

CSE215

Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

March 28, 2022

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

Agenda

- Last lecture: Direct proof.
- This lecture: (1) Proof by contradiction (2) proof by division
- Very much appreciated questions during last class

Review: Direct Proof

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

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

Proof by contradiction



**Prove: There is no greatest
integer**

Proposition

- There is no greatest integer.

Proof

- **Negation.** Suppose there is a greatest integer N .
Then $N \geq n$ for every integer n .
Let $M = N + 1$.
 M is an integer since addition is closed on integers.
 $M > N$ since $M = N + 1$.
 M is an integer that is greater than N .
So, N is not the greatest integer.
Contradiction! Hence, the proposition is true.

n^2 is even $\implies n$ is even

Proposition

- For all integers n , if n^2 is even, then n is even.

Proof

- **Negation.** Suppose there is an integer n such that n^2 is even but n is odd.
- $n = 2k + 1$ (definition of odd number)
 $\implies n^2 = (2k + 1)^2$ (squaring both sides)
 $\implies n^2 = 4k^2 + 4k + 1$ (expand)
 $\implies n^2 = 2(2k^2 + 2k) + 1$ (taking 2 out from two terms)
 $\implies n^2 = 2m + 1$ (set $m = 2k^2 + 2k$)
(m is an integer as multiplication is closed on integers)
 $\implies n^2 = \text{odd}$ (definition of odd number)
- Contradiction! Hence, the proposition is true.

$\sqrt{2}$ is irrational

Proposition

- $\sqrt{2}$ is irrational.

Proof

- Suppose $\sqrt{2}$ is the simplest rational.
 - $\implies \sqrt{2} = m/n$ (m, n have no common factors, $n \neq 0$)
 - $\implies m^2 = 2n^2$ (squaring and simplifying)
 - $\implies m^2 = \text{even}$ (definition of even)
 - $\implies m = \text{even}$ (why?)
 - $\implies m = 2k$ for some integer k (definition of even)
 - $\implies (2k)^2 = 2n^2$ (substitute m)
 - $\implies n^2 = 2k^2$ (simplify)
 - $\implies n^2 = \text{even}$ (definition of even)
 - $\implies n = \text{even}$ (why?)
 - $\implies m, n$ are even (previous results)
 - $\implies m, n$ have a common factor of 2 (definition of even)
- Contradiction! Hence, the proposition is true.

for any prime number p

If $p|n$, then $p \nmid (n + 1)$.

for any prime number p

If $p|n$, then $p \nmid (n + 1)$.

Proposition

- For any integer n and any prime p , if $p|n$, then $p \nmid (n + 1)$.

Proof

- **Negation.** Suppose there exists integer n and prime p such that $p|n$ and $p|(n + 1)$.
 $p|n$ implies $pr = n$ for some integer r
 $p|(n + 1)$ implies $ps = n + 1$ for some integer s
Eliminate n to get:
 $1 = (n + 1) - n = ps - pr = p(s - r)$
Hence, $p|1$, from the definition of divisibility.
As $p|1$, we have $p \leq 1$.
As p is prime, $p > 1$.
Contradiction! Hence, the proposition is true.

(why?)

#Primes is infinite

Proposition

- The set of prime numbers is infinite.

Proof

- **Negation.** Assume that there are only finite number of primes. Let the set of primes be $\{p_1, p_2, \dots, p_n\}$ such that $(p_1 = 2) < (p_2 = 3) < \dots < p_n$. Consider the number $N = p_1 p_2 p_3 \dots p_n + 1$. Clearly, $N > 1$.
 - (i) There is a prime that divides N .
Use **unique prime factorization theorem**.
 - (ii) No prime divides N .
For all $i \in [1, n]$, p_i does not divide N as it leaves a remainder of 1 when it divides N .
So, $p_1 \nmid N, p_2 \nmid N, \dots, p_n \nmid N$.
Contradiction! Hence, the proposition is true.

**A special kind of proof by
contradiction — proof by
contraposition**

n^2 is even $\implies n$ is even

- Proposition, for all integer n , n^2 even $\rightarrow n$ even
- Equivalently, for all integer n , n is odd $\rightarrow n^2$ is odd

Break 5 min?

**Proof by
division into cases**

To finish around 4h45

$n^2 + 3n + 2$ is composite

1. **Prove that n is even $\implies n^2 + 3n + 2$ is composite.**

n is even

$\implies n^2$ is even and $3n$ is even (even \times integer = even)

$\implies n^2 + 3n + 2$ is even (even + even = even)

$\implies n^2 + 3n + 2$ is composite (2 is a factor)

2. **Prove that n is odd $\implies n^2 + 3n + 2$ is composite.**

n is odd

$\implies n^2$ is odd and $3n$ is odd (odd \times odd = odd)

$\implies n^2 + 3n$ is even (odd + odd = even)

$\implies n^2 + 3n + 2$ is even (even + even = even)

$\implies n^2 + 3n + 2$ is composite (2 is a factor)

Exercises

Rational + irrational = irrational. [Hint: Contradiction.]

Let n be a positive integer. Prove that the closed interval $[n, 2n]$ contains a power of 2. [Hint: Division into cases (power of 2 and not a power of 2).]

Problem 4. [5 points]

Prove that $n^2 + 9n + 27$ is odd for all natural numbers n . You can use any proof technique.

Problem 6. [5 points]

Prove that if $n^2 + 8n + 20$ is odd, then n is odd for natural numbers n .

That is all for today

- proof by contradiction
- Proof by division
- Practice, practice, and practice

Thank you!