CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

March 23, 2022

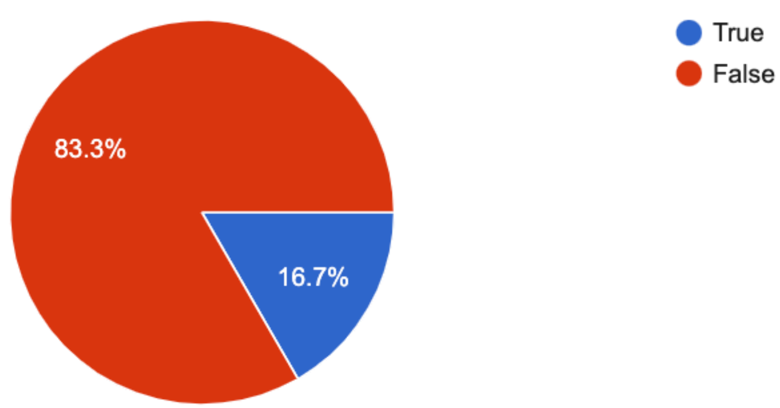
Many slides taken from Prof. Pramod Ganapathi (Stony Brook). Thanks!

Midterm exam feelings poll results

Anonymous Google form: https://forms.gle/ddi1TBYqNkdyqJ7v6

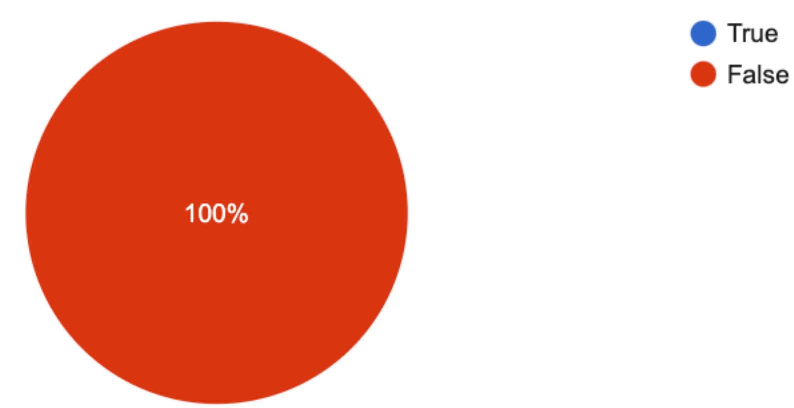
Problems are too easy

12 responses



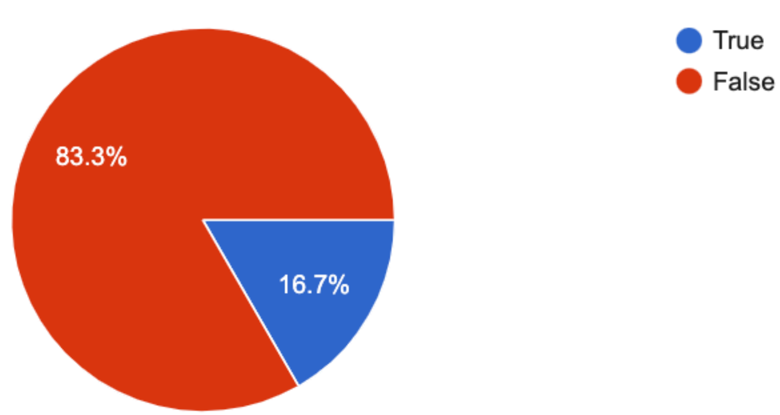
Problems are too few

12 responses



Problems are unclear

12 responses



Today

- Some definitions and facts about numbers
- Direct proof
- ~5 mins break.
- Exercises

To finish around 4h45 pm

Symbols

- Integers Z
- Natural numbers
- Real numbers R
- | x |
- sum Σ
- a | b
- b div a
- b mod a

Formal definitions

- Even/Odd numbers
- Rational/Irrational numbers
- Prime/Composite numbers

Even/odd numbers

We say an integer n is even if: $\exists k \in \mathbf{Z}$ such that $n = 2k$

How can you define an odd number?

Rational/Irrational numbers

We say a real number r is rational if $\exists m, n \in \mathbf{Z}$ such that $r = n/m$.

Prime/Composite numbers

We say a natural number n is prime if $n > 1$, and

$$\forall r, s \in \mathbf{N}, n = rs \to r = 1 \land s = n \lor s = 1 \land r = n.$$

d | n

We say a non-zero integer d divides an integer n, if

$$\exists k \in \mathbf{Z}, \text{ such that } n = k * d.$$

Unique prime factorization of natural numbers

n	Unique prime factorization
2	2
3	3
4	2^2
5	5
6	2×3
7	7
8	2^3
9	3^2
10	2×5
11	11
12	$2^2 \times 3$
13	13
14	2×7
15	3×5

n	Unique prime factorization
16	2^4
17	17
18	2×3^2
19	19
20	$2^2 \times 5$
21	3×7
22	2×11
23	23
24	$2^3 \times 3$
25	5^2
26	2×13
27	3^3
28	$2^2 \times 7$
29	29

n	Unique prime factorization
30	$2 \times 3 \times 5$
31	31
32	2^5
33	3×11
34	2×17
35	5×7
36	$2^2 \times 3^2$
37	37
38	2×19
39	3×13
40	$2^3 \times 5$
41	41
42	$2 \times 3 \times 7$
43	43

- What is the pattern?

Fact: Unique factorization of prime numbers

- Any natural number $n > 1$ can be uniquely represented as a product of as follows:

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$$

such that $p_1 < p_2 < \cdots < p_k$ are primes in $[2, n]$, $e_1, e_2, \ldots, e_k$ are whole number exponents, and k is a natural number.

- The theorem is also called fundamental theorem of arithmetic
- The form is called standard factored form

Fact: Quotient-remainder theorem

Theorem

- Given any integer n and a positive integer d, there exists an integer q and a whole number r such that

$$n = qd + r \text{ and } r \in [0, d-1]$$

Examples

- Let $n = 6$ and $d \in [1, 7]$

Num. (n)	Divisor (d)	Theorem	Quotient (q)	Rem. (r)
6	1	$6 = 6 \times 1 + 0$	6	0
6	2	$6 = 3 \times 2 + 0$	3	0
6	3	$6 = 2 \times 3 + 0$	2	0
6	4	$6 = 1 \times 4 + 2$	1	2
6	5	$6 = 1 \times 5 + 1$	1	1
6	6	$6 = 1 \times 6 + 0$	1	0
6	7	$6 = 0 \times 7 + 6$	0	6

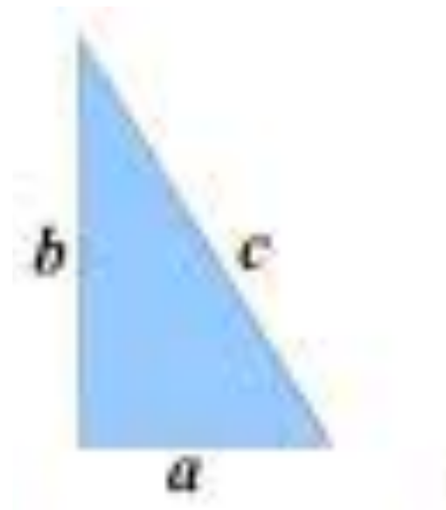
Direct proof

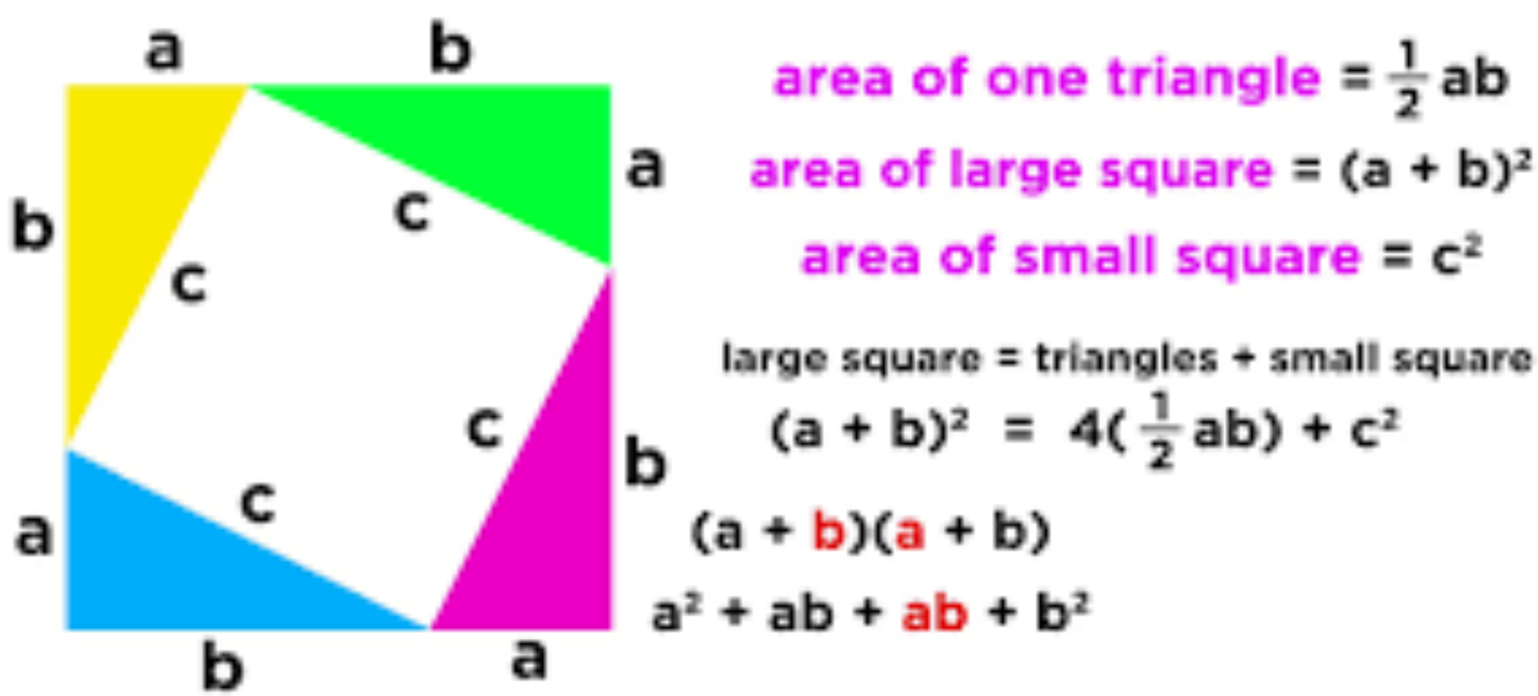
Methods of mathematical proof

Statements	Method of proof
Proving existential statements (Disproving universal statements)	Constructive proof Non-constructive proof
Proving universal statements (Disproving existential statements)	Direct proof Proof by mathematical induction Well-ordering principle Proof by exhaustion Proof by cases Proof by contradiction

PYTHAGORAS.

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





Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

Proof

- Suppose a is even and b is odd. Then

$$
\begin{aligned}
& a+b \\
&= (2m)+b && \text{(defn. of even, } a=2m \text{ for integer } m\text{)} \\
&= (2m)+(2n+1) && \text{(defn. of odd, } b=2n+1 \text{ for integer } n\text{)} \\
&= 2(m+n)+1 && \text{(taking 2 as common factor)} \\
&= 2p+1 && (p=m+n \text{ and addition is closed on integers)} \\
&= \text{odd} && \text{(defn. of odd)}
\end{aligned}
$$

n is odd $\Rightarrow n^2$ is odd

Proposition

- The square of an odd integer is odd.

Proof

- Prove: If n is odd, then n^2 is odd.

  n is odd

  $\Longrightarrow \; n = (2k+1)$ (defn. of odd, k is an integer)

  $\Longrightarrow \; n^2 = (2k+1)^2$ (squaring on both sides)

  $\Longrightarrow \; n^2 = 4k^2 + 4k + 1$ (expanding the binomial)

  $\Longrightarrow \; n^2 = 2(2k^2 + 2k) + 1$ (factoring 2 from first two terms)

  $\Longrightarrow \; n^2 = 2j + 1$ (let $j = 2k^2 + 2k$)

  (j is an integer as mult. and add. are closed on integers)

  $\Longrightarrow \; n^2$ is odd (defn. of odd)

Odd = difference of squares

Proposition

- Every odd integer is equal to the difference between the squares of two integers

Workout

- Write a formal statement.
  $\forall$ integer k, $\exists$ integers m, n such that $(2k+1) = m^2 - n^2$.
- Try out a few examples.

$$
\begin{aligned}
1 &= 1^2 - 0^2 & -1 &= 0^2 - (-1)^2 \\
3 &= 2^2 - 1^2 & -3 &= (-1)^2 - (-2)^2 \\
5 &= 3^2 - 2^2 & -5 &= (-2)^2 - (-3)^2 \\
7 &= 4^2 - 3^2 & -7 &= (-3)^2 - (-4)^2
\end{aligned}
$$

- Find a pattern.
  $(k+1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 =$ odd

Odd = difference of squares

Proposition

- Every odd integer is equal to the difference between the squares of two integers.

Proof

- Any odd integer can be written as $(2k+1)$ for some integer k.
- We rewrite the expression as follows.

  $2k+1$

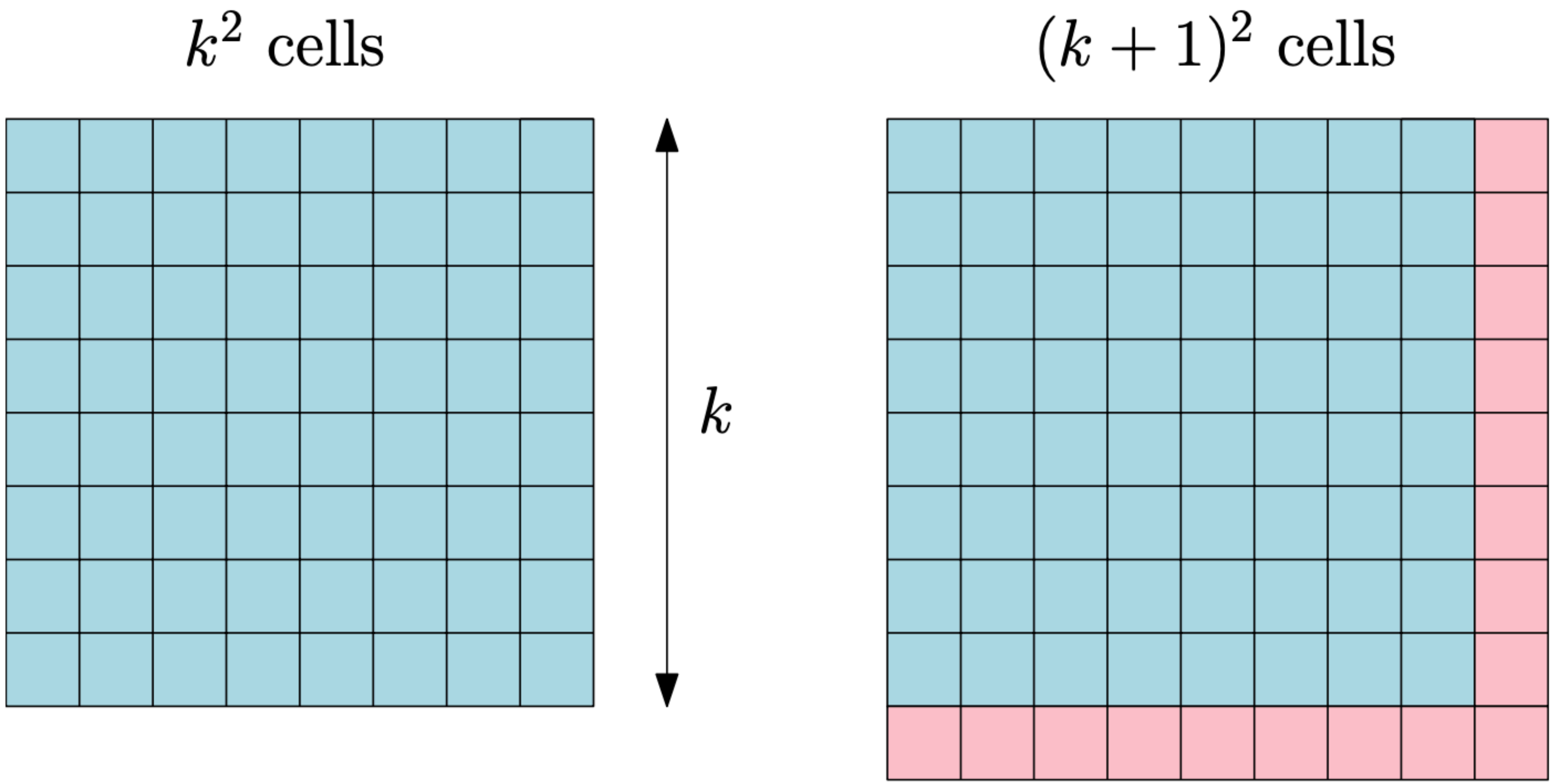
  $= (k^2+2k+1) - k^2$ (adding and subtracting k^2)

  $= (k+1)^2 - k^2$ (write the first term as sum)

  $= m^2 - n^2$ (set $m = k+1$ and $n = k$)

  The term m is an integer as addition is closed on integers.
- So, every odd integer can be written as the difference between two squares.

Odd = difference of squares



If $a|b$ and $b|c$, then $a|c$

Proposition

- (Transitivity) For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

Proof

- Formal statement.
  $\forall$ integers a, b, c, if $a|b$ and $b|c$, then $a|c$.
- $$\begin{aligned} & c \\ &= bn && (b|c \text{ and definition of divisibility}) \\ &= (am)n && (a|b \text{ and definition of divisibility}) \\ &= a(mn) && (\text{multiplication is associative}) \\ &= ak && (\text{let } k = mn \text{ and multiplication is closed on integers}) \\ &\implies a|c && (\text{definition of divisibility and } k \text{ is an integer}) \end{aligned}$$

Summation

Proposition

- $1 + 2 + 3 + \cdots + n = n(n+1)/2.$

Proof

- Formal statement. $\forall$ natural number n, prove that $1 + 2 + 3 + \cdots + n = n(n+1)/2.$
- $S = 1 + 2 + 3 + \cdots + n$

$$\implies S = n + (n-1) + (n-2) + \cdots + 1$$

(addition on integers is commutative)

$$\implies 2S = \underbrace{(n+1) + (n+1) + (n+1) + \cdots + (n+1)}_{n \text{ terms}}$$

(adding the previous two equations)

$$\implies 2S = n(n+1) \quad \text{(simplifying)}$$

$$\implies S = n(n+1)/2 \quad \text{(divide both sides by 2)}$$

Break ~ 5 minutes
Exercises

To finish by 4h45

Problem 4. [5 points]

Prove that the sum of the squares of any two consecutive odd integers is even.

Problem 5. [5 points]

Suppose that x and y are real numbers. Prove that $x = y$ if and only if $xy = (x + y)^2/4$.

That is all for today

- Proof techniques — direct proof
- Theory of Arithmetics

Thank you!