corresponding coordinate being the same across all three 4-tuples. In the example above, all three cards are red. Therefore, the entries in the third coordinates of all three 4-tuples are 1.

   The condition that a property has all different options across the three cards translates to each of 1, 2, and 3 appearing in the corresponding coordinate in the three 4-tuples. In the example above, all three cards have different shadings. Therefore, the entries 1, 2, and 3 appear in some order in the second coordinates of the three 4-tuples.

   Our goal now is to characterise exactly when a collection of three numbers $\{a, b, c\}$ is either $\{1, 1, 1\}$, $\{2, 2, 2\}$, $\{3, 3, 3\}$, or $\{1, 2, 3\}$. Note that in the last case, a, b, c must be equal to $1, 2, 3$ in some order (not necessarily $a = 1$, $b = 2$, and $c = 3$).

   Claim: Suppose a, b, c are three integers, each of which is either 1, 2, or 3. Then $a+b+c$ is a multiple of three exactly when either $a = b = c$ or a, b, and c are all distinct.

   Let's justify this claim. First, if $a = b = c$ then $a + b + c$ is equal to 3, 6, or 9. If a, b, and c are distinct, then a, b, and c are 1, 2, and 3 in some order. Therefore,

$a+b+c = 1+2+3 = 6$. Now suppose it is not true that all three of a, b, and c are equal or distinct. That means two of the numbers are equal, and one is not. We can check the sum $a+b+c$ in each of these cases.

$$\begin{aligned}
1+1+2 &= 4\\
1+1+3 &= 5\\
2+2+1 &= 5\\
2+2+3 &= 7\\
3+3+1 &= 7\\
3+3+2 &= 8.
\end{aligned}$$

In all of these cases, the sum $a+b+c$ is not a multiple of 3, so the claim is true!

Great! Let's harness this by adding up coordinates among tuples to check whether or not three 4-tuples come from cards that form a set.

To make our lives a little easier, given two 4-tuples, let's add them together to create another 4-tuple by simply adding up the coordinates. More precisely, given two 4-tuples $\mathbf{v} = (a, b, c, d)$ and $\mathbf{w} = (p, q, r, s)$, we define

$$\mathbf{v} + \mathbf{w} = (a+p, b+q, c+r, d+s).$$

If you have experience with vectors, you may recognise that this is exactly how we add two vectors together. Using this definition of addition for 4-tuples, we can repeatedly add as many 4-tuples together as we like!

In particular, given three 4-tuples we can add them together to get another 4-tuple. The resulting 4-tuple may include entries other than 1, 2, and 3, but that's okay! By using the claim above, we know that the three 4-tuples correspond to three cards that form a set exactly when the 4-tuple resulting from adding them together has the property that every entry is a multiple of 3. Check for yourself that this works for the example set at the beginning of the solution to Problem 5.

More precisely, suppose $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{u}$ are three 4-tuples corresponding to SET! cards. Then $\mathbf{v}+\mathbf{w}+\mathbf{u}$ has every coordinate a multiple of 3 exactly when the cards corresponding to $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{u}$ form a set. Choose your favourite set, and your favourite non-set, and check this for yourself!

We are now ready to attack the original question. First convert the 81 cards in a SET! deck into 4-tuples. For each coordinate, the integers 1, 2, and 3 appear exactly 27 times each (this is because once the entry in a coordinate has been fixed, there are three different options for each of the remaining three coordinates, and $3\times3\times3 = 27$). Therefore, for each coordinate, the sum over all 81 entries in that coordinate is $27\times1+27\times2+27\times3 = 162$, which is a multiple of 3.

Considering the question at hand, we have collected 26 sets from a full SET! deck. We want to show that the remaining three cards also form a set. Let $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$ be the three 4-tuples corresponding to the remaining three cards. For the 78 cards used in the 26 sets, label the 78 4-tuples $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{78}$ so that for every positive integer $k \leq 26$, $\mathbf{v}_{3k-2}, \mathbf{v}_{3k-1}$, and $\mathbf{v}_{3k}$ form a set (ie, $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ form a set, $\mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6$ form a set and so on).

Then we know that for every positive integer $k \leq 26$, $\mathbf{v}_{3k-2}+\mathbf{v}_{3k-1}+\mathbf{v}_{3k}$ is a 4-tuple where every coordinate is a multiple of 3. Summing up all of the resulting 4-tuples gives us that

$$\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_{78} = (a, b, c, d)$$

where a, b, c, d are all multiples of 3. We also know

$$\mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_{78} + \mathbf{w}_1 + \mathbf{w}_2 + \mathbf{w}_3 = (162, 162, 162, 162).$$

We can now conclude that

$$\mathbf{w}_1 + \mathbf{w}_2 + \mathbf{w}_3 = (162 - a, 162 - b, 162 - c, 162 - d).$$

All of 162, a, b, c, and d are all multiples of 3. Therefore, $162 - a$, $162 - b$, $162 - c$, and $162 - d$ are multiples of 3. We can finally conclude that $\mathbf{w}_1, \mathbf{w}_2$, and $\mathbf{w}_3$ are 4-tuples corresponding to three cards that form a set.

Problem of the Month

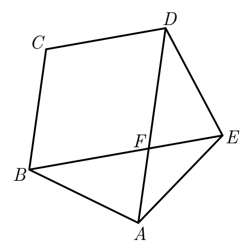
Problem 6: Regular Polygons and Lattice Points

March 2025

A *lattice point* in the Cartesian plane is a point (a, b) with the property that both a and b are integers. In this Problem of the Month, we will investigate regular polygons that have every vertex lying on a lattice point.

1. Let A and B be distinct lattice points on the Cartesian plane, neither of which have coordinates $(0, 0)$. Show that the measure of $\angle AOB$ cannot equal $60°$, where O has coordinates $(0, 0)$.

2. Consider a regular pentagon $ABCDE$. Let F be the point of intersection of lines AD and BE.

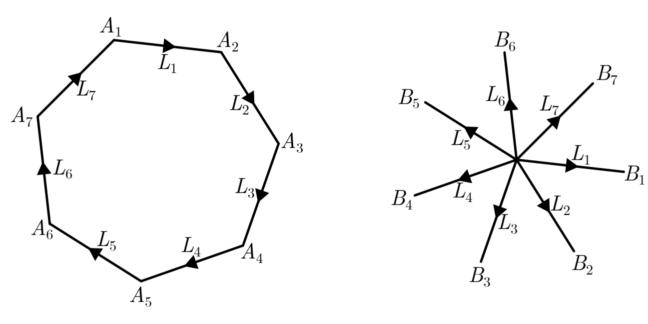


   (a) Show that the quadrilateral $FBCD$ is a parallelogram.

   (b) Show that if B, C, and D are lattice points then so is F.

3. View a regular n-gon as a collection of n line segments. Give each line segment a direction (indicated by an arrow), moving in a clockwise direction (see the image below). Label the line segments $L_1, L_2, \ldots, L_n$. For each i, label the starting point of L_i by A_i. Note that the points $A_1, A_2, \ldots, A_n$ are the vertices of the n-gon.

   Now, translate the line segments (without any rotation) so that the points A_i all coincide. For each L_i, label its new endpoint by B_i. Below is an image of this process when $n = 7$.



   (a) Show that the polygon $B_1B_2 \cdots B_n$ is a regular n-gon.

   (b) Let y be the length of L_1 and x be the length of the line segment B_1B_2. Compute $\frac{x}{y}$ in terms of n.

4. We call a polygon that has every vertex lying on a lattice point a *lattice polygon*. Show that if a regular n-gon is a lattice polygon, then $n = 4$.

Problem of the Month

Problem 6: Regular Polygons and Lattice Points

March 2025

Hint

1. Choose some lattice points A and B and compute $\tan(\angle AOB)$. The values of $\tan(\angle AOB)$ are limited to some subset of the real numbers. Can you figure out what this subset is, and can you prove that $\tan(60^\circ)$ is not in that subset?

2. (a) Compute the interior angle of a regular pentagon. Then compute $\angle CBF$. Is there a theorem from geometry you can use to prove that two lines are parallel?

   (b) Suppose X and Y are points with coordinates (x_1, x_2) and (y_1, y_2). Let Z be the point with coordinates $(x_1 + y_1, x_2 + y_2)$. Plot the four points O, X, Y, Z on the Cartesian plane. Is there anything special about the quadrilateral with vertices O, X, Y, Z? Try it with some specific points X and Y.

3. (a) Start by computing the angle between L_1 and L_2.

   (b) Let A be the center of the n-gon $B_1B_2 \cdots B_n$ (that is, A is the point where all the lines L_i meet in the second image in the statement of the problem). Then $\triangle AB_1B_2$ is an isosceles triangle with one of its side lengths equal to x, and another one equal to y.

4. Use Question 1 to rule out the existence of regular lattice triangles and hexagons. Use Question 2 to rule out the existence of regular lattice pentagons. Use Question 3 to rule out the existence of regular lattice n-gons where $n \geq 7$.

   As a general strategy, assume that there is a regular lattice n-gon, and try to construct a smaller regular lattice n-gon. If you can do this once, then you can do it again and again. Is it a problem to have smaller and smaller lattice polygons? Is this even possible?

Problem of the Month

Solution to Problem 6: Regular Polygons and Lattice Points

March 2025

1. Let A and B have coordinates (a, b) and (c, d) respectively. Let α and β be the angles from the positive x-axis to the lines OA and OB respectively, measured in the clockwise direction. For example, if A has coordinates $(1, 1)$ and B has coordinates $(-1, -1)$, $\alpha = 45°$ and $\beta = 215°$.

   Assume towards a contradiction, that a, b, c, and d are integers and $\angle AOB$ is $60°$.

   Case 1, $a \neq 0$ and $c \neq 0$: Since $0 \leq \alpha, \beta < 360°$, then $\beta - \alpha = \pm 60°$ or $\pm 300°$. Therefore, $\tan(\beta - \alpha) = \pm\tan(60°) = \pm\sqrt{3}$. We have $\tan(\alpha) = \frac{b}{a}$ and $\tan(\beta) = \frac{d}{c}$. By the angle sum formula for tan,

   $$\begin{aligned}\tan(\beta - \alpha) &= \frac{\tan(\beta) - \tan(\alpha)}{1 + \tan(\alpha)\tan(\beta)} \\ &= \frac{\frac{d}{c} - \frac{b}{a}}{1 + \left(\frac{b}{a}\right)\left(\frac{d}{c}\right)}.\end{aligned}$$

   Since a, b, c, and d are integers with $a \neq 0$ and $c \neq 0$, $\tan(\beta - \alpha)$ is rational. However, $\sqrt{3}$ is well known to be irrational, which gives us a contradiction. We can now conclude that if A and B are lattice points, then $\angle AOB$ is not $60°$.

   Case 2, $a = 0$ or $c = 0$: In this case, at least one of A or B is on the y-axis. Note that if A is on the y-axis, then B cannot be on the x- or y- axis (since $\angle AOB$ is not $0°$, $90°$, or $180°$). Similarly, if B is on the y-axis, then A cannot be on the x- or y-axis. So actually, exactly one of A or B is on the y-axis, and the other is not on the x-axis.

   Let A' and B' be the result of rotating A and B $90°$ clockwise about the origin. Now exactly one of A' and B' are on the x-axis, and the other is not on the y-axis. Furthermore, $\angle AOB = \angle A'OB'$. We are now back in Case 1 above but with the points A' and B', and can conclude $\angle AOB$ cannot be $60°$.

2. (a) The interior angle of a regular n-gon is $180° - \frac{360°}{n}$, and so $\angle BCD = \angle BAE = 108°$. Since $\triangle EAB$ is isosceles, $\angle ABE = 36°$. Therefore, $\angle CBF = 72°$. Since

   $$180° = 72° + 108° = \angle CBF + \angle BCD,$$

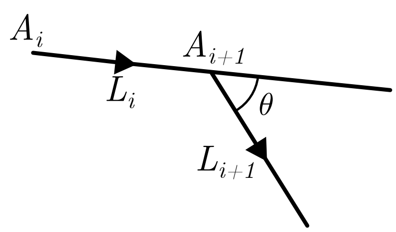
   we have that CD is parallel to BF. We can similarly argue that BC and DF are parallel, and conclude that quadrilateral $FBCD$ is a parallelogram.

   (b) Suppose B, C, and D have coordinates (b_1, b_2), (c_1, c_2), and (d_1, d_2) respectively. Since quadrilateral $FBCD$ is a parallelogram, the difference between the x-coordinates of D and C is equal to the difference between the x-coordinates of F and B. The same holds for the y-coordinates. Therefore, F has coordinates $(b_1 + d_1 - c_1, b_2 + d_2 - c_2)$. We are assuming that B, C, and D are lattice points, so b_1, b_2, c_1, c_2, d_1, and d_2 are all integers. Therefore, the coordinates of F are integers and F is a lattice point.

If you are familiar with vectors, we can rephrase the above argument in terms of vector addition. Since $FBCD$ is a parallelogram, we know $\overrightarrow{CD} + \overrightarrow{CB} = \overrightarrow{CF}$. Therefore, $\vec{D} - \vec{C} + \vec{B} - \vec{C} = \vec{F} - \vec{C}$. This implies $\vec{F} = \vec{D} + \vec{B} - \vec{C}$. Since B, C, and D are lattice points, the corresponding vectors $\vec{B}$, $\vec{C}$, and $\vec{D}$ have integer coordinates. Since $\vec{F}$ is the sum of three vectors with integer coordinates, $\vec{F}$ also has integer coordinates and we can conclude that F is a lattice point.

3. (a) We begin by showing that the angle between L_i and L_{i+1} is $\frac{360°}{n}$ for all i such that $1 \leq i \leq n-1$. The same argument shows that the angle between L_n and L_1 is also $\frac{360°}{n}$.

Let θ be the angle between L_i and L_{i+1}. Then, on the original regular n-gon, we can compute θ by extending the end of L_i past the beginning of L_{i+1} as in the diagram below.



Since the interior angle of a regular n-gon is $180° - \frac{360°}{n}$, we must have

$$\theta = 180° - (180° - \frac{360°}{n}) = \frac{360°}{n}.$$

Let A be the center of $B_1B_2 \cdots B_n$. Then

$$\frac{360°}{n} = \angle B_1AB_2 = \angle B_2AB_3 = \cdots = \angle B_{n-1}AB_n = \angle B_nAB_1.$$

Since each line segment AB_i is the side length of the original regular n-gon, the n triangles $\triangle B_1AB_2, \triangle B_2AB_3, \ldots, \triangle B_{n-1}AB_n$, and $\triangle B_nAB_1$ are all congruent.

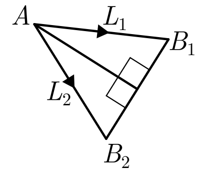
Therefore, the edges of the polygon $B_1B_2, B_2B_3, \ldots, B_{n-1}B_n$, and B_nB_1 all have equal length.

Consider $\triangle B_1AB_2$. Since AB_1 and AB_2 have the same length, it is an isosceles triangle. Since $\angle B_1AB_2 = \frac{360°}{n}$, we have $\angle AB_1B_2 = \angle AB_2B_1 = 90° - \frac{180°}{n}$. By the congruence $\triangle B_1AB_2$ and $\triangle B_2AB_3$, we have $\angle AB_2B_3 = \angle AB_3B_2 = 90° - \frac{180°}{n}$. We can finally compute

$$\angle B_1B_2B_3 = \angle B_1B_2A + \angle AB_2B_3 = 90° - \frac{180°}{n} + 90° - \frac{180°}{n} = 180° - \frac{360°}{n}.$$

We can compute every interior angle of the n-gon $B_1B_2 \cdots B_n$ in the same way to get that all interior angles are equal to $180° - \frac{360°}{n}$. Therefore, $B_1B_2 \cdots B_n$ is a regular n-gon.

(b) As in the previous solution, let A be the center of the regular n-gon $B_1B_2 \cdots B_n$, and consider the isosceles triangle $\triangle B_1AB_2$.



Recall from part (a) that $\angle B_1AB_2 = \frac{360°}{n}$. By drawing a line from the midpoint of B_1B_2 to A, we divide $\triangle B_1AB_2$ into two congruent right-angled triangles. Considering one of these right-angled triangles gives

$$\sin\left(\frac{180°}{n}\right) = \frac{x}{2y}.$$

Therefore,

$$\frac{x}{y} = 2\sin\left(\frac{180°}{n}\right).$$

4. **Case 1, $n = 3$ and $n = 6$:**

Question 1 tells us that there are no equilateral lattice triangles. In fact, we can also rule out the existence of a regular lattice n-gon where n is a multiple of three. To see this, label the vertices $V_1, \ldots, V_{3n}$ in a clockwise order. Then $\angle V_nV_{2n}V_{3n} = 60°$. Therefore, all three of V_n, V_{2n}, and V_{3n} cannot be lattice points.

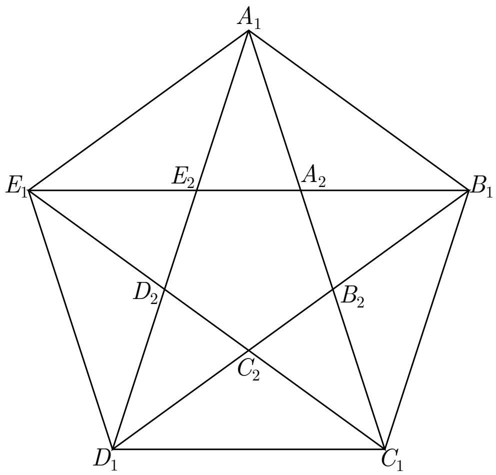
Case 2, $n = 5$:

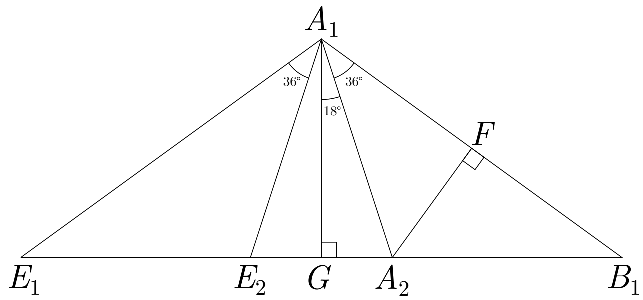
Next we will show that there are no regular lattice pentagons. We will approach this by showing that if there is a regular lattice pentagon, then we can create a smaller regular lattice pentagon. Then we can do it again, and create an even smaller regular lattice pentagon. We can continue to create smaller and smaller lattice pentagons, until we have a lattice pentagon with side length less than 1, so it cannot be a lattice pentagon! The only way to resolve this contradiction is to conclude that the original pentagon does not exist! Let's execute this plan.

Consider a regular pentagon $A_1B_1C_1D_1E_1$. Create a smaller regular pentagon by drawing all five diagonals of the pentagon, and taking the five intersections to be the vertices of our smaller pentagon (see the diagram below). More precisely,

- the lines E_1B_1 and A_1C_1 intersect at A_2,
- the lines A_1C_1 and B_1D_1 intersect at B_2,
- the lines B_1D_1 and C_1E_1 intersect at C_2,
- the lines C_1E_1 and D_1A_1 intersect at D_2, and
- the lines D_1A_1 and E_1B_1 intersect at E_2.

Then $A_2B_2C_2D_2E_2$ is a regular pentagon (see if you can prove this!). Suppose the side length of pentagon $A_1B_1C_1D_1E_1$ is l_1, and the side length of $A_2B_2C_2D_2E_2$ is l_2. The goal now is to write down an expression for l_2 in terms of l_1.





By the solution to Question 2, $\angle E_1A_1E_2 = \angle B_1A_1A_2 = 36°$. Since the interior angle of a regular pentagon is 108°, we have $\angle E_2A_1A_2 = 108° - 36° - 36° = 36°$.

As in the image above, let G be a point on E_2A_2 so that GA_1 is perpendicular to E_2A_2. Let F be the point on A_1B_1 so that FA_2 is perpendicular to A_1B_1. Then G and F are the midpoints of E_2A_2 and A_1B_1 respectively (this fact needs proof, but I will leave it up to you!).

There are now two right-angled triangles, $\triangle A_1FA_2$ and $\triangle A_1GA_2$. Consider the former triangle. Note that the length of A_1F is $\frac{1}{2}l_1$ and $\angle A_2A_1F = 36°$. Let x be the length of A_1A_2. Then

$$\frac{l_1}{2x} = \cos(36°).$$

Now consider right-angled triangle $\triangle A_1GA_2$. We have $\angle GA_1A_2 = 18°$, and the length of GA_2 is $\frac{1}{2}l_2$. Therefore,

$$\sin(18°) = \frac{l_2}{2x}.$$

Solving for x in both of these equations and rearranging gives

$$l_2 = l_1\frac{\sin(18°)}{\cos(36°)}.$$

At the end of this solution, there is an extra section which shows how to deduce that $\sin(18°) = \frac{\sqrt{5}-1}{4}$ and $\cos(36°) = \frac{\sqrt{5}+1}{4}$. Using these exact values we have

$$l_2 = \frac{\sqrt{5}-1}{\sqrt{5}+1}l_1 = \frac{3-\sqrt{5}}{2}l_1.$$

Note that $2 < \sqrt{5} < 3$ and so $0 < \frac{3-\sqrt{5}}{2} < 1$.

Great, we can now repeat this process of creating smaller and smaller pentagons, and we can compute the side length of each one as follows.

Let k be a positive integer, and suppose $A_kB_kC_kD_kE_k$ is a regular pentagon with side length l_k. Create the pentagon $A_{k+1}B_{k+1}C_{k+1}D_{k+1}E_{k+1}$ as above by declaring that

- the lines E_kB_k and A_kC_k intersect at A_{k+1},
- the lines A_kC_k and B_kD_k intersect at B_{k+1},

- the lines B_kD_k and C_kE_k intersect at C_{k+1},
- the lines C_kE_k and D_kA_k intersect at D_{k+1}, and
- the lines D_kA_k and E_kB_k intersect at E_{k+1}.

Then $A_{k+1}B_{k+1}C_{k+1}D_{k+1}E_{k+1}$ is a regular pentagon with side length l_{k+1} where

$$l_{k+1} = \frac{3-\sqrt{5}}{2} l_k.$$

Repeatedly applying the equation $l_{k+1} = \frac{3-\sqrt{5}}{2} l_k$ we have that for any positive integer k,

$$l_k = \left(\frac{3-\sqrt{5}}{2}\right)^{k-1} l_1.$$

We will now prove that there is some k large enough so that $l_k < 1$. Choose a positive integer k so that

$$k > \frac{-\log(l_1)}{\log(3-\sqrt{5}) - \log(2)} + 1.$$

Here we don't care what the base is for the logs, so we will be lazy and not write anything down as the base. After rearranging the inequality a little, and applying some log laws we have

$$k - 1 > \frac{\log\left(\frac{1}{l_1}\right)}{\log\left(\frac{3-\sqrt{5}}{2}\right)}.$$

Since $\frac{3-\sqrt{5}}{2} < 1$, $\log\left(\frac{3-\sqrt{5}}{2}\right) < 0$. Therefore,

$$\begin{aligned}
(k-1)\log\left(\frac{3-\sqrt{5}}{2}\right) &< \log\left(\frac{1}{l_1}\right) \\
\Rightarrow \quad \left(\frac{3-\sqrt{5}}{2}\right)^{k-1} &< \frac{1}{l_1} \\
\Rightarrow \quad l_1\left(\frac{3-\sqrt{5}}{2}\right)^{k-1} &< 1 \\
\Rightarrow \quad l_k &< 1.
\end{aligned}$$

Great! Let's put everything together. Suppose $A_1B_1C_1D_1E_1$ is a regular lattice pentagon with length l_1. Then by Question 2(b), the regular pentagon $A_kB_kC_kD_kE_k$ is a lattice pentagon for all positive integers k. However, when

$$k > \frac{-\log(l_1)}{\log(3-\sqrt{5}) - \log(2)} + 1$$

we have shown that the side length l_k of $A_kB_kC_kD_kE_k$ satisfies $l_k < 1$. Since the smallest distance between two lattice points in the plane is 1, $A_kB_kC_kD_kE_k$ cannot be a lattice pentagon, which is a contradiction! Therefore, a regular pentagon cannot be a lattice pentagon.

Case 3, $n \geq 7$:
The general strategy for this case will be the same as in the case $n = 5$. The difference here will be our construction of successive smaller regular polygons.

Let P_1 be a regular n-gon with side length l_1. Let P_k be the regular n-gon obtained from P_1 by applying k times the process from Question 3. Let P_k have side length l_k. Then from the solution to 3(b) above we have

$$l_k = l_1 \left(2 \sin\left(\frac{180°}{n}\right)\right)^k.$$

Between 0° and 90°, the sine function is strictly increasing. Therefore, for $n \geq 7$ we have

$$0 < 2\sin\left(\frac{180°}{n}\right) < 2\sin\left(\frac{180°}{6}\right) = 1.$$

As in the $n = 5$ case, we want to show that if we choose k to be big enough, $l_k < 1$. To that end, let $a = 2\sin\left(\frac{180°}{n}\right)$ and choose a positive integer k so that

$$k > \frac{-\log(l_1)}{\log(a)}.$$

Then again, since $0 < a < 1$, $\log(a) < 0$ and we have

$$\begin{aligned} k\log(a) &< \log\left(\frac{1}{l_1}\right) \\ \Rightarrow \qquad a^k &< \frac{1}{l_1} \\ \Rightarrow \qquad l_1 a^k &< 1 \\ \Rightarrow \qquad l_k &< 1. \end{aligned}$$

It remains to show that if P_k is a lattice polygon, then so is P_{k+1}. Let P_k be the lattice polygon $A_1 A_2 \cdots A_n$, where A_i has coordinates (a_i, b_i). Now, translate the polygon P_{k+1} so that its center is at the origin O, with coordinates $(0, 0)$. Let P_{k+1} be the polygon $B_1 B_2 \cdots B_n$. Then for each $i < n$, B_i has coordinates $(a_{i+1} - a_i, b_{i+1} - b_i)$, and B_n has coordinates $(a_1 - a_n, b_1 - b_n)$. Since each of the a_i and b_i are integers, we have that each of the B_i is a lattice point and P_{k+1} is a lattice polygon.

Great, now we can put everything together. Suppose P_1 is a regular lattice n-gon with side length l_1. Then for each positive integer k, we can create another regular lattice n-gon with side length $l_k = l_1 a^k$, where $a = 2\sin\left(\frac{180°}{n}\right)$. If $k > \frac{-\log(l_1)}{\log(a)}$, then $l_k < 1$, contradicting the fact that P_k is a lattice polygon.

Therefore, we can conclude that for $n \geq 7$, there is no regular lattice n-gon.

Through the cases we have ruled out the existence of a regular lattice n-gon for all $n \geq 3$ except for $n = 4$. Of course, there are plenty of lattice squares!

There are a couple of things worth discussing about the solutions above.

1. With a little bit of love and care, the solution to Question 1 can be massaged to show that if A, B, and C are distinct lattice points, and if $\theta = \angle ABC$, then $\tan(\theta)$ is a rational

number. There is a theorem called *Niven's Theorem* which says the following:

Niven's Theorem: *Let* $\theta = (180^\circ)\left(\frac{a}{b}\right)$, *where* a *and* b *are integers. If* $\tan(\theta)$ *is rational, then* $\frac{a}{b}$ *is an integer or* $\frac{a}{b} = \frac{2k+1}{4}$ *where* k *is an integer.*

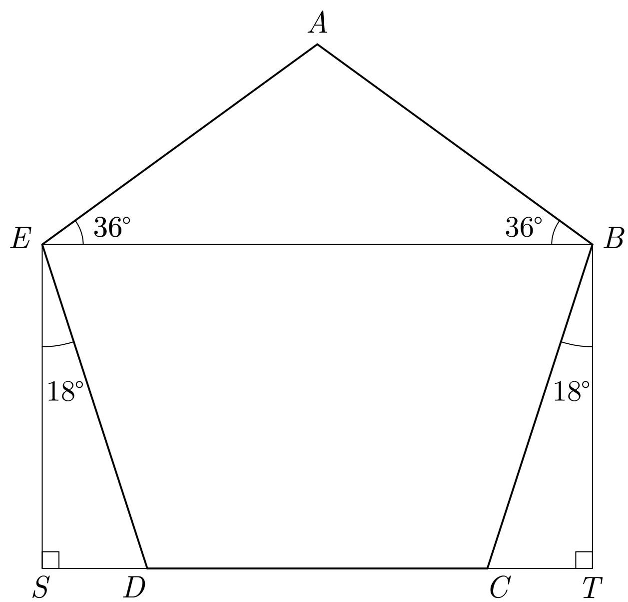
This theorem can be used to rule out the existence of regular lattice n-gons for all n except for $n = 8$. The case of regular lattice octagons can then be dealt with separately.

2. When dealing with the case $n = 5$ and the case $n \geq 7$ in the solution to Question 4, we obtained an infinite sequence of positive numbers $l_1, l_2, l_3, \ldots$ with the property that $l_i > l_{i+1}$ for all positive integers i. We needed to show that there is some k large enough so that $l_k < 1$. The fact that the sequence $l_1, l_2, l_3, \ldots$ is decreasing *does not* guarantee that the sequence eventually becomes smaller than 1. To see this, consider the sequence $1 + \frac{1}{2}, 1 + \frac{1}{3}, 1 + \frac{1}{4}, \ldots$. This is a sequence of positive numbers that is decreasing, but is never less than 1. This is why we had to go through so much trouble to find an explicit k and prove that $l_k < 1$.

A computation of $\sin(18^\circ)$ and $\cos(36^\circ)$

Here we will prove that $\sin(18^\circ) = \frac{1}{4}(\sqrt{5} - 1)$ and $\cos(36^\circ) = \frac{1}{4}(\sqrt{5} + 1)$.

Consider the regular pentagon $ABCDE$ with side length 1 as shown in the diagram below.



Extend the line DC in both directions and let S and T be points on the extended line so that ES and BT are perpendicular to DC. From our solution to Question 2(a), we know ST is parallel to EB, and therefore, the length of EB is equal to the length of ST.

In our solution to Question 2(a) we showed that $\angle AEB = \angle ABE = 36^\circ$. Therefore the length of EB is $2\cos(36^\circ)$.

Since $\angle EDC = \angle BCD = 108^\circ$, we have $\angle EDS = \angle BCT = 72^\circ$ and so $\angle SED = \angle CBT = 18^\circ$. Then the length of ST is the sum of the lengths of SD, DC, and CT. The length of DC is 1, and the lengths of SD and CT are both $\sin(18^\circ)$. Since the length of EB is equal to the length of ST we have

$$2\cos(36^\circ) = 2\sin(18^\circ) + 1.$$

By the double angle formula for cosine, we have

$$2(1 - 2(\sin(18^\circ))^2) = 2\sin(18^\circ) + 1.$$

If we let $x = \sin(18^\circ)$ we have that x satisfies

$$4x^2 + 2x - 1 = 0.$$

The quadratic formula then gives us

$$x = \frac{-1 \pm \sqrt{5}}{4}.$$

Since $\sin(18^\circ) > 0$ we must have $\sin(18^\circ) = \frac{1}{4}(\sqrt{5} - 1)$. Using the equation

$$2\cos(36^\circ) = 2\sin(18^\circ) + 1$$

gives us

$$\cos(36^\circ) = \frac{\sqrt{5} - 1}{4} + \frac{1}{2} = \frac{\sqrt{5} + 1}{4}.$$

Problem of the Month

Problem 7: Smooth lists

April 2025

Define a function f whose input and output are both lists of n nonnegative integers by

$$f(a_1, a_2, \ldots, a_n) = (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_{n-1} - a_n|, |a_n - a_1|)$$

where, as usual, $|x|$ represents the absolute value of x.

For example,

$$f(1, 2, 3, 4) = (|1 - 2|, |2 - 3|, |3 - 4|, |4 - 1|) = (1, 1, 1, 3)$$

and

$$f(2, 3, 5) = (|2 - 3|, |3 - 5|, |5 - 2|) = (1, 2, 3).$$

We will denote by f^k the function that *iterates* the application of f a total of k times. For example,

$$f^4(1, 1, 1, 3) = f^3(0, 0, 2, 2) = f^2(0, 2, 0, 2) = f(2, 2, 2, 2) = (0, 0, 0, 0).$$

We will call a list $(a_1, a_2, \ldots, a_n)$ *smooth* if there is some m for which $f^m(a_1, \ldots, a_n) = (0, 0, \ldots, 0)$. That is, a list is smooth if some number of applications of f will result in the list of all zeros. For example, $(1, 1, 1, 3)$ is smooth since $f^4(1, 1, 1, 3) = (0, 0, 0, 0)$, as demonstrated above.

1. Find a list of length 5 that is not smooth. Find a list of length 7 that is not smooth.
2. Show that for all odd integers $n \geq 1$ there exists a list L of length n that is not smooth.
3. How many smooth lists (a, b, c) are there with a, b, and c each no larger than 100?
4. Suppose L is a list of length 4 consisting of only zeros and ones. Show that L is smooth.
5. Show that all lists of length 4 are smooth.

Problem of the Month

Problem 7: Smooth lists

April 2025

Hint

1. Consider lists that only contain the integers 0 and 1.
2. As with part (a), construct a list L so that all of its entries are either 0 or 1. If the number of 1s in L is a positive even number, what can you say about the number of 1s in $f(L)$?
3. If L is a list of three integers, how do the *parities* (parity refers to whether an integer is even or odd) of the integers in L compare to the parities of integers in $f(L)$? You might want to consider what happens to lists with various combinations of even and odd integers. It may also be helpful to think about how things can be simplified if the integers a, b, and c have a common factor.
4. There are only 16 such lists, so you could show this by checking all of them.
5. Compute $f^4(a, b, c, d)$ for a few lists (a, b, c, d). What do you notice?

Problem of the Month

Solution to Problem 7: Smooth lists

April 2025

1. The list $(1,1,0,0,0)$ is not smooth. To see this, we apply f fifteen times. Setting $L = (1,1,0,0,0)$, we have

$$\begin{array}{rclrclrcl} f(L) &=& (0,1,0,0,1) & f^2(L) &=& (1,1,0,1,1) & f^3(L) &=& (0,1,1,0,0) \\ f^4(L) &=& (1,0,1,0,0) & f^5(L) &=& (1,1,1,0,1) & f^6(L) &=& (0,0,1,1,0) \\ f^7(L) &=& (0,1,0,1,0) & f^8(L) &=& (1,1,1,1,0) & f^9(L) &=& (0,0,0,1,1) \\ f^{10}(L) &=& (0,0,1,0,1) & f^{11}(L) &=& (0,1,1,1,1) & f^{12}(L) &=& (1,0,0,0,1) \\ f^{13}(L) &=& (1,0,0,1,0) & f^{14}(L) &=& (1,0,1,1,1) & f^{15}(L) &=& (1,1,0,0,0) \end{array}$$

and so $f^{15}(1,1,0,0,0) = (1,1,0,0,0)$. This means no matter how many times f is applied, the list of lists above will repeat every fifteen applications, so we will never arrive at the list of five 0s.

The list $(1,1,0,0,0,0,0)$ is not smooth. Setting $L = (1,1,0,0,0,0,0)$, we have

$$\begin{array}{rclrcl} f(L) &=& (0,1,0,0,0,0,1) & f^2(L) &=& (1,1,0,0,0,1,1) \\ f^3(L) &=& (0,1,0,0,1,0,0) & f^4(L) &=& (1,1,0,1,1,0,0) \\ f^5(L) &=& (0,1,1,0,1,0,1) & f^6(L) &=& (1,0,1,1,1,1,1) \\ f^7(L) &=& (1,1,0,0,0,0,0) & & & \end{array}$$

which means $f^7(1,1,0,0,0,0,0) = (1,1,0,0,0,0,0)$. As with the previous example, applying f repeatedly to $(1,1,0,0,0,0,0)$ will yield the original list every seven applications and no list of 0s in this list of lists. Thus, the list of seven 0s will never appear, so $(1,1,0,0,0,0,0)$ is not smooth.

2. There are two important observations to make from part (a).

Observation 1: It appears that if every integer in a list L is either 0 or 1, then every integer in $f(L)$ is also either 0 or 1. Indeed, if every integer in L is either 0 or 1, then every integer in $f(L)$ is one of $|0-1|$, $|1-0|$, $|0-0|$, or $|1-1|$, which all simplify to either 0 or 1. We will use this observation in later parts of this problem as well.

Observation 2: If L is a list in which every integer is equal to either 0 or 1, then it appears that $f(L)$ has an even number of integers equal to 1.

Let us verify the second observation. We suppose $L = (a_1, a_2, \ldots, a_n)$ is such that $a_k = 0$ or $a_k = 1$ for each $k = 1, 2, \ldots, n$. The number of entries equal to 1 in the list $f(L)$ is equal to the number of times that the sequence

$$a_1, a_2, a_3, a_4, \ldots, a_{n-2}, a_{n-1}, a_n, a_1$$

changes value. For example, if $(a_1, a_2, a_3, a_4, a_5, a_6) = (0,0,1,1,0,1)$, then the sequence above changes value going from a_2 to a_3, a_4 to a_5, a_5 to a_6, and a_6 back to a_1. If the sequence above changed value an odd number of times, then its first and last integers would be different. However, the sequence starts and ends with a_1, so it must change value an even (possibly zero) number of times. Hence, $f(L)$ has an even number of integers equal to 1.

We now suppose n is odd with $n \geq 3$ and that $L = (a_1, a_2, \ldots, a_n)$ is a list of nonnegative integers having the following three properties:

(i) For every k in $\{1, \ldots, n\}$, either $a_k = 0$ or $a_k = 1$.

(ii) There are an even number of indices k with $a_k = 1$.

(iii) $a_k = 1$ for at least one k.

We will show that $f(L) = (b_1, b_2, \ldots, b_n)$ also satisfies properties (i), (ii), and (iii) (with "a" replaced by "b").

Since L satisfies property (i), Observation 1 and Observation 2 imply that $f(L)$ satisfies properties (i) and (ii). To see that $f(L)$ satisfies property (iii), first observe that n is odd, so properties (i) and (ii) of L imply that there are an odd number of k for which $a_k = 0$. In particular, this means the number of k for which $a_k = 0$ is not 0, so there is at least one integer in L that is equal to 0. Since L has at least one 0 and at least one 1 (by property (iii) of L), it must change values at some point. This will give rise to at least one 1 in $f(L)$. Therefore, $f(L)$ satisfies condition (iii).

Let n be an odd positive integer and consider the list $L = (a_1, a_2, \ldots, a_n)$ where $a_1 = a_2 = 1$ and $a_k = 0$ for $k \geq 3$. Then L has properties (i), (ii), and (iii). Therefore, by the above reasoning, $f(L)$ has properties (i), (ii), and (iii). In turn, this implies $f^2(L)$ has properties (i), (ii), (iii), and so on. That is, $f^m(L)$ has properties (i), (ii), and (iii) for all $m \geq 0$. Property (iii) ensures that $f^m(L)$ has at least one integer that does not equal 0, so this means $f^m(L)$ is not the list of 0s for any m. Therefore, L is not smooth.

3. We will show that a list (a, b, c) is smooth exactly when $a = b = c$. Since each of a, b, and c is between 1 and 100 inclusive, this will give a total of 100 smooth lists.

   Notice that if $a = b = c$, then $f(a, b, c) = (0, 0, 0)$, so (a, b, c) is smooth. What needs to be verified is that if (a, b, c) is smooth, then $a = b = c$.

   To start, we will establish a seemingly much less ambitious claim:

   Fact 1: If (a, b, c) is smooth, then a, b, and c have the same *parity*. That is, a, b, and c are either all even or all odd. (The parity of a number refers to whether it is even or odd.)

   To establish this claim, we will assume that a, b, and c do not all have the same parity and deduce that (a, b, c) is not smooth.

   Suppose a, b, and c are nonnegative integers at least one of which is even and at least one of which is odd. Consider the list

$$f(a, b, c) = (|a - b|, |b - c|, |c - a|).$$

   Since there are three integers in the list (a, b, c), at least two of a, b, and c must have the same parity (are both even or both odd). This means at least one of the integers $|a - b|$, $|b - c|$, or $|c - a|$ is even. On the other hand, we are assuming at least two of a, b, and c have different parity (one is even and one is odd), so this means $f(a, b, c)$ has at least one odd integer. Applying this reasoning repeatedly, it follows that if (a, b, c) has at least one even integer and at least one odd integer, then $f^m(a,b,c)$ has this property for every $m \geq 1$. This means $f^m(a,b,c)$ is never equal to $(0,0,0)$, so (a,b,c) cannot be smooth.

We now know that if (a,b,c) is smooth, then a, b, and c have the same parity. Since the difference between two integers of the same parity is even, this actually implies that if (a,b,c) is smooth, then the integers in $f(a,b,c)$ are all even. This will be important in finishing the argument, but we also need the following fact that allows for a sort of "reduction" in a smooth list having a common factor among its integers.

<u>Fact 2</u>: Suppose $a_1, a_2, \ldots, a_n$ are nonnegative integers with a common factor $r > 0$. Then the list $(a_1, a_2, \ldots, a_n)$ is smooth if and only if the list $\left(\frac{a_1}{r}, \frac{a_2}{r}, \ldots, \frac{a_n}{r}\right)$ is smooth.

Suppose $f(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$. By the definition of f, this means

$$(b_1, b_2, \ldots, b_n) = (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_n - a_1|)$$

Using properties of absolute values and that $r > 0$, we have

$$\begin{aligned} f\left(\frac{a_1}{r}, \frac{a_2}{r}, \ldots, \frac{a_n}{r}\right) &= \left(\left|\frac{a_1}{r} - \frac{a_2}{r}\right|, \left|\frac{a_2}{r} - \frac{a_3}{r}\right|, \ldots, \left|\frac{a_n}{r} - \frac{a_1}{r}\right|\right) \\ &= \left(\frac{|a_1 - a_2|}{r}, \frac{|a_2 - a_3|}{r}, \ldots, \frac{|a_n - a_1|}{r}\right) \\ &= \left(\frac{b_1}{r}, \frac{b_2}{r}, \ldots, \frac{b_n}{r}\right). \end{aligned}$$

In words, dividing each integer in a list by a common factor and then applying f has the same effect as applying f and then dividing each integer in the resulting list by that same common factor. Applying this fact repeatedly, it follows that if for some $m \geq 1$ we have $f^m(a_1, a_2, \ldots, a_n) = (c_1, c_2, \ldots, c_n)$, then

$$f^m\left(\frac{a_1}{r}, \frac{a_2}{r}, \ldots, \frac{a_n}{r}\right) = \left(\frac{c_1}{r}, \frac{c_2}{r}, \ldots, \frac{c_n}{r}\right)$$

Since $r \neq 0$, $c_k = 0$ if and only if $\frac{c_k}{r} = 0$, and this is true for any $1 \leq k \leq n$. This means $f^m(a_1, a_2, \ldots, a_n)$ is the list of all 0s if and only if $f^m\left(\frac{a_1}{r}, \frac{a_2}{r}, \ldots, \frac{a_n}{r}\right)$ is the list of all 0s. This completes the proof of the fact.

We established earlier that if (a,b,c) is smooth, then the integers in $f(a,b,c)$ are all even. To use the above fact, we need a way of keeping track of the number of common factors of 2 among the integers in $f(a,b,c)$.

To help with this, define a function E on the nonzero integers by $E(a) = r$ where r is the largest power of 2 that is a divisor of a. For example, $E(12) = 4$ since 4 is a divisor of 12, but 8 is not and neither is any higher power of 2. Also, $E(n) = 1$ for any odd number n since $2^0 = 1$ is the largest power of 2 that divides any odd number.

Here are three features of the function E that we will use. Their proofs are left as an exercise.

(F1) $\frac{a}{E(a)}$ is an odd integer.

(F2) If r is a power of 2 and $\frac{a}{r}$ is an odd integer, then $r = E(a)$.

(F3) $E(a) = E(-a) = E(|a|)$.

Suppose $L = (a, b, c)$ is smooth and that a, b, and c are all even and not all 0. We let $r = \min\{E(a), E(b), E(c)\}$ and set $K = \left(\frac{a}{r}, \frac{b}{r}, \frac{c}{r}\right)$. If some of a, b, and c are 0, then some of $E(a)$, $E(b)$, and $E(c)$ are undefined. In this situation, r is the minimum of the values that are defined.

Because of how r is chosen, we will have that $\frac{a}{r}$, $\frac{b}{r}$, and $\frac{c}{r}$ are all integers. Also, since $r = E(a)$ or $r = E(b)$ or $r = E(c)$, at least one integer in K must be odd by F1. We are assuming that L is smooth, so Fact 2 implies that K is smooth as well. Thus, K is a smooth list with at least one odd integer, which means that all three of the integers in K must be odd by Fact 1. By F2, this means $E(a) = E(b) = E(c)$. We have established the following: If (a, b, c) is smooth with a, b, and c all even and not all 0, then $E(a) = E(b) = E(c)$.

Next, suppose $L = (a, b, c)$ is smooth and that a, b, and c are all odd. We want to prove that $a = c$. To do this, we will suppose $a \neq c$ and deduce a contradiction. Since a, b, and c are all odd, $f(L) = (|a - b|, |b - c|, |c - a|)$ has all even integers and since $a \neq c$, $|c - a| \neq 0$. Also, L is smooth, so $f(L)$ is smooth. From the previous paragraph, this means $E(|a-b|) = E(|b-c|) = E(|c-a|)$. By F3 above, $E(a-b) = E(b-c) = E(c-a)$. Let this common value be r. Then by F1, $\frac{a-b}{r}$ and $\frac{b-c}{r}$ are both some odd integer m, so $\frac{a-b}{r} + \frac{b-c}{r} = 2m$. Then

$$\frac{a-c}{r} = \frac{a-b}{r} + \frac{b-c}{r} = 2m,$$

so $a - c = 2rm$. Therefore, $2r$ is a divisor of $a - c$. Since r is a power of 2, so is $2r$, and this means $E(a - c) \geq 2r > r$. However, $E(a - c) = r$, so this is a contradiction. We are forced to conclude that our assumption $a \neq c$ is false, implying $a = c$. By a similar argument, it can be shown that $b = c$, so $a = b = c$.

We have now established the following: If (a, b, c) is smooth with a, b, and c all odd, then $a = b = c$.

We now return to (and finish) the case when (a, b, c) is smooth with a, b, and c all even.

Suppose again that (a, b, c) is smooth and that a, b, and c are all even. If $a = b = c = 0$, then there is nothing to prove. Otherwise, we know $E(a) = E(b) = E(c) = r$, so $\frac{a}{r}$, $\frac{b}{r}$, and $\frac{c}{r}$ are all odd. Since $\left(\frac{a}{r}, \frac{b}{r}, \frac{c}{r}\right)$ is also smooth, $\frac{a}{r} = \frac{b}{r} = \frac{c}{r}$, from which it follows that $a = b = c$.

Therefore, if (a, b, c) is smooth, then $a = b = c$.

4. You may be getting the idea that keeping track of the parity of the elements in a list is of great importance in this problem. In the previous part, we showed that if (a, b, c) is smooth, then the integers in $f(a, b, c)$ are all even.

   The critical observation of this and the next part is that if a, b, c, and d are any positive integers, then there is some m for which the integers in $f^m(a, b, c, d)$ are all even. If you are familiar with *modular arithmetic*, you may be able to streamline most of the upcoming work. However, this solution will not assume any such knowledge.

For a list $(a_1, a_2, \ldots, a_n)$ of nonnegative integers, define

$$g(a_1, a_2, \ldots, a_n) = (a_1 + a_2, a_2 + a_3, a_3 + a_4, \cdots, a_{n-1} + a_n, a_n + a_1).$$

For $m \geq 2$, we define $g^m(a_1, a_2, \ldots, a_n)$ to be the list attained from $(a_1, a_2, \ldots, a_n)$ by applying g repeatedly m times.

The function g looks similar to f, but it lacks absolute values and involves addition rather than subtraction. While g and f are genuinely different functions, g can be used to keep track of the parity of the integers in lists produced by applying f. More precisely, suppose $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are lists of nonnegative integers with the property that for each $1 \leq k \leq n$, a_k and b_k have the same parity. If we set $f(a_1, a_2, \ldots, a_n) = (c_1, c_2, \ldots, c_n)$ and $g(b_1, b_2, \ldots, b_n) = (d_1, d_2, \ldots, d_n)$, then for each k with $1 \leq k \leq n$, c_k and d_k have the same parity as well. To see this, observe that for $k \leq n$, we have $c_k = |a_k - a_{k+1}|$ and $d_k = b_k + b_{k+1}$ (where we take the convention that $a_{n+1} = a_1$ and $b_{n+1} = b_1$). If $c_k = a_k - a_{k+1}$, then $c_k + d_k = (a_k + b_k) - (a_{k+1} - b_{k+1})$. By the assumptions on $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$, $a_k + b_k$ and $a_{k+1} - b_{k+1}$ are both even, so $c_k + d_k$ is even. This means c_k and d_k must have the same parity. Similarly, if $c_k = a_{k+1} - a_k$, then c_k and d_k have the same parity.

The above paragraph shows that the integers in $g(a_1, a_2, \ldots, a_n)$ have the same parities as the corresponding integers in $f(a_1, a_2, \ldots, a_n)$. Applying the fact again, we have that the integers in $g^2(a_1, a_2, \ldots, a_n)$ have the same parities as the corresponding integers in $f^2(a_1, a_2, \ldots, a_n)$. This can be repeated to get that the integers in $g^m(a_1, a_2, \ldots, a_n)$ have the same parities as the corresponding integers in $f^m(a_1, a_2, \ldots, a_n)$ for all $m \geq 2$.

We can use this to prove that the integers in $f^4(a, b, c, d)$ are all even for any nonnegative integers a, b, c, and d. Consider an arbitrary list (a, b, c, d) of four nonnegative integers and compute $g^4(a, b, c, d)$:

$$\begin{aligned}
&g^4(a, b, c, d)\\
=&g^3(a + b, b + c, c + d, d + a)\\
=&g^2(a + 2b + c, b + 2c + d, c + 2d + a, d + 2a + b)\\
=&g(a + 3b + 3c + d, b + 3c + 3d + a, c + 3d + 3a + b, d + 3a + 3b + c)
\end{aligned}$$

which is equal to

$$(2a + 4b + 6c + 4d, 2b + 4c + 6d + 4a, 2c + 4d + 6a + 4b, 2d + 4a + 6b + 4c).$$

While this could be seen as a bit of a mess, the important thing to notice is that every integer in $g^4(a, b, c, d)$ is even. By the discussion above, this means every integer in $f^4(a, b, c, d)$ is even. Finally, recall from part (b) that if a, b, c, and d are all either 0 or 1, then every integer in $f^4(a, b, c, d)$ is either 0 or 1. Hence, every integer in $f^4(a, b, c, d)$ must be equal to 0 since 1 is odd. That is, $f^4(a, b, c, d) = (0, 0, 0, 0)$, so (a, b, c, d) is smooth.

5. We can solve this problem by putting together several ideas that have come up in previous parts.

This proof is formalizing the following idea, which can be observed if you apply f repeatedly to an arbitrary list of four positive integers: After at most four applications, all numbers in the resulting list will have a common factor of 2. Also, the largest integer in the resulting list will be no larger than the largest integer in the original list. Using Fact 2 from the solution to part (c), the common factor of 2 can be divided out and we will have "reduced" to a list whose largest integer is strictly smaller than the largest integer in the original list. Applying f at most four more times, we can "reduce" again. Eventually, the integers in the list will have a common factor so large that when it is factored out, the remaining integers are all either 0 or 1. At this point, part (d) can be applied.

As mentioned, the final observation we will need is that for a list L of nonnegative integers, the largest integer in $f(L)$ is no larger than the largest integer in L. In other words, the largest integer in $f(L)$ could be the same as the largest integer in L, but it cannot be bigger. This is because the largest integer in $f(a_1, a_2, \ldots, a_n)$ is equal to the largest difference between two adjacent integers in $(a_1, a_2, \ldots, a_n)$ (where a_1 and a_n are considered adjacent). The largest difference that can possibly occur between adjacent integers in L is equal to the largest integer in L. This occurs if a 0 happens to be adjacent to an occurrence of the largest integer in L. In this case, the largest integer in $f(L)$ will be equal to the largest integer in L. Otherwise, the largest integer in $f(L)$ is strictly smaller than the largest integer in L.

We now suppose (a, b, c, d) is a list of nonnegative integers that is *not* smooth. We will derive a contradiction from this assumption, thereby proving that all lists of four nonnegative integers are smooth.

If (a, b, c, d) is not smooth, then $f^4(a, b, c, d)$ is not smooth either. From part (d), $f^4(a, b, c, d)$ consists of only even integers, say $f^4(a, b, c, d) = (2a', 2b', 2c', 2d')$. By the fact in part (c), (a', b', c', d') is smooth if and only if $(2a', 2b', 2c', 2d')$ is smooth, and so (a', b', c', d') is not smooth since $(2a', 2b', 2c', 2d')$ is not smooth. We also know that the largest integer among a, b, c, d is at least as large as the largest integer among $2a', 2b', 2c', 2d'$. This means the largest integer among a, b, c, d is strictly larger than the largest among a', b', c', d'.

We have shown that if there is a list (a, b, c, d) of nonnegative integers that fails to be smooth, then there is a list (a', b', c', d') that fails to be smooth *and* its largest integer is smaller than the largest integer in (a, b, c, d). This fact can be applied to (a', b', c', d') to get another list (a'', b'', c'', d'') that fails to be smooth but has a smaller largest integer than (a', b', c', d'). Since the largest integer in these lists keeps getting smaller, we must eventually get a list whose largest integer is 1 and is not smooth. In part (d), we showed that no such list exists. This gives the contradiction we sought.

In other words, every list (a, b, c, d) of four nonnegative integers is smooth.

Problem of the Month

Problem 8: Some Surprising Squares

May 2025

This month's problem is inspired by Question 9 on the 2025 Euclid contest. The question in its original form is on the next page. As a warm up, try the problem yourself before attempting the Problem of the Month.

While solving Q9(c), you need to find pairs of integers (m, e) satisfying that $m^2 - 8e^2$ is a perfect square. Let's investigate this problem further.

1. For each of the following equations, find one pair (m, e) of non-zero integers that solve it: $m^2 - 8e^2 = 1$, $m^2 - 8e^2 = 4$ and $m^2 - 8e^2 = 9$.

Integers a and b are called *coprime* if they share no positive common divisors other than 1. For example, 3 and 5 are coprime but 4 and 6 are not.

2. Find a pair (m, e) of coprime integers satisfying $m^2 - 8e^2 = 49$.

Let's focus on expressions of the form $a + b\sqrt{8}$, where a and b are integers. Define the *norm* of $a + b\sqrt{8}$ to be $N(a + b\sqrt{8}) = (a + b\sqrt{8})(a - b\sqrt{8})$.

3. Let a, b, c, d be integers. Prove that $N\big((a + b\sqrt{8})(c + d\sqrt{8})\big) = N(a + b\sqrt{8})N(c + d\sqrt{8})$.
4. It turns out that $19^2 - 8(3^2) = 17^2$ and $27^2 - 8(5^2) = 23^2$. Find coprime integers a, b so that $a^2 - 8b^2 = 391^2$.
5. Find infinite sequences of integers $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ satisfying that for all positive integers n,
   - a_n and b_n are coprime, and
   - $a_n^2 - 8b_n^2 = 7^{2^n}$.

   When we write 7^{2^n} we mean $7^{(2^n)}$. So, for example, when $n = 5$, 7^{2^n} is equal to 7^{32} and **not** 49^5.

Here is Question 9 from the 2025 Euclid contest.

Suppose that $p(x) = qx^3 - rx^2 - sx + t$ for some positive integers $q < r < s < t$ which form an arithmetic sequence.

(a) Show that $x = 1$ is a root of $p(x)$.

(b) Suppose that the average of q, r, s, t is 19 and that $p(x)$ has three rational roots. Determine the roots of $p(x)$.

(c) Prove that, for every positive integer $n > 3$, there are at least two arithmetic sequences of positive integers $q < r < s < t$ with common difference $2n$ for which $p(x)$ has three rational roots.

(An *arithmetic sequence* is a sequence in which each term after the first is obtained from the previous term by adding a constant, called the common difference. For example, $3, 5, 7, 9$ are the first four terms of an arithmetic sequence.)

Problem of the Month

Problem 8: Some Surprising Squares

May 2025

Hint

1. There is a solution to $m^2 - 8e^2 = 1$ where both m and e are integers between 0 and 5. Can you somehow use your solution for the equation $m^2 - 8e^2 = 1$ to find solutions to the equations $m^2 - 8e^2 = 4$ and $m^2 - 8e^2 = 9$?
2. There is a pair of integers (m, e) satisfying $m^2 - 8e^2 = 49$ where both m and e are single-digit positive integers.
3. Try expanding out $N\big((a + b\sqrt{8})(c + d\sqrt{8})\big)$ and $N(a + b\sqrt{8})N(c + d\sqrt{8})$.
4. Expand out $N(a + b\sqrt{8})$ and use the result from Question 3.
5. You will need to apply Question 3 repeatedly here. Consider your m and e from Question 2. What is $N((m + e\sqrt{8})^2)$? What about $N((m + e\sqrt{8})^{2^n})$?

Problem of the Month

Solution to Problem 8: Some Surprising Squares

May 2025

1. The pair $m = 3$, $e = 1$, satisfies $m^2 - 8e^2 = 1$. We can use this solution to find the pairs m and e that satisfy $m^2 - 8e^2 = 4$ as follows:

$$4 = 4(3^2 - 8(1^2)) = (2 \cdot 3)^2 - 8(2 \cdot 1)^2 = 6^2 - 8(2)^2.$$

Similarly we have

$$9 = 9(3^2 - 8(1^2)) = (3 \cdot 3)^2 - 8(3 \cdot 1)^2 = 9^2 - 8(3)^2.$$

So, the pairs $(m, e) = (6, 2)$ and $(m, e) = (9, 3)$ satisfy $m^2 - 8e^2 = 4$ and $m^2 - 8e^2 = 9$ respectively.

2. The pair $m = 9$ and $e = 2$ satisfies $m^2 - 8e^2 = 49$. There are lots of other pairs too. Here are a few others: $(m, e) = (11, 3), (43, 15), (57, 20), (249, 88)$.

It is tempting to just imitate what we did in Question 1. However, that yields the pair $(m, e) = (21, 7)$, and 21 and 7 are *not* coprime!

3. We have

$$\begin{aligned}
N((a + b\sqrt{8})(c + d\sqrt{8})) &= N(ac + 8bd + (ad + bc)\sqrt{8}) \\
&= (ac + 8bd + (ad + bc)\sqrt{8})(ac + 8bd - (ad + bc)\sqrt{8}) \\
&= (ac + 8bd)^2 - 8(ad + bc)^2 \\
&= a^2c^2 + 16abcd + 64b^2d^2 - 8a^2d^2 - 16abcd - 8b^2c^2 \\
&= (a^2 - 8b^2)(c^2 - 8d^2) \\
&= (a + b\sqrt{8})(a - b\sqrt{8})(c + d\sqrt{8})(c - d\sqrt{8}) \\
&= N(a + b\sqrt{8})N(c + d\sqrt{8}).
\end{aligned}$$

4. There are two important observations to make here. First, $391 = 17 \times 23$. Second, is that $N(a + b\sqrt{8}) = a^2 - 8b^2$. So, finding integers a, b satisfying $a^2 - 8b^2 = d$ is equivalent to finding integers a, b satisfying $N(a + b\sqrt{8}) = d$.

From the information given in the problem statement, we have $N(19 + 3\sqrt{8}) = 17^2$ and $N(27 + 5\sqrt{8}) = 23^2$. Therefore, applying Question 3 we have

$$\begin{aligned}
391^2 = 17^2 \cdot 23^2 &= N(19 + 3\sqrt{8})N(27 + 5\sqrt{8}) \\
&= N\big((19 + 3\sqrt{8})(27 + 5\sqrt{8})\big) \\
&= N(633 + 176\sqrt{8}).
\end{aligned}$$

Therefore $633^2 - 8(176^2) = 391^2$. It remains to check that 633 and 176 are coprime.

The positive divisors of 633 are $1, 3, 211, 633$. Since $3, 211$, and 633 are not divisors of 176, we can conclude that 1 is the only positive common divisor of 633 and 176.

5. From Question 2, we know $9^2 - 8 \cdot 2^2 = 7^2$. Notice that $N(9+2\sqrt{8}) = 9^2 - 8 \cdot 2^2 = 7$. So, with the result from Question 3 at our disposal, we can repeatedly square $9+2\sqrt{8}$ to get elements a_n and b_n of our sequence.

   To that end, define $a_1 = 9$ and $b_1 = 2$. We then recursively define a_n and b_n by

   $$a_n + b_n\sqrt{8} = (a_{n-1} + b_{n-1}\sqrt{8})^2 = (a_{n-1}^2 + 8b_{n-1}^2) + 2a_{n-1}b_{n-1}\sqrt{8}.$$

   Therefore $a_n = a_{n-1}^2 + 8b_{n-1}^2$ and $b_n = 2a_{n-1}b_{n-1}$. To see $a_n^2 - 8b_n^2 = 7^{2^n}$ we have

   $$a_n^2 - 8b_n^2 = N(a_n + b_n\sqrt{8}) = N((a_1 + b_1\sqrt{8})^{2^{n-1}}) = (N(a_1 + b_1\sqrt{8}))^{2^{n-1}} = 7^{2^n}$$

   where the third equality is obtained by applying Question 3 repeatedly.

   It remains to show that for every n, a_n and b_n are coprime. To this end, first note that a_1 and b_1 are coprime (since $a_1 = 9$ and $b_1 = 2$).

   Next we will prove that if a_n and b_n share a prime factor p (which is equivalent to the statement that a_n and b_n are *not* coprime), then a_{n-1} and b_{n-1} must also share a prime factor p. Once we have proved this, we can repeatedly apply it to show that if there is some n for which a_n and b_n share a prime factor, then a_1 and b_1 must share the same prime factor, a contradiction!

   So, assume p is a prime that divides both a_n and b_n. Since $a_n^2 - 8b_n^2 = 7^{2^n}$, which is odd, a_n and b_n cannot both be even. Therefore $p \neq 2$.

   To proceed, we will repeatedly exploit the following two properties of prime numbers, which we now state without proof:

   - *If p is a prime and p divides ab, then p divides a or p divides b.*
   - *If p is a prime and p divides n^2, then p divides n.*

   The first property is orten called *Euclid's lemma*. Note that the second property is a special case of the first.

   With these facts in our back pocket, let's return to the proof. Since p is an odd prime and p divides $2a_{n-1}b_{n-1}$, we must have that p divides a_{n-1} or b_{n-1}.

   Since p divides a_n, write $pm = a_n$ for some integer m. Suppose first that p divides a_{n-1}, so $pk = a_{n-1}$ for some integer k. Then $pm = p^2k^2 + 8b_{n-1}^2$, which rearranges to $8b_{n-1} = p(m - pk^2)$. Therefore p divides $8b_{n-1}^2$. Since p is an odd prime, we must have that p divides b_{n-1}.

   On the other hand, suppose that p divides b_{n-1} and write $pk = b_{n-1}$. Then similar to the previous case we have $pm = a_{n-1}^2 + 8p^2k^2$. Therefore p also divides a_{n-1}.

   We have proved what we set out to prove: If a_n and b_n share a prime divisor p, then a_{n-1} and b_{n-1} share the prime divisor p. Repeatedly applying this result, we get that if a_n and b_n share a prime divisor p, then $a_1 = 9$ and $b_1 = 2$ share a prime divisor p. However, since 2 and 9 share no prime divisors, a_n and b_n share no prime divisors for all n, completing the proof.

   If you are familiar with induction, you can formalise the above argument as an inductive argument.

To finish things off, let's explicitly calculate the first few terms in our sequences. We have

$$\begin{aligned}
(a_1, b_1) &= (9, 2) \\
(a_2, b_2) &= (113, 36) \\
(a_3, b_3) &= (23\,137, 8\,136) \\
(a_4, b_4) &= (1\,064\,876\,737, 376\,485\,264).
\end{aligned}$$

Sure enough, it turns out that

$$(1\,064\,876\,737)^2 - 8(376\,485\,264)^2 = 33\,232\,930\,569\,601 = 7^{16}.$$

Cool.