CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

Today

- Direct proof exercises and revision

Problem 4. [5 points]

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

- Proof.
  - We need to prove the following:
    - for any integer n, $(2n+1)^2 + (2n+3)^2$ is even.
  - Let n be an arbitrary integer.
  - We have $(2n+1)^2 + (2n+3)^2 = 8n^2 + 20n + 2 = 2(4n^2 + 10n+1)$ following algebraic Identities.
  - Therefore, $(2n+1)^2 + (2n+3)^2$ is even.
- QED.

Problem 5. [5 points]

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

- Proof.
  - Let x and y be two real numbers.
  - We need to prove
    - (1) $x = y \to xy = (x+y)^2/4$
    - (2) $xy = (x+y)^2/4 \to xy$
  - We first prove (1):
    - Suppose $x = y$
    - Therefore $xy = (x+y)^2/4$ following algebraic Identities
    - We have proved (1)
  - We then prove (2)
    - Suppose $xy=(x+y)^2/4$.
    - We have $x^2 - 2xy + y^2 = 0$, namely $(x-y)^2=0$, following algebraic Identities
    - Therefore $x=y$
    - We have proved (2)
- QED

Problem 5. Direct proof (points = 5)

Suppose a, b and c are integers. If $a^2 | b$ and $b^3 | c$, then $a^6 | c$.

- Proof.
    - Let a, b, and c be three integers.
    - Suppose $a^2 \mid b$ and $b^3 \mid c$
    - By definition, we have $b = k a^2$ for some integer k, and $c = k' b^3$ for some integer k'.
    - Thus, $c = (k' k^3) a^6$
    - Therefore $a^6 \mid c$.
- QED

Templates for Direct proof

- Start with “Proof.” and what needs to be proven if it is not extremely clear. End with “QED.”
- How to prove “If A, then B”
  - Suppose A, … Therefore B.
- How to prove “for all real number x, P(x)”
  - Let x be a real number. …Therefore P(x).
- How to prove “for all real number x, P(x) -> Q(x) ”
  - Let x be a real number. Suppose P(X). … Therefore Q(x).
- How to prove “there exist x, P(x)”
  - Let x be <something you choose>. …. We have P(x) holds.

Tips for writing a proof

- Core principle: AS CLEAR AS POSSIBLE.
- When using handwriting, envision it being read by a grandparent.
- Adhere to the provided templates but be prepared to make minor adjustments.
- Link your arguments using words such as "Let," "Suppose," "We have," "Thus," "Therefore," and "Following."
- It's alright to use drawings or diagrams to explain your proof, but ensure to provide comprehensive English explanations alongside them at all times.

Additional Exercises on Direct Proof

Review exercise 1

Prove $2^{999}+1$ is composite

Review exercise 1

Prove $2^{999}+1$ is composite

- Proof.
  - $2^{999}+1$
    $= (2^{333})^3 + 1^3$
    $= (2^{333}+1) * (2^{666}-2^{333}+1)$
- QED.

Review exercise 2

Prove: For any natural number n, $n^2 + 3n + 2$ is composite

Review exercise 2

Prove: For any natural number n, $n^2 + 3n + 2$ is composite

- Proof.
    - Suppose n is an arbitrary integer.
    - $n^2 + 3n + 2$ can be written as $(n+1)*(n+2)$
    - Thus, $n^2 + 3n + 2$ is a composite number
- QED.

Review exercise 3

For any integer x, y, if x is even, then xy is even.

Review exercise 3

For any integer x, y, if x is even, then xy is even.

Proof. Suppose $x, y \in \mathbb{Z}$ and x is even.
Then $x = 2a$ for some integer a, by definition of an even number.
Thus $xy = (2a)(y) = 2(ay)$.
Therefore $xy = 2b$ where b is the integer ay, so xy is even. ■

Review exercise 4

Prove: there exist two irrational number r1, r2, such that r1*r2 is a rational number.

Review exercise 4

Prove: there exist two irrational number r1, r2, such that r1*r2 is a rational number.

- Proof.
  - Let r1 and r2 be square root of 2.
  - r1 and r2 are irrational, and r1*r2 is rational.
- QED.

Review exercise 5

Prove: Suppose a is an integer. If $7|4a$, then $7|a$.

Review exercise 5

Prove: Suppose a is an integer. If 7|4a, then 7|a.

Proof. Suppose $7 \mid 4a$.
By definition of divisibility, this means $4a = 7c$ for some integer c.
Since $4a = 2(2a)$ it follows that $4a$ is even, and since $4a = 7c$, we know $7c$ is even.
But then c can't be odd, because that would make $7c$ odd, not even.
Thus c is even, so $c = 2d$ for some integer d.
Now go back to the equation $4a = 7c$ and plug in $c = 2d$. We get $4a = 14d$.
Dividing both sides by 2 gives $2a = 7d$.
Now, since $2a = 7d$, it follows that $7d$ is even, and thus d cannot be odd.
Then d is even, so $d = 2e$ for some integer e.
Plugging $d = 2e$ back into $2a = 7d$ gives $2a = 14e$.
Dividing both sides of $2a = 14e$ by 2 produces $a = 7e$.
Finally, the equation $a = 7e$ means that $7 \mid a$, by definition of divisibility. ■

That is all for today

- Direct proof exercises and revision
- Practice, practice, and practice

Thank you!