CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

October 05, 2022

Midterm 1 tomorrow

* Guideline
  Midterm Exam 1 (October 06, 2022, 12:30 pm - 01:50 pm)

  CSE 215: Foundations of Computer Science

  State University of New York, Korea, Fall 2022

  Instructor: Zhoulai Fu <zhoulai dot fu at sunykorea.ac.kr> or <zhoulai dot fu at stonybrook.edu>

  TA: Wonbin Kim <ownbin dot kim at stonybrook.edu>

  Format: Open-book. Open-notes. Open-Internet.

  Submit your answers in PDF on Blackboard. Multiple submissions are possible before the deadline. The last submission will be graded.

  If you use handwriting, try to make it easy to read.

  Do your own work; do not ask others. Violation of academic integrity will cause serious consequences.

Today

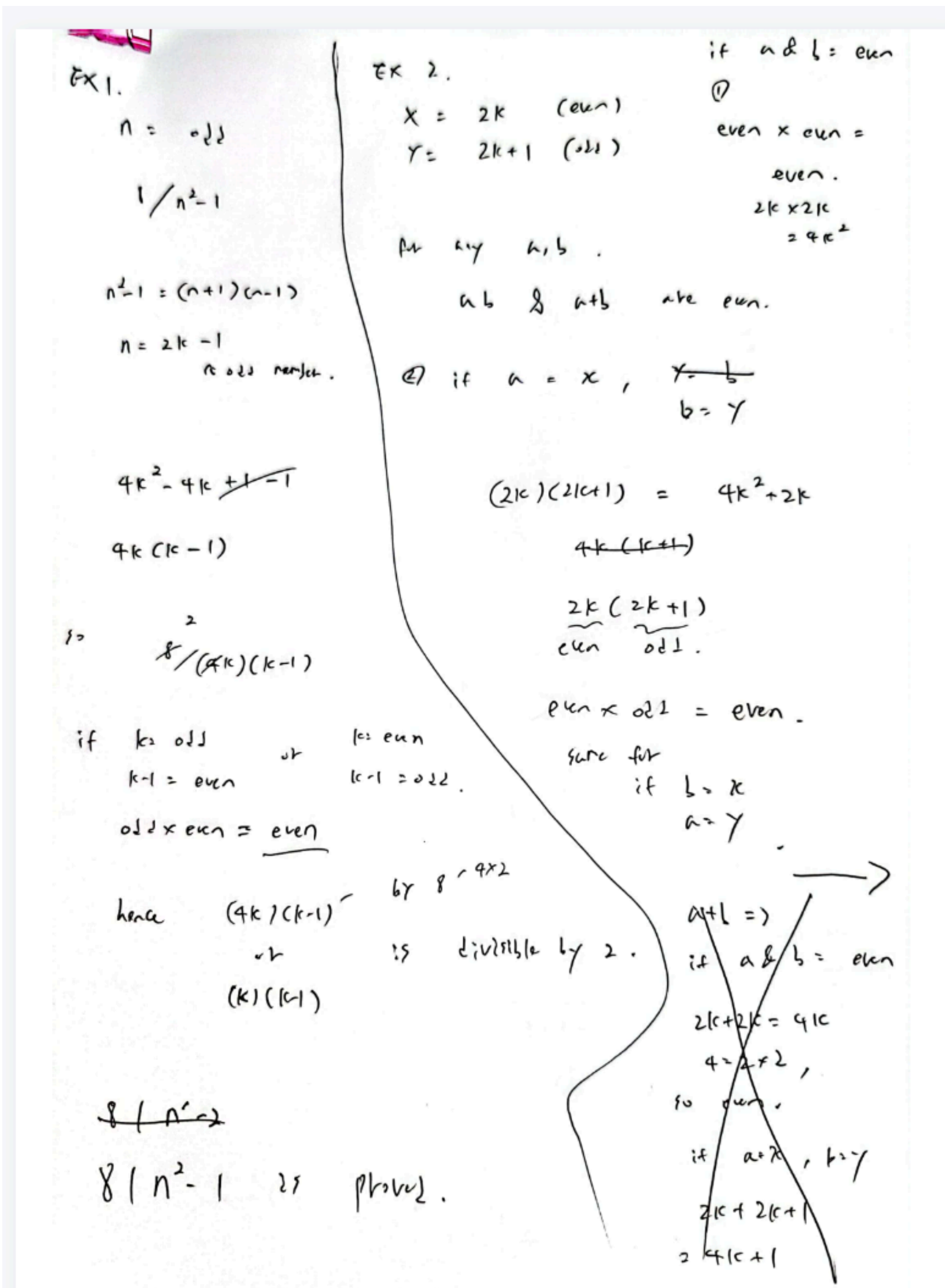
Homework 04

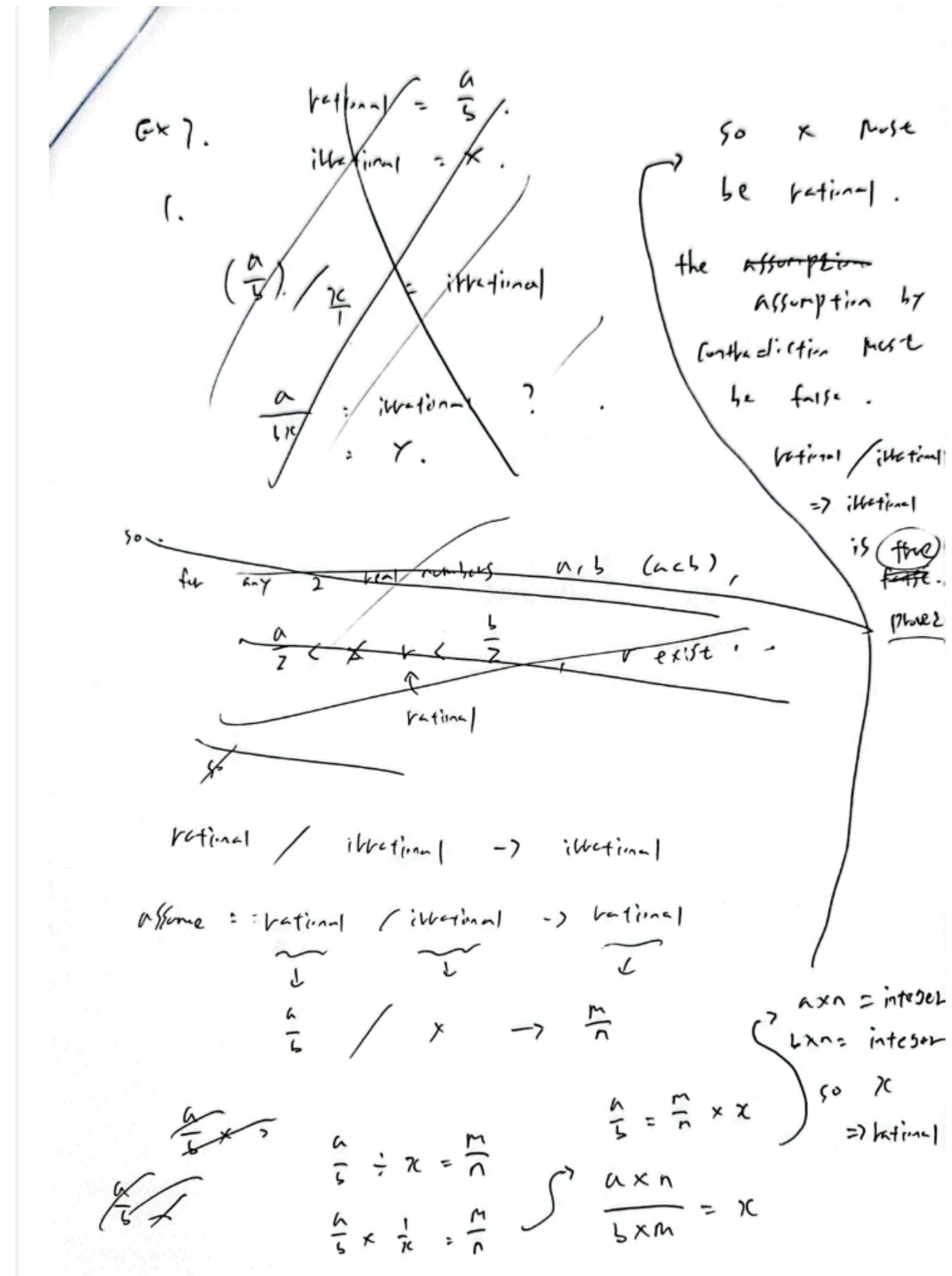
- To finish by 4h25

Exercise 1 (points = 10)

Prove: If n is odd, then 8|(n^2−1).

Not a proof


Ex 1.
n = odd
8 | n² - 1
n² - 1 = (n+1)(n-1)
n = 2k - 1
4k² - 4k
4k(k - 1)
if k = odd
k-1 = even
or
k = even
k-1 = odd.
odd x even = even
hence
is divisible by 2.
8 | n² - 1 is proved.
Ex 2.
X = 2k (even)
Y = 2k+1 (odd)
if a & b = even
even x even = even.
2k x 2k = 4k²
for any a, b.
ab & a+b are even.
if a = x,
b = Y
(2k)(2k+1) = 4k² + 2k
2k(2k+1)
even odd.
even x odd = even.
same for
if b = x
a = Y
if a & b = even


Ex 7.
rational = a/b.
irrational = x.
1.
irrational
?
so x must be rational.
the assumption by contradiction must be false.
rational / irrational => irrational is true
proved
rational
rational / irrational -> irrational
assume : rational / irrational -> rational
a/b / x -> m/n
a/b ÷ x = m/n
a/b x 1/x = m/n
a/b = m/n x x
a x n / b x m = x
a x n = integer
b x n = integer
so x => rational

Wrong solution

Exercise 1

Prove : If n is odd, then $8 \mid (n^2-1)$

Proof.

we want to prove : n is odd $\rightarrow 8 \mid (n^2-1)$

Let $n = 2k+1$ for some integer k

Wrong here —> Suppose $8 \mid (n^2-1)$,

$n^2-1 = 8k'$ for some integer k'

$(2k+1)^2 - 1 = 4k^2 + 4k = 4(k^2+k) = 8k'$

$k^2+k = k(k+1)$, even $\times$ odd $=$ even, thus k^2+k is always even.

so $k^2+k = 2a$ for some integer a.

$4(k^2+k) = 4(2a) = 8a = 8k'$

thus $8 \mid 8a$, $8 \mid (n^2-1)$.

QED.

Solution

Exercise 1

Suppose n is an odd number.

Then, $n = 2k + 1$, where k is some integer k.

Then, $n^2 - 1 = (2k + 1)^2 - 1$

$$= 4k^2 + 4k$$

$$= 4k(k + 1)$$

Since $k(k + 1)$ is always even, $k(k + 1) = 2m$, where m is some integer m.

Thus, $4k(k + 1) = 4 \cdot 2m = 8m$, which will always be divisible by 8.

QED.

Exercise 2 (points = 10)

Prove: For any integers a and b, if both ab and a+b are even, then both a and b are even.

Wrong Solution

Exercise 2.

Proof.

- a and b are any integer.
- Suppose both $a \cdot b$ and $a+b$ are even
- Thus, at least one of a or b is even.
- Suppose a is even.
- Then, b is even $\Rightarrow$ $a+b$ is even

  b is odd $\Rightarrow$ $a+b$ is odd.
- Thus, b is even.

Missing case —>

- Therefore a and b are even.

Solution

Exercise 2

We need to prove that for any $a, b \in Z$, if both ab and $a + b$ are even, then both a and b are even.

Proof by contraposition can be used to prove the given statement.

Suppose at least one of a and b is odd.

Then, we prove the contraposition by division into cases.

Case 1: a is even and b is odd

Then, $a = 2n$ and $b = 2m + 1$ for some integers n and m.

Then, $ab = 2n(2m + 1)$, which is even, and $a + b = 2n + 2m + 1$, which is odd.

So at least one of ab and $a + b$ is odd.

Case 2: a is odd and b is even

Then, $a = 2n + 1$ and $b = 2m$ for some integers n and m.

Then, $ab = (2n + 1)2m$, which is even, and $a + b = 2n + 1 + 2m$, which is odd.

So at least one of ab and $a + b$ is odd.

Case 3: a is odd and b is odd

Then, $a = 2n + 1$ and $b = 2m + 1$ for some integers n and m.

Then, $ab = (2n + 1)(2m + 1) = 4nm + 2n + 2m + 1$, which is odd,

and $a + b = 2n + 1 + 2m + 1 = 2(n + m + 1)$, which is even.

So at least one of ab and $a + b$ is odd.

Since all cases are true, the contraposition of the given statement is true.

Therefore, the given statement is true.

QED.

Exercise 3 (points = 30)

Determine which statements are true and which are false. Prove those that are true and disprove those that are false.

1. rational/irrational is irrational.
2. Irrational*irrational is irrational.
3. The sum of any two positive irrational numbers is irrational.
4. The square root of any rational number is irrational.

Solution

3.

1. False, 0/ sqrt(2) = 0, which means rational/irrational = rational in this case.

2. False, sqrt(2) * sqrt(2) = 2, which means irrational * irrational = rational in this case.

3. False, sqrt(2), 2-sqrt(2), sqrt(2) + {2-sqrt(2)} = 2, which means the sum of two positive irrational numbers is rational in this case.

4. False, sqrt(4) = 2, which means the square root of a rational number is also rational in this case.

Exercise 4 (points = 10)

Prove that there are no integers x and y such that $x^3 = 4y + 6$.

Wrong solution

4. $\forall x, y \in \mathbb{Z} : x^3 \neq 4y+6$

Prove by contradiction

$\exists x, y \in \mathbb{Z} : x^3 = 4y+6$

Suppose $x, y : x^3 = 4y+6$

$x^3 = 2(2y+3)$

$\Leftrightarrow x^3$ is even

so $x = 2K$ for some K

so $8K^3 = 4y+6$

$K^3 = \frac{1}{2}y + \frac{3}{4}$

$\therefore$ Both x and y cannot be integers.

No contradiction raised

Solution

Exercise 4

Suppose there exists integers x and y such that $x^3 = 4y + 6$.

Then, $x^3 = 4y + 6 = 2(2y + 3)$.

Since $2(2y + 3)$ is always even, x must be even.

So, $x = 2k$ for some integer k.

Then, $(2k)^3 = 2(2y + 3)$

$$8k^3 = 2(2y + 3)$$

$$4k^3 = 2y + 3$$

$4k^3$ is always even but $2y + 3$ is odd, which is a contradiction.

Therefore, the given statement is true.

QED.

Exercise 5 (points = 10)

Fermat's Last Theorem states that no three positive integers a, b, and c satisfy the equation a^n + b^n = c^n for any integer value of n greater than 2.

Now, prove:

- The cube root of 2 is irrational. (The cube root of a number a is a number b such that b*b*b=a.)

You can prove this either with Fermat's Last Theorem or not.

Solution

Exercise 5

Suppose the cube root of 2 is rational.

Then $\sqrt[3]{2} = \frac{p}{q}$, where p and q have no common factors.

$p = \sqrt[3]{2}q$

$p^3 = 2q^3p^3 = q^3 + q^3$

This is a contradiction due to the Fermat's Last Theorem.

Therefore, the given statement is true.

QED.

Exercise 6 (points = 20)

The quotient remainder theorem says: Given any integer A and a positive integer B, there exist unique integers Q and R such that A= B * Q + R where $0 \le R < B$. Examples:

- A = 7, B = 2: 7 = 2 * 3 + 1
- A = 8, B = 4: 8 = 4 * 2 + 0
- A = 13, B = 5: 13 = 5 * 2 + 3
- A = -16, B = 26 :-16 = 26 * -1 + 10

From the quotient-remainder theorem, we know that any integer divided by a positive integer will have a set number of remainders and thus a set number of representations. For example, any integer divided by 7 will produce a remainder between 0 and 6 (inclusive). So every integer n can be represented by one of the following forms: n=7q, n=7q+1, n=7q+2, n=7q+3, n=7q+4, n=7q+5, n=7q+6 (where q is an integer).

Now prove the following two propositions. Perhaps you can use the quotient remainder theorem.

1. The product of any four consecutive integers is a multiple of 8.
2. The square root of 3 is irrational.

Wrong solution

Exercise 6.

• The product of any four consecutive integers is a multiple of 8.

Suppose 4 consecutive integers are $n, n+1, n+2, n+3$.

n can be written as $4k$ for some integer k.

Then, $n(n+1)(n+2)(n+3) = 4k(4k+1)(4k+2)(4k+3) = 8(32k^4+48k^3+18k^2+3k)$

So the statement is true.

Assumption not valid

1) Proof.
suppose for consecutive integers
$n, n+1, n+2, n+3$
the product of four consecutive numbers be
$=(n^2+n)(n^2+5n+6)$
$=n^4+5n^3+6n^2+n^3+5n^2+6n$
$=n^4+6n^3+11n^2+6n$
When we suppose n as $1,2,3\ldots$
all the result is multiple of 8.

n	$n^4+6n^3+11n^2+6n$
1	$1+6+11+6=24$
2	$16+48+44+12=120$
3	$81+162+99+18=360$
⋮	⋮

therefore the product of any four consecutive integer is a multiple of 8
QED.

Prove for-all by examples

Confuse conclusion & assumption

Exercise 6.
the quotient remainder theorem:
$\forall A \in \mathbb{Z}, \forall B \in$ positive integer, $\exists Q, R$, $A = B*Q+R$, such that $0 \le R < B$.
Prove: the product of any 4 consecutive integers is a multiple of 8.
Proof.
We want to prove: $\forall x \in \mathbb{Z},\ 8 \mid (x-1)x(x+1)(x+2)$
Suppose $8 \mid (x-1)x(x+1)(x+2)$, so $(x-1)x(x+1)(x+2) = 8k$ for some integer k
so $(x-1)x(x+1)(x+2)$ is even, so $(x-1)x(x+1)(x+2) = 2k'$ for some integer k
so $2k' = 8k$, $k' = 4k$, so k' is even. so $k' = 2k''$ for some integer k''
so $4k'' = 8k$, $k'' = 2k$, so k' is even, so $k'' = 2k'''$ for some integer k'''
so $8k''' = 8k$
Therefore $8 \mid (x-1)x(x+1)(x+2)$
QED.

Solution

Exercise 6

- **The product of any four consecutive integers is a multiple of 8.**

Suppose $n \in Z$.
According to the quotient-remainder theorem, any integer n can be expressed as $n = 4k + r$, where k and r are some integers and $0 \leq r < 4$.
Therefore, we can consider 4 cases.

Case 1: $n = 4k$
Then, $4k(4k+1)(4k+2)(4k+3) = 8k(4k+1)(2k+1)(4k+3)$, which is divisible by 8.

Case 2: $n = 4k + 1$
Then, $$(4k+1)(4k+1+1)(4k+1+2)(4k+1+3) = (4k+1)(4k+2)(4k+3)(4k+4)$$
$$= 8(4k+1)(2k+1)(4k+3)(k+1)$$
, which is divisible by 8.

Case 3: $n = 4k + 2$
Then, $$(4k+2)(4k+2+1)(4k+2+2)(4k+2+3) = (4k+2)(4k+3)(4k+4)(4k+5)$$
$$= 8(2k+1)(4k+3)(k+1)(4k+5)$$
, which is divisible by 8.

Case 4: $n = 4k + 3$
Then, $$(4k+3)(4k+3+1)(4k+3+2)(4k+3+3) = (4k+3)(4k+4)(4k+5)(4k+6)$$
$$= 8(4k+3)(k+1)(4k+5)(2k+3)$$
, which is divisible by 8.

For all cases, the product of 4 consecutive numbers is divisible by 8.
Therefore, the given statement is true.
QED.

Suppose the square root of 3 is rational.
There exist integers m, n such that sqrt(3) = m/n (n is not 0, and gcd(m,n) =1)
3n^2 = m^2. 3 divides m^2, so 3 divides m. There exists an integer k such that m=3k.
Otherwise m=3k+1 and m^2 = 3(3k^2 + 2k) +1 or m= 3k+2 and m^2 =3(3k^2 +4k +1) +1. For both cases, m^2 is not divided by 3.
3n^2 = 9k^2
n^2 = 3k^2
For the same logic as before, n^2 is divided by 3 and n is also divided by 3.
We got a contradiction that gcd (m, n) =1 and m and n are both divided by 3.
Therefore, the square root of 3 is irrational.
QED

Exercise 7 (points = 10)

Before 1930, mathematicians were in the mindset that any true mathematical statement could be proved. That turned out to be wrong, as is later shown in Godel's incompleteness theorem, which shocked the whole community of mathematics and science. With the advent of computers, people once believed – informally speaking — that any mathematical problem can be solved with an algorithm. But later, Alan Turing proved that there are problems that absolutely no algorithms can solve. We now examine such a problem, known as the Halting Problem. We will use proof by contradiction to prove it is not solvable by any algorithm.

Imagine a computer program (or algorithm) called HaltCheck. Its purpose is to determine whether a program will halt or not. For example, a program may go into an infinite loop or recursive call, making it not halt. More specifically, HaltCheck reads a computer program P and an input x of the program, and HaltCheck (P, x) returns "halt" if P halts with the input x or "not halt" if P does not halt with that input.

Turing discovered that it is impossible to write HaltCheck as any algorithm. In other words, no computers can solve the halting problem. Turing proved so by constructing an artificial program that looks like the following:

```
prog(x):
    if HaltCheck (x, x) == "halt":
      go into an infinite loop
    else:
      return
```

Now, your job is to use proof by contradiction to prove the following:

1. HaltCheck (prog, prog) = "halt"
2. HaltCheck (prog, prog) = "not halt"

Solution

7. Suppose Haltcheck (prog, prog) = “halt”

That means prog(prog) halts somewhere.
However, if you look at prog(x), we go under Haltcheck (x, x) and an infinite loop turns out.
That means prog(prog) does not halt. Contradiction.

Now, suppose Haltcheck (prog, prog) = “not halt”
That means prog(prog) is an infinite loop.
However, if you look at prog(x), we go under else and prog halts.
prog (prog) halts and does not halt. Contradiction.