Introduction to Discrete Math

Felipe P. Vista IV



Course Outline

- Mathematical Thinking
 - Convincing Arguments, Find Example, Recursion, Logic, Invariants
- Probability & Combinatronics
 - Counting, Probability, Random Variables
- Graph Theory
 - Graphs (cycles, classes, parameters)
- Number Theory & Cryptography
 - Arithmetic in modular form
 - Intro to Cryptography

Mathematical Thinking – Logic

EXAMPLES, COUNTEREXAMPLES, LOGIC

Logic

Examples

Counterexamples

Logic

- Sometimes, one example is already enough
- If we want to prove that white lions exists
 - It is enough to show just one white lion
 - such examples are not always easy to come up with
 - 13 in the wild and approximately 300 in captivity
 - https://whitelions.org/white-lion/faqs/

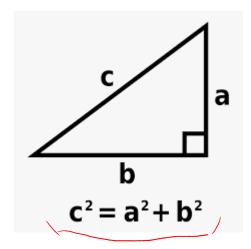


Problem I

• Is it possible that for three positive integer numbers a, b, and c so that $a^2+b^2=c^2$?

Solution

- To come up with this example, recall
 - Pythagorean Theorem with right angle, and sides 3, 4, and 5



$$h = \sqrt{(a^{2} + b^{2})}; h = c$$

$$c^{2} = a^{2} + b^{2}$$

$$25 = 16 + 9$$

$$5^{2} = 4^{2} + 3^{2}$$

Problem II

• Is it possible that for three positive integer numbers a, b, and c so that $a^3 + b^3 = c^3$?

Solution

- * conjecture conclusion assume to be true due to initial supporting evidence but no proof or disproof has yet been found
- This is in fact impossible, so there is no example
- Fermat's Last Theorem (1637), a famous mathematical conjecture
 - for any integer n > 2, there are no such integers a, b, & c such that $a^n + b^n = c^n$.
- Mathematicians failed tried to prove it for hundreds of years
 - Andrew Wiles was able to prove it in 1995

Problem III

• Is it possible that for positive integer numbers a, b, c, and d so that $a^4 + b^4 + c^4 = d^4$?

Solution

- We could initially assume that it is impossible due to <u>Fermat's</u> Last Theorem
- But the theorem only focus on equations with the form

$$\underline{\alpha}^n + b^n = \underline{c}^n$$

Hence, it is not applicable for this problem a, b c.

Solution

- It is actually possible, the smallest number though is very big $95800^4 + 217519^4 + 414560^4 = 422481^4$
- Computers used to derive the examples
- But the possible number of values are so huge that it is hard to find examples that satisfy the equation, even with the help of computers

Introduction to Discrete Math

Logic - Examples

Examples

Problem IV

• Is there a power of 2 that starts with 65?

Logic - Examples

Examples

Problem IV

• Is there a power of 2 that starts with 65?

Solution

- The answer is $2^{16} = 65536$ | 10 24 8 14 32 49
- This is the complete solution
- In fact, there is a power of 2 that starts w/ any integer n, n > 0
 - But much more difficult to prove

Counterexamples

• Logic

Logic - Counterexamples

Counterexamples

- Just one counterexample is enough to disprove a statement
- If we want to prove that all swans are white
 - Just one instance of black swan is enough to disprove it
 - However, it is often difficult to find such counterexamples





Introduction to Discrete Math

Logic - Counterexamples

Counterexamples

Theorem I

All rectangles are squares

Logic - Counterexamples

Counterexamples

Theorem I

• All rectangles are squares

Solution

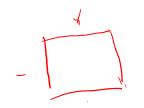
- A rectangle with sides of sizes 1 and 2, respectively, is not a square.
- This is a counterexample for the theorem, hence the theorem is wrong

Logic - Counterexamples

Counterexamples

Theorem II

All square are rectangles



Solution

- There is no counterexample for this case, hence the theorem is true
- Since square is a rectangle with equal sides.

Introduction to Discrete Math

Logic - Counterexamples

Counterexamples

Theorem II

• All square are rectangles

Logic - Counterexamples

Counterexamples

Theorem III

- Euler came up w/ a generalization of Fermat's Last Theorem
- For any n > 2, it is impossible for an n-th power of a positive integer to be represented as a sum of n-1 numbers w/c are the n-th powers of positive integers
- For n=3, it is the same as Fermat's Last Theorem: It is impossible that $a^3+b^3=c^3$.

Logic - Counterexamples

Counterexamples

Solution

• Lander came up with a counterexample in 1966 for n=5:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

• Elkies found another counterexample in 1986 for n=4:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

- Frye found the smallest counterexample for n=4 in 1988:
 - Which is an example for one statement & counterexample for another

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

Counterexamples

Logic

Logic - Logic

Logic

Logical Operators

- Negation
- Logical AND
- Logical OR
- If-then

Introduction to Discrete Math

Logic - Logic

Negation

Statement

All swans are white.

Introduction to Discrete Math

Logic - Logic

Negation

Statement

All swans are white.

Negation

Not all swans are white. Or, there are swans that are not white.

Statement

• There exists three positive integers a, b, & c, such that

$$a^3 + b^3 = c^3$$

Statement

• There exists three positive integers a, b, & c, such that $a^3 + b^3 = c^3$.

Negation

- There are no such positive integer numbers a, b, & c, such that $a^3 + b^3 = c^3$.
- Or for any positive integers a, b, & c, such that $a^3 + b^3 \neq c^3$.

Statement

- 4 = 2 + 2
- 5 = 2 + 2

Statement

- 4 = 2 + 2
- 5 = 2 + 2

Negation

- 4 ≠ 2 + 2 //
 5 ≠ 2 + 2

Negation

- Is true, if and only if the initial statement is wrong
- Is false, if and only if the initial statement is correct

Logical AND

Statement

- 4 = 2 + 2 AND $4 = 2 \times 2$
- The logical AND of two statements is true if and only if both statements are true.
- $4 = 2 + 2 \text{ AND } 4 = 2 \times 2 \rightarrow \text{TRUE}$
- 4 = 2 + 2 AND $5 = 2 \times 2 \rightarrow FALSE$
- 5 = 2 + 2 AND $4 = 2 \times 2 \rightarrow FALSE >$
- 5 = 2 + 2 AND $5 = 2 \times 2 \rightarrow FALSE \times$

Logical OR

Statement

- $4 = 2 + 2 OR 4 = 2 \times 2$
- The logical OR of two statements is true if and only if at least one of the statements is true.

•
$$4 = 2 + 2 \text{ OR } 4 = 2 \times 2 \rightarrow \text{TRUE}$$

•
$$4 = 2 + 2 \text{ OR } 5 = 2 \times 2 \rightarrow \text{TRUE}$$

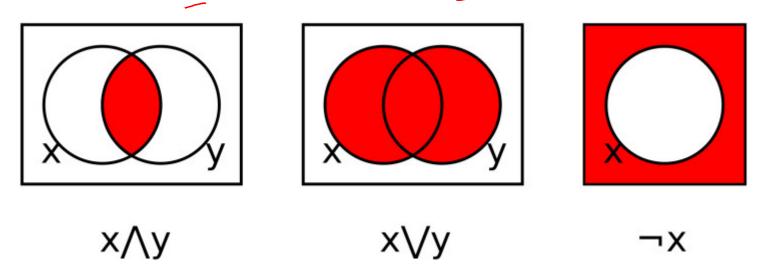
•
$$5 = 2 + 2 \text{ OR } 4 = 2 \times 2 \rightarrow \text{TRUE}$$

•
$$5 = 2^7 + 2 \text{ OR } 5 = 2 \times 2 \rightarrow \text{FALSE} \times$$

Venn Diagram

Symbols:

• Logical NOT (\neg) , logical AND (\land) , and logical OR (\lor)



https://en.wikipedia.org/wiki/Logical_connective

Negation of AND

Statement

Negation of AND is OR of negations:

Negation of "A AND B" is "Not A OR Not B"



Negation of AND

Statement

Negation of AND is OR of negations:

Negation of "A AND B" is "Not A OR Not B"

Negation of
$$4 = 2 + 2$$
 AND $4 = 2 \times 2$.

• $4 \neq 2 + 2$ OR $4 \neq 2 \times 2$. Note that AND

Introduction to Discrete Math

Logic - Logic

Negation of OR

Statement

Negation of OR is AND of negations:

Negation of "A OR B" is "Not A AND Not B"

Negation of OR

Statement

Negation of OR is AND of negations:

Negation of "A OR B" is "Not A AND Not B"

Negation of
$$4 = 2 + 2$$
 OR $5 = 2 \times 2$:

• $(4 \neq 2 + 2)$ AND $(5 \neq 2 \times 2)$

Intro to Discrete Structure

Reminder

- Everybody, make sure that your name in ZOOM is in the following format:
 - Ex: 202054321 Juan Dela Cruz

Not changing your name to this format

* you will be marked Absent * → absent?

* *

Introduction to Discrete Math

Logic - Logic

If-Then

Consider a promise:

• If there is an elephant in the refrigerator, then I'll give you 100,000 won.

Consider a promise:

 If there is an elephant in the refrigerator, then I'll give you 100,000 won.

The interesting case:

- There is no elephant in the refrigerator, but I gave you 100,000 won anyways, did I keep my promise?
- In terms of technical sciences, it is considered a kept promise, hence the statement is true

Introduction to Discrete Math

Logic - Logic

If-Then

Statement

 In general, the phrase "If P, Then Q" is true whenever either P is false or Q is true.

Statement

- In general, the phrase "If P, Then Q" is TRUE whenever either P is FALSE or Q is TRUE. T = (P=F)66(Q=7)
- If n = 6, then n is even \rightarrow TRUE
- If n = 5, then n is even \rightarrow FALSE
- If 1 = 2, then 2 = 3 is even \rightarrow TRUE
- If 1 = 2, then I am an elephant \rightarrow TRUE \rightarrow (122) to Not (F)

If-Then Generalization



- "If n is divisible by 4, then n is divisible by 2"
 - means "For all n, if n is divisible by 4, then n is divisible by 2"
 - statement is TRUE



- both "if" and "then" parts are true, statement is TRUE
- For any number *n* that is not divisible by 4 $\frac{P = F}{\sqrt{1 + \frac{1}{2}}}$
 - "if" part is false, statement is TRUE, no matter if n divisible by 2 or not

If-Then
$$n = \frac{4}{4} = \frac{n/4}{4}$$
 en n is divisible by 4^n $P = T$

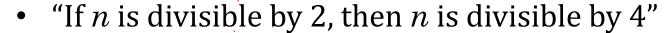
If-Then Generalization

- "If *n* is divisible by 2, then *n* is divisible by 4"
 - means "For all n, if n is divisible by 2, then n is divisible by 4"
 - statement is FALSE
- Because when n = 2, n is divisible by 2 but not by 4, hence
 - "if" part is true but "then" statement is false
 - statement is FALSE

Direct & Converse



direct statement



- converse statement
- When both direct ("If *P*, then *Q*") and converse ("If *Q*, then *P*") statements are true, they are equivalent to

$$-$$
 "P if and only if Q'





Negation of If-Then

- The negation of the phrase "If P, then Q" is "P and not Q"
- Check if it is true whenever the corresponding If-Then is false
- Check if it is false whenever the corresponding If-Then is true

Universal Quantification

- Statements that are examples of universal quantification:
 - All swans are white
 - All integers ending with the digit "2" are even
 - For all n, $2 \times n = n + n$
- Fermat's Last Theorem states that for all n > 2, equation $a^n + b^n = c^n$ does not have solutions with positive integers a, b, & c.
 - This is another example universal negation

antbr = c1 2 272

Existential Quantification

- Statements that are examples of existential quantification:
 - There are black swans
 - There is a way to get a change of 12 ewans with 4 ewan & 5 ewan coins
 - There exists such integers a, b, c, and d that $a^4 + b^4 + c^4 = d^4 \subseteq$
 - There exists a power of 2 starting with 65

Combination of Quantifiers

- Mathematical statements are usually combinations of universal and existential qualifications.
- Example is a corollary from Fermat's Last Theorem:
- Theorem:
 - There exists such integer m that for any integer n > m, equation $a^n + b^n = c^n$ has no solutions with positive integers a, b, and c.

Combination of Quantifiers

• Theorem: 🗲 🔾

- 44
- There exists such integer m that for any integer n > m, equation $a^n + b^n = c^n$ has no solutions with positive integers a, b, and c.
- If we take m=2, then it follows from Fermat's last theorem. It is a combination of
 - existential quantifier: "there exists such integer m" and
 - universal quantifier: "for any integer n > m..."

Combination of Quantifiers

- Theorem:
 - There exists such integer m that for any integer n > m, equation $a^n + b^n = c^n$ has no solutions with positive integers a, b, and c.
- If we take m=2, then it follows from Fermat's last theorem. It is a combination of
 - existential quantifier: "there exists such integer m" and
 - universal quantifier: "for any integer n > m..."

Introduction to Discrete Math

Logic - Logic

If-Then

- Negation of universal quantification is a corresponding existential quantification
- Negation of existential quantification is a corresponding universal quantification

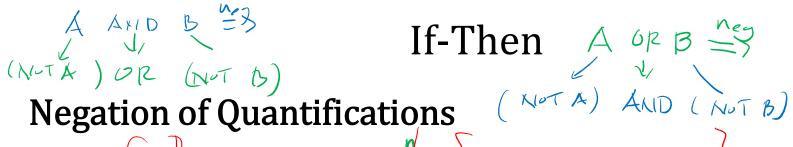
- Negation of universal quantification is a corresponding existential quantification
- Negation of existential quantification is a corresponding universal quantification
- Example: ५ 🛭
 - UQ: "For all n, statement A is true"
 - Negation of UQ: "There exists such n that statement A is false"

- Euler's hypothesis is a combination of two universal quantifications:
 - For any n > 3, for any positive integer a, it is impossible to represent a^n as a sum of n-1 numbers which are the n-th powers of positive integers.

- Euler's hypothesis is a combination of two universal quantifications:
 - For any n > 3, for any positive integer a, it is impossible to represent a^n as a sum of n-1 numbers which are the n-th powers of positive integers.
- Negation:
 - There exists such n > 3 and such positive integer a that a^n can be represented as a sum of n-1 numbers which are the n-th powers of positive integers.

Introduction to Discrete Math

Logic – Logic





- UQ: "All positive integers are either even OR odd"
- Negation: "There exists such positive integer n that is not even AND not odd"
- To negate:
 - We switch universal quantification (UQ) to existential qualification (EQ) and switch OR to AND
 - We switch existential quantification (EQ) to universal qualification (UQ) and switch AND to OR

- UQ: "All positive integers are either even OR odd"
- Negation: "There exists such positive integer n that is not even AND not odd"
- To negate:
 - We switch universal quantification (UQ) to existential qualification (EQ) and switch OR to AND
 - We switch existential quantification (EQ) to universal qualification (UQ) and switch AND to OR

Examples & Counterexamples

- Counterexample for Euler's hypothesis that was previously given is an example of negation
- By proving negation of Euler's hypothesis, we prove that the Euler's hypothesis itself is false

Reductio ad Absurdum

- A popular way of proving mathematical statements is through Reductio ad Absurdum
 - basically proving that the negation of the initial statement is false, hence the statement itself is true.
- We will study about this next

Mathematical Thinking – Reductio ad absurdum

REDUCTIO AD ABSURDUM

- Reduction ad absurdum
- Balls in Boxes
- Numbers in Boxes
- Pigeonhole Principle
- An(-1,0,1) Antimagic Square
- Handshakes

Reductio ad absurdum

Reductio ad absurdum

- How to prove that something is true?
- Show that the opposite is impossible
- Reductio ad absurdum
 - Proof by contradiction
- One of the base methods of reasoning
 - Used everywhere
- Often combined with other methods
- We will use constantly throughout the course

Reductio ad absurdum

Socratic Method

- Reductio ad absurdum is classic
 - Used in Socratic method (Plato, ~400BC)
- Socrates revealed contradictions in what his student believed
 - By asking them questions step-by-step



https://www.thoughtco.com/thmb/ZTk_AKXdOg904jzKDaqzk_jSvA=/768x0/filters:no_upscale():max_bytes(150000):strip_icc()/GettyImages-51242030-3fcdb51321cc4d49a89bd81a64e93a44.jpg

Reductio ad absurdum - Socratic Method

Socratic Method

• *Nontrivial* – Not obvious or easy to prove

Problem

 There are boys and girls in the class. They are divided into two groups for the foreign language: there are students studying French, and there are students studying German. Each student picks one of the two languages. Show that there is a boy and a girl who study different languages.

Seems impossible at first: we know basically nothing and we claim something nontrivial.

Reductio ad absurdum - Socratic Method

Socratic Method

Solution

• There are boys and girls in the class. They are divided into two groups for the foreign language: there are students studying French, and there are students studying German. Each student picks one of the two languages. Show that there is a boy and a girl who study different languages.

Reductio ad absurdum - Socratic Method

Socratic Method

Solution

• There are boys and girls in the class. They are divided into two groups for the foreign language: there are students studying French, and there are students studying German. Each student picks one of the two languages. Show that there is a boy and a girl who study different languages.

- G
- → some girls learn German

Socratic Method

Solution

• There are boys and girls in the class. They are divided into two groups for the foreign language: there are students studying French, and there are students studying German. Each student picks one of the two languages. Show that there is a boy and a girl who study different languages.

- G → some girls learn German
- $oxed{B}$ $oxed{B}$ ightarrow then all boys learn German

Socratic Method

Solution

• There are boys and girls in the class. They are divided into two groups for the foreign language: there are students studying French, and there are students studying German. Each student picks one of the two languages. Show that there is a boy and a girl who study different languages.

- G → some girls learn German
- $footnote{B}$ $footnote{B}$ o then all boys learn German
- \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc then all girls learn German

Socratic Method

Solution

• There are boys and girls in the class. They are divided into two groups for the foreign language: there are students studying French, and there are students studying German. Each student picks one of the two languages. Show that there is a boy and a girl who study different languages.

Our statement: there are no boy & no girl studying different languages. (Assume original statement is wrong)

- G → some girls learn German
- lacksquare lacksquare
- \hookrightarrow G G \longrightarrow then all girls learn German

Everyone learns German! It is a contradiction!

Therefore our assumption is wrong & original statement is true.

- Reduction ad absurdum
- Balls in Boxes
- Numbers in Boxes
- Pigeonhole Principle
- An(-1,0,1) Antimagic Square
- Handshakes

Balls in Boxes

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Reductio ad absurdum - Balls in Boxes

Balls in Boxes

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Reductio ad absurdum - Balls in Boxes

Balls in Boxes

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Reductio ad absurdum - Balls in Boxes

Balls in Boxes

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

1 2 ≥0 ≥1

1

3 **≥2**

4 ≥3 5 **≥4**

6 **≥5**

≥6

8

9

Problem

We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

1 ≥0

≥1

≥2

≥3

≥4

≥5

≥6

≥7

Problem

We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

1

≥8

10

≥0

≥1

≥2

≥3

≥4

≥5

≥6

≥7

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

1 ≥0 2 ≥1 3

4 ≥3 5

6

7

≥7

9

Reductio ad absurdum - Balls in Boxes

Balls in Boxes

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with increasing number of black balls.

Problem

 We have 10 boxes filled with lots of white balls. We additionally have 30 black balls. We want to distinguish boxes by placing different number of black balls in all of them. Can we do that?

Suppose we can do it. Let's see what will happen. Let us enumerate all boxes with

increasing number of black balls.

There is a contradiction.

Total number of balls is at least 45, 45 > 30.

Therefore our assumption is wrong. It cannot be done.

Reductio ad absurdum

- Reduction ad absurdum
- Balls in Boxes
- Numbers in Tables
- Pigeonhole Principle
- An(-1,0,1) Antimagic Square
- Handshakes

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

Introduction to Discrete Math

Reductio ad absurdum – Numbers in Boxes

Numbers in Boxes

Puzzle

 There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 30

Introduction to Discrete Math

Reductio ad absurdum - Numbers in Tables

Numbers in Boxes

Puzzle

 There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 30

Introduction to Discrete Math

Reductio ad absurdum - Numbers in Tables

Numbers in Boxes

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 7 30

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 7 10 30

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 7 10 13 30

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 7 10 13 16 30

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 7 10 13 16 19 30

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1 4 7 10 13 16 19 22 30

Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?



Puzzle

• There is a sequence of 10 cells. The leftmost contains "1" while the rightmost has "30". Is it possible to fill other cells with consecutive numbers in such a way that they differ by 3 at the most?

1

4

7

10

13

16

19

22

25

30

Suppose we can do it. Let's see what will happen

There is a contradiction.

The numbers in the cells grow too slow ⊗.

Therefore our assumption is wrong. It cannot be done.

This is a very common way to estimate running time of some algorithm.

Thank you.