CSCI 2824 - CU Boulder, 2019 Summer

Lecture 8: More Proof Writing!

13 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications and Andrew Altomare's notes.

1 Review

- Proof by cases
- Proof by contradiction
- Proof by contrapositive

2 Irrationality of $\sqrt{2}$

Theorem 2.1. *$\sqrt{2}$ is irrational.*

Proof. Suppose not, i.e. $\sqrt{2}$ is rational. Then, $\exists m, n \in \mathbb{Z}$ with no common factors and $n \neq 0$ such that $\sqrt{2} = \frac{m}{n}$. Then, squaring both sides yields $2 = \frac{m^2}{n^2}$. Equivalently, $m^2 = 2n^2$. This implies that m^2 is even. It follows that m is even. So $m = 2k$ for some integer k. Then, $m^2 = (2k)^2 = 4k^2 = 2n^2$. Dividing both sides by two yields that $n^2 = 2k^2$. Therefore, n^2 is even, and so is n. But then they share a common factor of 2, a contradiction. $\square$

Exercise
Prove: $1 + 3\sqrt{2}$ is irrational.

3 Infinitude of primes

Remember that little kid example from before? Let's finally prove that there infinitely many primes.

Theorem 3.1. *For any integer a and any prime number p, if $p|a$ then $p \nmid (a+1)$.*

Proof. Suppose not, i.e. $\exists a \in \mathbb{Z}$ and a prime number p such that $p|a$ and $p|(a+1)$. Then, by definition of divisibility there exists integers r and s such taht $a = pr$ and $a + 1 = ps$. Then,

$$1 = (a+1) - a = ps - pr = p(s-r)$$

and so (since $s - r$ is an integer) $p|1$. But, by a previous theorem the only integer divisors of 1 are 1 and -1, and $p > 1$ because p is prime. Thus, $p \leq 1$ and $p > 1$, which is a contradiction. □

Theorem 3.2. *The set of prime numbers if infinite.*

Proof. Suppose not, i.e. the set of prime numbers is finite. Then, some prime number p is the largest of all prime numbers and we can list the primes in ascending order $2, 3, 5, 7, 11, \ldots, p$. Let N be the product of all the prime numbers plus 1, $N = (2 \times 3 \times 5 \times \ldots \times p) + 1$. Then, $N > 1$ and so by our previous work N is divisible by some prime number q. Because q is prime, q must equal one of the prime numbers $2, 3, 5, \ldots, p$. Thus, by definition of divisibility $q|N - 1$ and by the previous theorem it does not divide N. Hence, N is divisible by q and is not divisible by q, a contradiction. □

4 Division algorithm

See book.