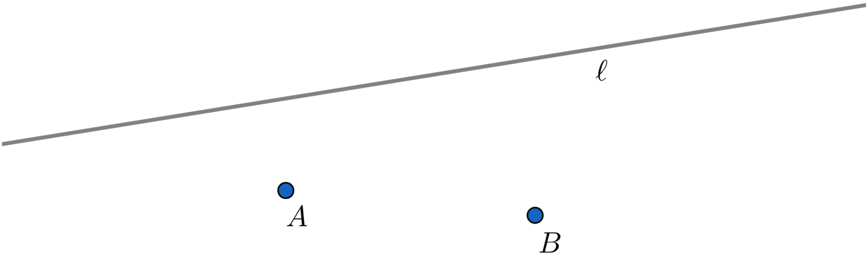
COMP 761: Lecture 2 – Proofs

David Rolnick

September 4, 2020

Problem

You would like to travel from your work (point *A*) to your house (point *B*), stopping off at some point along the river (line ℓ) to gather water. What's an algorithm for finding the shortest total distance you have to travel?



Course Announcements

Course Announcements

- TA: Vincent Luczkow

Course Announcements

- TA: Vincent Luczkow
- Vincent's office hours: 11-12 am Thursdays

Course Announcements

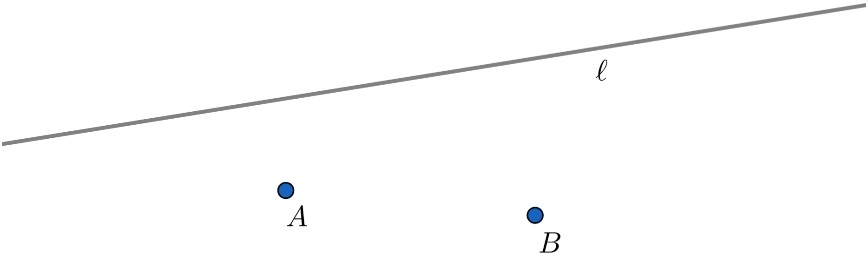
- TA: Vincent Luczkow
- Vincent's office hours: 11-12 am Thursdays
- Slack workspace for class discussions (will send invites soon)

Course Announcements

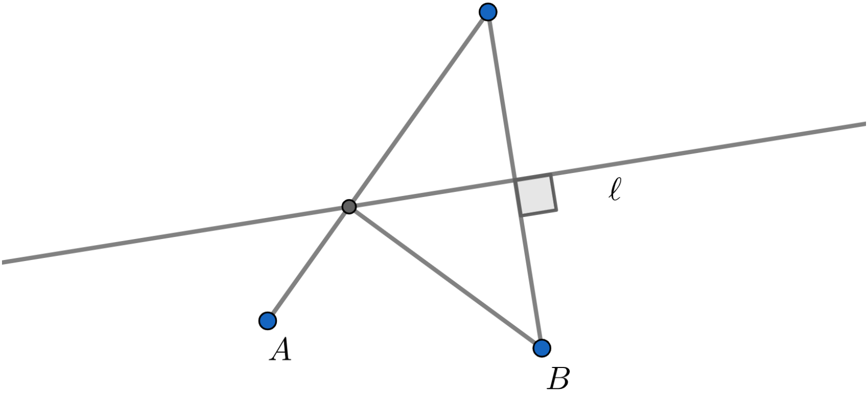
- TA: Vincent Luczkow
- Vincent's office hours: 11-12 am Thursdays
- Slack workspace for class discussions (will send invites soon)
- Problem Set 1 will be released Tuesday, due Friday Sept 18

Problem

You would like to travel from your work (point A) to your house (point B), stopping off at some point along the river (line ℓ) to gather water. What's an algorithm for finding the shortest total distance you have to travel?



Answer



What is a proof?

A proof is a set of logical steps that explains why an answer is true.

What is a proof?

A proof is a set of logical steps that explains why an answer is true.

- Convince someone else

What is a proof?

A proof is a set of logical steps that explains why an answer is true.

- Convince someone else
- Convince yourself, make sure you didn't make a mistake

What is a proof?

A proof is a set of logical steps that explains why an answer is true.

- Convince someone else
- Convince yourself, make sure you didn't make a mistake
- Sometimes provide more insight into what is going on

What is a proof?

A proof is a set of logical steps that explains why an answer is true.

- Convince someone else
- Convince yourself, make sure you didn't make a mistake
- Sometimes provide more insight into what is going on

You can think of an *answer* as something short ($x = 2$) but a proof as the full *solution* (this is why $x = 2$)

In this course

In this course

- You will be expected to provide proofs on the problem sets.

In this course

- You will be expected to provide proofs on the problem sets.
- In class, sometimes full proofs, sometimes just intuitions for why true, if proof is hard

In this course

- You will be expected to provide proofs on the problem sets.
- In class, sometimes full proofs, sometimes just intuitions for why true, if proof is hard
- Useful to be able to understand a proof might look like, even if we don't always dive into it

Proof-writing tips

1. Indicate how you are making each conclusion

Proof-writing tips

1. Indicate how you are making each conclusion

- Good: *Combining equations (1) and (5), we find that* $x = y + 1$*.*

Proof-writing tips

1. Indicate how you are making each conclusion

- Good: *Combining equations (1) and (5), we find that* $x = y + 1$*.*
- Bad: *We get* $x = y + 1$*.*

Proof-writing tips

1. Indicate how you are making each conclusion

- Good: *Combining equations (1) and (5), we find that* $x = y + 1$*.*
- Bad: *We get* $x = y + 1$*.*

This is also good to make sure you aren't assuming what you are trying to prove!

Proof-writing tips

2. Define new things clearly (just like in code)

Proof-writing tips

2. Define new things clearly (just like in code)

- Good: *Let m be the right-hand side of the previous equation. Then, the algorithm runs in time $O(n + m)$, where n is the number of bits in the input.*

Proof-writing tips

2. Define new things clearly (just like in code)

- Good: *Let m be the right-hand side of the previous equation. Then, the algorithm runs in time $O(n + m)$, where n is the number of bits in the input.*
- Bad: *Then, the algorithm runs in time $O(n + \text{the right-hand side})$.*

Proof-writing tips

3. Use words in addition to equations

Proof-writing tips

3. Use words in addition to equations

- Good: *Because* $x = y^2$ *and* $y = z^2$*, we have*

$$x = z^4.$$

Proof-writing tips

3. Use words in addition to equations

- Good: *Because* $x = y^2$ *and* $y = z^2$*, we have*
$$x = z^4.$$
- Bad: $x = y^2, y = z^2, \Rightarrow x = z^4$.

Proof-writing tips

3. Use words in addition to equations

- Good: *Because* $x = y^2$ *and* $y = z^2$*, we have*
$$x = z^4.$$
- Bad: $x = y^2, y = z^2, \Rightarrow x = z^4$.

Also, remember to break into paragraphs, otherwise it can get very hard to read.

Proof-writing tips

4. Aim for a concise, formal style. Use "we" instead of "I" or "you".

Proof-writing tips

4. Aim for a concise, formal style. Use “we” instead of “I” or “you”.

- Good: *Squaring both sides of the equation, we obtain* $(x-1)^2 = \sin(z - \sqrt{3}\omega)$.

Proof-writing tips

4. Aim for a concise, formal style. Use "we" instead of "I" or "you".

- Good: *Squaring both sides of the equation, we obtain* $(x-1)^2 = \sin(z - \sqrt{3}\omega)$.
- Bad: *What happens if you square both sides of the equation? You get* $(x-1)^2 = \sin(z - \sqrt{3}\omega)$*!*

Proof-writing tips

5. Figures are great!

Proof-writing tips

5. Figures are great!

- Though remember to define anything in the main body of the text, rather than just in the figure.

Proof-writing tips

5. Figures are great!

- Though remember to define anything in the main body of the text, rather than just in the figure.
- Good: *In figure 1, point P is the intersection of segment AB with line L.*

Proof-writing tips

6. If your approach is complicated, describe it and break it up.

Proof-writing tips

6. If your approach is complicated, describe it and break it up.

- Good: *We will prove the result by induction, dividing into 3 cases according to whether a is positive, negative, or* 0. *We begin by proving the following Claim.*

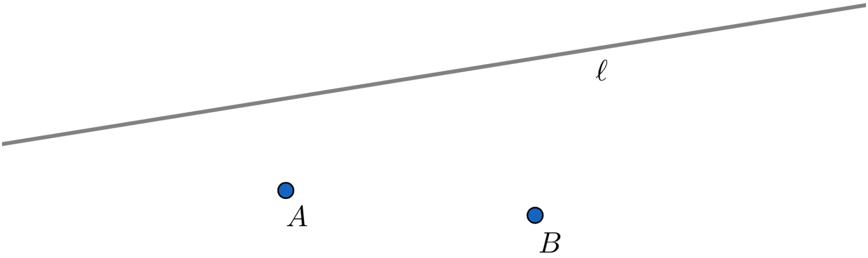
  Claim: b is even.
  Proof of Claim: ....

  Having proven the claim, we proceed to our three cases:

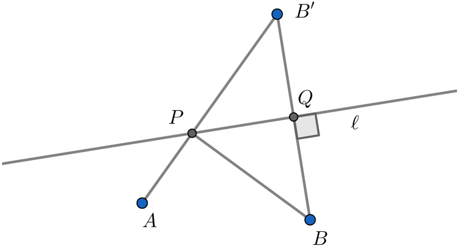
  Case 1: $a > 0$
  Proof in Case 1: ....

Problem

You would like to travel from your work (point *A*) to your house (point *B*), stopping off at some point along the river (line ℓ) to gather water. What's an algorithm for finding the shortest total distance you have to travel?



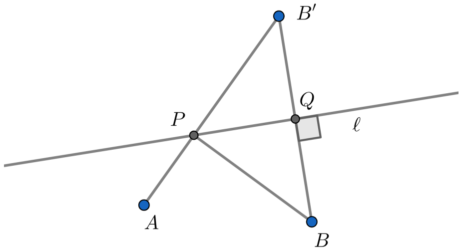
Proof



To minimize the distance traveled, it is optimal to travel from A to some point P along ℓ, and then from P to B. We therefore must find the point P on ℓ such that $AP + BP$ is minimized.

Let B' be the reflection of point B across line ℓ (that is, BB' is perpendicular to ℓ and B and B' are equidistant from ℓ), as shown in the Figure. Let Q be the intersection of BB' with ℓ.

Example proof



Claim: for any point P on ℓ, the distance $B'P$ equals the distance BP.
Proof of Claim: By the Pythagorean Theorem on right triangle PQB:

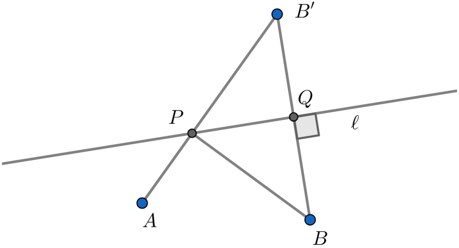
$$BP^2 = PQ^2 + BQ^2.$$

Similarly, from the Pythagorean Theorem on right triangle PQB', we obtain:

$$B'P^2 = PQ^2 + B'Q^2.$$

Combining these two equations and using the fact that $B'Q = BQ$, we conclude that $BP = B'P$, proving the claim.

Example proof



Now, since $B'P = BP$ for any P, we know that minimizing $AP + BP$ is equivalent to minimizing $AP + B'P$. Since a straight line is the shortest distance between two points, the optimum is attained where P is the intersection of AB' with ℓ.

Thus, our algorithm is to reflect B across ℓ to B' and to take the intersection of AB' with ℓ.

■

Problem (Monty Hall).

You are in a game show where you can win a prize. There are three doors. Behind two of them are goats. Behind the third is a car. (Assume for this problem that you want a car more than a goat.) You pick a door at random. The host (who knows what is where) then opens one of the other doors, revealing a goat. You can either stick with your door, or switch to the other one. Which is better?

Solution

Solution

There are two cases to be considered: either the initial pick is a car or a goat.

Solution

There are two cases to be considered: either the initial pick is a car or a goat.

Case 1. The initial pick is a car.

Solution

There are two cases to be considered: either the initial pick is a car or a goat.

Case 1. The initial pick is a car.
In this case, it is optimal to stay with the initial pick.

Solution

There are two cases to be considered: either the initial pick is a car or a goat.

Case 1. The initial pick is a car.
In this case, it is optimal to stay with the initial pick.

Case 2. The initial pick is a goat.

Solution

There are two cases to be considered: either the initial pick is a car or a goat.

Case 1. The initial pick is a car.
In this case, it is optimal to stay with the initial pick.

Case 2. The initial pick is a goat.
In this case, the remaining door must be the car, so it is optimal to switch.

Solution

There are two cases to be considered: either the initial pick is a car or a goat.

Case 1. The initial pick is a car.
In this case, it is optimal to stay with the initial pick.

Case 2. The initial pick is a goat.
In this case, the remaining door must be the car, so it is optimal to switch.

Since Case 1 occurs with 1/3 probability and Case 2 with 2/3 probability, 2/3 of the time it will be optimal to switch. Therefore, switching is the best strategy.
■

Problem-solving tips

Problem-solving tips

1. Write down assumptions/conditions mathematically
    - This is not always easy
    - Framing it the right way is sometimes half the problem

Problem-solving tips

1. Write down assumptions/conditions mathematically
   - This is not always easy
   - Framing it the right way is sometimes half the problem
2. Try out a small example
   - By hand or via code
   - Good even if you don't know what you are looking for

Problem-solving tips

1. Write down assumptions/conditions mathematically
   - This is not always easy
   - Framing it the right way is sometimes half the problem
2. Try out a small example
   - By hand or via code
   - Good even if you don't know what you are looking for
3. Think backwards from what you want
   - Make guesses about intermediate things that might be useful if true
   - Try to disprove them first, then try to prove them
   - But when writing the proof, work forwards

Problem-solving tips

1. Write down assumptions/conditions mathematically
   - This is not always easy
   - Framing it the right way is sometimes half the problem
2. Try out a small example
   - By hand or via code
   - Good even if you don't know what you are looking for
3. Think backwards from what you want
   - Make guesses about intermediate things that might be useful if true
   - Try to disprove them first, then try to prove them
   - But when writing the proof, work forwards
4. Think about what info you haven't used
   - What conditions are necessary or else it wouldn't work?
   - Good sign you'll need to use them!

Problem.

Out of any 1000 integers, prove that some subset of them sum to a multiple of 1000.

Trying to solve it

Trying to solve it

- Maybe we can try out an example

Trying to solve it

- Maybe we can try out an example
- But 1000 is a large number

Trying to solve it

- Maybe we can try out an example
- But 1000 is a large number
- Let's try 10 numbers

Trying to solve it

- Maybe we can try out an example
- But 1000 is a large number
- Let's try 10 numbers
- Maybe $1, 2, 3, 4, 5, 6, 6, 8, 9, 10$...whoops that is easy

Trying to solve it

- Maybe we can try out an example
- But 1000 is a large number
- Let's try 10 numbers
- Maybe $1, 2, 3, 4, 5, 6, 6, 8, 9, 10$...whoops that is easy
- How can that be harder?

Trying to solve it

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 = 32$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 = 32$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 = 43$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 = 32$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 = 43$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 = 44$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 = 32$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 = 43$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 = 44$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 + 1 = 45$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 = 32$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 = 43$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 = 44$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 + 1 = 45$

Trying to solve it

- Let's try picking them one by one so at least the sum of all of them isn't divisible by 10
- $1 = 1$
- $1 + 2 = 3$
- $1 + 2 + 3 = 6$
- $1 + 2 + 3 + 5 = 11$
- $1 + 2 + 3 + 5 + 6 = 17$
- $1 + 2 + 3 + 5 + 6 + 7 = 24$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 = 32$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 = 43$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 = 44$
- $1 + 2 + 3 + 5 + 6 + 7 + 8 + 1 + 1 + 1 = 45$
- $8 + 1 + 1 = 10$

Trying to solve it

Trying to solve it

- Will some of these partial sums always have the same last digit?

Trying to solve it

- Will some of these partial sums always have the same last digit?
- Yeah! There are 10 sums, and only 9 possible non-0 last digits

Trying to solve it

- Will some of these partial sums always have the same last digit?
- Yeah! There are 10 sums, and only 9 possible non-0 last digits
- (Sidenote: This is called the *Pigeonhole Principle*, and it's often really useful even though it's really obvious.)

Trying to solve it

- Will some of these partial sums always have the same last digit?
- Yeah! There are 10 sums, and only 9 possible non-0 last digits
- (Sidenote: This is called the *Pigeonhole Principle*, and it's often really useful even though it's really obvious.)
- So are we done for 10 numbers?

Trying to solve it

- Will some of these partial sums always have the same last digit?
- Yeah! There are 10 sums, and only 9 possible non-0 last digits
- (Sidenote: This is called the *Pigeonhole Principle*, and it's often really useful even though it's really obvious.)
- So are we done for 10 numbers?
- Yes!

Trying to solve it

- Will some of these partial sums always have the same last digit?
- Yeah! There are 10 sums, and only 9 possible non-0 last digits
- (Sidenote: This is called the *Pigeonhole Principle*, and it's often really useful even though it's really obvious.)
- So are we done for 10 numbers?
- Yes!
- What about 1000?

Trying to solve it

- Will some of these partial sums always have the same last digit?
- Yeah! There are 10 sums, and only 9 possible non-0 last digits
- (Sidenote: This is called the *Pigeonhole Principle*, and it's often really useful even though it's really obvious.)
- So are we done for 10 numbers?
- Yes!
- What about 1000?
- Same idea...

Let's write a formal proof

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$.

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Otherwise, there are only 999 possible remainders for the 1000 different S_k when divided by 1000.

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Otherwise, there are only 999 possible remainders for the 1000 different S_k when divided by 1000. By the Pigeonhole Principle, there must be some j, k such that S_j and S_k have the same remainder.

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Otherwise, there are only 999 possible remainders for the 1000 different S_k when divided by 1000. By the Pigeonhole Principle, there must be some j, k such that S_j and S_k have the same remainder.

Suppose without loss of generality that $j < k$.

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Otherwise, there are only 999 possible remainders for the 1000 different S_k when divided by 1000. By the Pigeonhole Principle, there must be some j, k such that S_j and S_k have the same remainder.

Suppose without loss of generality that $j < k$. Then, 1000 must divide the difference

$$S_k - S_j = \sum_{i=j+1}^{k} a_i.$$

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Otherwise, there are only 999 possible remainders for the 1000 different S_k when divided by 1000. By the Pigeonhole Principle, there must be some j, k such that S_j and S_k have the same remainder.

Suppose without loss of generality that $j < k$. Then, 1000 must divide the difference

$$S_k - S_j = \sum_{i=j+1}^{k} a_i.$$

This gives us the desired subset.

Let's write a formal proof

Let the 1000 integers be $a_1, a_2, \ldots, a_{1000}$. For $k = 1, \ldots, 1000$, let S_k denote the sum of the first k integers:

$$S_k = \sum_{i=1}^{k} a_i.$$

Suppose that some S_k is divisible by 1000. In that case, we are done.

Otherwise, there are only 999 possible remainders for the 1000 different S_k when divided by 1000. By the Pigeonhole Principle, there must be some j, k such that S_j and S_k have the same remainder.

Suppose without loss of generality that $j < k$. Then, 1000 must divide the difference

$$S_k - S_j = \sum_{i=j+1}^{k} a_i.$$

This gives us the desired subset.

■

Next time!

Proof techniques: Induction