CSCI 2824 - CU Boulder, 2019 Summer

Lecture 6: Rational Number Proofs, Divisibility, and Induction

11 June 2019

Lecturer: J. Marcus Hughes

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

1 Review

We learned about writing proofs. Let's practice with some ideas on rational numbers and divisibility.

2 Rational Number Proofs

What is a rational number? You may have heard it defined as a decimal that terminates or repeats in your early math days, but we are going to use a more formal definition.

Definition: *Rational Number*
A (real) number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is is **irrational**. More formally, if r is a real number, then

$$r \text{ is rational} \leftrightarrow \exists a, b \in \mathbb{Z} \text{ such that} r = \frac{a}{b}, b \neq 0$$

What are some examples of rational numbers? Well integers are! Let's prove it.

Theorem 2.1. *Every integer is a rational number*

Proof. Let n be an arbitrary integer. Then $n = \frac{n}{1}$ so n is a rational number. □

It's quite straight forward, but we are utilizing the idea of the generic particular. We do not specify what n is but show that for any arbitrary n we can make this argument. Seems pretty straight forward.

Now, try applying the same idea to show that any sum of rational numbers is rational.

Theorem 2.2. *The sum of two rational numbers is rational.*

Proof. Suppose r and s are rational numbers. Then, by the definition of rational, $r = a/b$ and $s = c/d$ for some $a, b, c, d \in \mathbb{Z}$ where $b \neq 0$ and $d \neq 0$. Thus,

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad + bc}{bd} \end{aligned}$$

Let $p = ad + bc$ and $q = bd$. Then, p and q are integers because products and sums of integers are integers and because $a, b, c, d \in \mathbb{Z}$. Also $q \neq 0$ by the zero product property. Thus, $r + s = \frac{p}{q}$ where p and q are integers and $q \neq 0$. Therefore, $r + s$ is rational by the definition of a rational number. $\square$

We can thus say that the rational numbers are closed under addition. Closed (in computer science lingo) means that performing that operation with a given input type always yields the same output type.

Can you show that any integer multiple of a rational number is rational? Is the product/quotient/difference of any two rational numbers also rational? What about the average?

3 Divisibility

Do you remember in elementary school when you talked about division? You knew that 12 wasn't divisible by 5 since it didn't go into it evenly. It may seem simplistic, but divisibility is a central idea in number theory; something so elementary is in advanced math! We can practice our proof writing skills in this domain too.

Definition: *Divisible*
If n and d are integers and $d \neq 0$ then, n is **dibisible by** d if, and only if, n equals d times some integer. The notation $d|n$ is read "d divides n". Symbolically for $n, d \in \mathbb{Z}$ and $d \neq 0$:

$$d|n \leftrightarrow \exists k \in \mathbb{Z} \text{ such that} n = dk$$

We call a number the divides another number a divisor of it. What do we know about divisors.

Exercise
For all integers a and b, if a and b are positive and $a|b$, then $a \leq b$.

The above is a nice universal proof to know.

Exercise
Prove: The only divisors of 1 are 1 and -1.

Exercise
Problem: For all integers a, b, and c if a divides b and b divides c, then a divides c.

Exercise
Prove: Any integer $n > 1$ is divisible by a prime number.

Is the following statement true? For all integers a and b if $a|b$ and $b|a$ then $a = b$. No. find a counterexample with $a = 2$ and $b = -2$.

A very powerful theorem is:

Theorem 3.1. *Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots, e_k$ such that $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ and any other expression for n as a product of prime numbers is identical to this, except, perhaps, for the order in which the factors are written. We call this the standard factored form of n when $p_1 < p_2 < \ldots < p_k$.*

We will come back to proving this later.

4 Mathematical Induction

We introduced the idea of mathematical induction yesterday. We will define two forms of

Definition: *Weak Induction*
Let S_n denote a statement regarding an integer n and let $k \in \mathbb{Z}$ be fixed. If

1. S_k holds and
2. for every $m \geq k$, $S_m \rightarrow S_{m+1}$

then for every $n \geq k$, the statement S_n holds.

Definition: *Strong Induction*
Let S_n denote a statement regarding an integer n. If

1. S_k holds and
2. For every $m \geq k$, $[S_k \wedge S_{k+1} \wedge \ldots \wedge S_m] \rightarrow S_{m+1}$

then for every $n \geq k$, the statement S_n is true.

Exercise
Show that strong and weak induction are equivalent.

Exercise
Prove that $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Exercise
Conjecture a formula for the sum of the first n positive odd integers. Then prove your conjecture using mathematical induction.

Exercise
Use mathematical induction to show that $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$.

Exercise
Prove that for all $n \in \mathbb{Z}^+$ that $3|n^3 - 3$.

References