# CS 30: Discrete Math in CS (Winter 2019): Lecture 2

Date: 4th January, 2019 (Friday)
Topic: Proofs by Contradiction
*Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.*
*Please discuss in Piazza/email errors to deeparnab@dartmouth.edu*

## 1 Proofs by Contradiction

This is one of the most commonly used styles of proof. When faced with a proposition $P$ which we wish to prove true, we *suppose for the sake of contradiction* that $P$ were false. Then we logically deduce something *absurd* (like $0 = 1$ or $3$ is even), that is, something which we know to be false. This implies that our supposition (which is, $P$ is false) must be wrong. Therefore, the proposition $P$ must be true. This method of proving is also called *reductio ad absurdum*; reducing to something absurd.

For this lecture, we will be tedious and itemize our proofs (hopefully) for clarity's sake. There is no need for this and paragraph answers are fine. We just need to ensure that what we write in a line logically follows from what we have written before.

- **A Simple Warm-up.**

  **Lemma 1.** For all numbers $a$, if $a^2$ is even, then $a$ is even.

  *Proof.*

  1. Suppose, for the sake of contradiction, the proposition is *not true*.
  2. That is, there exists a number $a$ such that $a^2$ is even but $a$ is not even. That is, $a$ is odd.
  3. So $a = 2k + 1$ for some integer $k$.
  4. But this implies $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. That is, $a^2$ is odd. This is a contradiction to the assumption that $a^2$ is odd.
  5. Therefore, our supposition must be wrong, that is, the proposition is true.

  □

  ✍

  **Exercise:** *Mimic the above proof to prove: For any number $a$, if $a^2$ is divisible by $3$, then $a$ is divisible by $3$.*

  ✍

  **Exercise:** *Prove by contradiction: the product of a* non-zero *rational number and an irrational number is irrational.*

- **A Pythogorean[1] Theorem.**

[1] This is of course not the famous Pythogorean theorem on right angled triangles, but nonetheless a Pythogorean may be the first to have proved it. See https://en.wikipedia.org/wiki/Irrational_number, for instance.

**Theorem 1.** $\sqrt{2}$ is irrational.

*Proof.*

1. Suppose, for the sake of contradiction, that $\sqrt{2}$ is indeed rational.
2. Since $\sqrt{2}$ is rational, there exists two integers $a, b$ such that $\sqrt{2} = a/b$.
3. By dividing out common factors, we may assume $\gcd(a, b) = 1$.
4. Since $a/b = \sqrt{2}$, we get $a = \sqrt{2} \cdot b$. Squaring both sides, we get $a^2 = 2b^2$.
5. Therefore $a^2$ is even.
6. Lemma 1 implies that $a$ is even. And therefore $a^2$ is divisible by $4$ (drill).
7. Therefore, $a^2 = 4k$ for some number $k$.
8. Since $a^2 = 2b^2$, we get $4k = 2b^2$, which in turn implies $b^2 = 2k$. That is, $b^2$ is even.
9. Lemma 1 implies that $b$ is even. But this **contradicts** $\gcd(a, b) = 1$.
10. Thus, our supposition that $\sqrt{2}$ is rational must be wrong. Therefore, $\sqrt{2}$ is rational.

□

✍

**Exercise:** *Mimic the above proof to prove that $\sqrt{3}$ is irrational. How far can you generalize? Can you prove that $\sqrt{n}$ is irrational if $n$ is not a* perfect square, *that is, $n$ is not $a^2$ for some integer $a$?*

- **A Euclidean Theorem.** Here is another classic example of Proof by Contradiction.

**Theorem 2.** There are infinitely many primes.

*Proof.*

1. Suppose, for the sake of contradiction, there were only finitely many primes. Suppose there are $N$ of them.
2. Order these $N$ primes in increasing order and let $q$ be the largest prime. Therefore any number $n > q$ is *not* a prime.
3. Consider the number $n = q! + 1$. Recall, $q! = 1 \times 2 \times \cdots \times q$.
4. To get the contradiction, observe two things.
   - One, $n > q$ and therefore, $n$ is not a prime. Therefore, $n$ *must be divisible* by some prime (indeed, it can be uniquely written as a product of primes). Since all the primes are less than or equal to $q$, we get that *$n$ is divisible by some number from $2$ to $q$*.
   - Two, $n$ is *not divisible by any number from $2$ to $q$*. This is because $q!$ *is* divisible by any number from $2$ to $q$, and therefore $n = q! + 1$ must leave a remainder $1$.
5. We have obtained a contradiction. Therefore, our supposition was wrong. There are infinitely many primes.

□