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 In-class practice

Theorem 1.1. $\forall n \in \mathbb{N}\ \left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\ldots\left(1+\frac{1}{n}\right) = n+1$

Proof. We first note that $\left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\ldots\left(1+\frac{1}{n}\right)$ can be rewritten as $\prod_{k=1}^{n} 1+\frac{1}{k}$. Let S_n be the statement $\prod_{k=1}^{n} 1+\frac{1}{k} = n+1$. We will prove this statement by induction, so we first consider the base case S_1. Note that for $n=1$ the left hand side simplifies $\prod_{k=1}^{1} 1+\frac{1}{1} = 1+1 = 2$ and the right hand side $1+1=2$. Therefore S_1 holds. Our inductive hypothesis indicates that S_m holds for some arbitrary $m \in \mathbb{Z}$ where $m \geq 1$. Thus, $\prod_{k=1}^{m} 1+\frac{1}{k} = m+1$. We consider statement S_{m+1}:

$$\begin{aligned}
\prod_{k=1}^{m+1} 1+\frac{1}{k} &= \left(\prod_{k=1}^{m} 1+\frac{1}{k}\right)\left(1+\frac{1}{m+1}\right) && \text{separating a term off} \\
&= (m+1)\left(1+\frac{1}{m+1}\right) && \text{using } S_m \\
&= m+1+\frac{m+1}{m+1} && \text{algebra} \\
&= (m+1)+1
\end{aligned}$$

This is what we wished to show. Thus, the inductive step is complete and the theorem holds. □

Theorem 1.2. *Suppose a sequence $a_0, a_1, a_2, a_3, \ldots$ is defined as follows:*

- $a_0 = 0$
- $a_1 = 1$
- *For $n \geq 2$, $a_n = 2a_{n-1} - a_{n-2} + 2$*

Then, $a_n = n^2$. (We found this after some trial and error.)

Proof. We will proceed by induction on the statement S_n that "For $n \in \mathbb{N}$, the recurrent formula and the closed formula are equivalent." First consider the base case, $n = 0$. Note, $a_0 = 0$ is defined in the recurrence relation and that $0^2 = 0$ for the closed expression.

By the inductive hypothesis, for arbitrary $m \in \mathbb{N}$ we know all S_k hold for $1 \leq k \leq m$. (We really only need S_m and S_{m-1}, but we'll just take them all since they're free.) Consider S_{m+1}. Working from the recurrence relation, we observe:

$$\begin{aligned} a_{m+1} &= 2a_m - a_{m-1} + 2 && \text{definition} \\ &= 2m^2 - a_{m-1} + 2 && \text{by } S_m \\ &= 2m^2 - (m-1)^2 + 2 && \text{by } S_{m-1} \\ &= 2m^2 - m^2 + 2m - 1 + 2 && \text{by expansion} \\ &= m^2 + 2m + 1 && \text{simplification} \\ &= (m+1)^2 && \text{factored} \end{aligned}$$

Therefore, we have shown that $S_1 \wedge S_2 \wedge \ldots \wedge S_m \to S_{m+1}$ and have completed the inductive step. Thus, the theorem holds by strong induction. □

Theorem 1.3. *In a basketball game with no fouls, players may score 2-point goals or 3-point goals. Prove that any number $n \geq 2$ of points may be scored in a basketball game with no fouls.*

Proof. The number of points scored could be even or odd. If even, then $\exists k \in \mathbb{Z}$ such that $n = 2k$. Thus, the team could score k 2-point goals to attain that score. If n is odd, then $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$. If the team scores $k - 1$ 2-point goals and 1 3-point shot, then they get $2(k-1) + 3(1) = 2k - 2 + 3 = 2k + 1 = n$ points and thus attain the goal. Therefore, regardless of n's parity, the score can be attained with only 2-point and 3-point goals. □

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. □

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 $p \not| (a+1)$.*

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. $\square$

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. $\square$