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. □

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 $a \leq b$.

Suppose $a, b \in \mathbb{Z}^+$ and $a|b$. Then, $\exists k \in \mathbb{Z}$ such that $b = ak$. From algebra (Property T25 of Appendix A), k must be positive because both a and b are positive. Then, $1 \leq k$ because every positive integer is greater than or equal to 1. Multiplying both sides by a gives $a \leq ka = b$ because multiplying both sides of an inequality by a positive number preserves the inequality property (T20 in Appendix A). Thus $a \leq b$.

The above is a nice universal proof to know.

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

Since $1 \times 1 = 1$ and $(-1)(-1) = 1$ both 1 and -1 are divisors of 1. Now suppose m is any integer that divides 1. Then $\exists n \in \mathbb{Z}$ such that $1 = mn$. By Theorem T25 in Appendix A, either both m and n are positive or both m and n are negative. If both m and n are positive, then m is a positive integer divisor of 1. By Tthe previous theorem, $m \leq 1$, and since the only positive integer that is less than or equal to 1 is 1 itself, it follows that $m = 1$. On the other hand, if both m and n are negative, then by Theorem T12 in Appendix A, $(-m)(-n) = mn = 1$. In this case, $-m$ is a positive integer divisor of 1, and so by the same reasoning $-m = 1$ and thus $m = -1$. Therefore, there are only two possibilities: either $m = 1$ or $m = -1$. So 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.

Suppose a, b, and c are integers such that a divides b and b divides c. By definition of divisibility $\exists r, s \in \mathbb{Z}$ such that $b = ar$ and $c = bs$. Then,

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \end{aligned}$$

Let $k = rs$. Then, k is an integer since it is a product of integers and therefore $c = ak$. Thus, a divides c by definition of divisibility.

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

Suppose n is an integer that is greater than 1. If n is prime, then n is divisible by itself, a prime number, and we are done. If n is not prime, then $n = r_0 s_0$ where r_0 and s_0 are integers and $1 < r_0 < n$ and $1 < s_0 < n$. It follows from the definition of divisibility that $r_0 | n$. If r_0 is prime, then r_0 is a prime number that divides n and we are done. If r_0 is not prime, then, $r_0 = r_1 s_1$ where $r_1, s_1 \in \mathbb{Z}$ and $1 < r_1 < r_0$ and $1 < s_1 < r_0$. IT follows that $r_1 | r_0$. But we already know that $r_0 | n$. So by the previous proof $r_1 | n$.

We may continue factoring in this way, until we find a prime factor. We must succeed in a finite number of steps because each new factor is both less than the previous one and greater than 1, and there are fewer than n integers strictly between 1 and n. Thus, we obtain a sequence $r_0, r_1, r_2, \ldots, r_k$ where $k \geq 0$, $1 < r_k < r_{k-1} < \ldots < r_2 < r_1 < r_0 < n$ and $r_i | n$ for each $i = 0, 1, \ldots, k$. The condition for termination is that r_k should be prime. Hence, r_k is a prime number that divides n.

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 $m \geq k$, $S_m \to S_{m+1}$

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 $m \geq k$, $[S_k \wedge S_{k+1} \wedge \ldots \wedge S_m] \to S_{m+1}$

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

Exercise
Show that strong and weak induction are equivalent.

Let S_n be our statement we wish to prove.

First suppose that strong induction holds for our statement. This means that S_1 holds and whenever $n \leq k$, it must hold for $n = k + 1$. This implies that $n = k$ holds and $n = k + 1$ holds, the criteria for weak induction. Therefore, weak induction follows from strong induction.

Now, suppose that weak induction works, also specifically for our statement. This means that S_1 holds and for $n = k$, it must be that $n = k + 1$ holds. Let Q_k be the statement "S_n is true for all $n \leq k$." We will prove Q_n is true for all positive integers n by weak induction. Since we have S_1 then we also have the base case of Q_1. Suppose the inductive hypothesis of Q_k, i.e. S_k is true for all $n \leq k$. This tells us that S_{k+1} is also true by the outer induction proof. This then implies that Q_{k+1} holds since S_{k+1} and Q_k hold. This establishes the inductive step for statement Q_n. Therefore, this holds for all positive integers n. This is the same conclusion as strong induction makes for S_n meaning it is equivalent.

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

We could prove this directly by using Euler's trick of folding the sequence $1, 2, 3, \ldots, n$ on itself and creating pairs $(1, n), (2, n-1), (3, n-2), \ldots, (n/2 - 1, n/2 + 1)$ which each sum to $n + 1$. There are $n/2$ such pairs so the total sum is $\frac{n(n+1)}{2}$.

However, you might not have that insight and thus rely on mathematical induction. Let S_n be the statement that $1+2+\ldots+n = \frac{n(n+1)}{2}$. Then, S_1 says $1 = \frac{1(1+1)}{2} = 1$ which holds. Now assume the inductive hypothesis that statement S_k holds for some $k \geq 1$, i.e. $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$. Then, we will show the inductive step that S_{k+1} follows.

$$\begin{aligned}
1 + 2 + \ldots + (k-1) + k + (k+1) &= [1 + \ldots + (k-1) + k] + (k+1) && \text{regrouping} \\
&= \frac{k(k+1)}{2} + k + 1 && \text{by inductive hypothesis} \\
&= \frac{k(k+1) + 2k + 2}{2} && \text{algebra} \\
&= \frac{k^2 + 3k + 2}{2} && \text{algebra} \\
&= \frac{(k+1)(k+2)}{2} && \text{algebra}
\end{aligned}$$

Therefore, we have proven the inductive step and by mathematical induction the theorem is proven.

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

First, we think about the conjecture. We might make a table like follows:

n	Integers	Sum
1	1	1 = 1^2
2	1, 3	4 = 2^2
3	1, 3, 5	9 = 3^2
4	1, 3, 5, 7	16 = 4^2

Thus, it seems we want to prove the sum of the first n positive odd integers is n^2.

Let S_n be the statement that the sum of the first n positive odd integers is n^2. The base case is then S_1, which holds since $1 = 1^2$.

Suppose the inductive hypothesis that S_k holds, i.e. the sum of the first k odd integers is k^2. Another way to state this is that $1 + 3 + 5 + \ldots + (2k-1) = k^2$. Now we show that S_{k+1} holds.

$$\begin{aligned}
1 + 3 + 5 + \ldots + (2k-1) + (2k+1) &= k^2 + 2k + 1 \\
&= (k+1)(k+1) = (k+1)^2
\end{aligned}$$

Therefore, the inductive step holds and we have proven the claim.

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

Let S_n be the statement that $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$. The base case, S_0, holds since $2^0 = 1 = 2^{0+1} - 1$.

Suppose the inductive hypothesis that S_k holds, i.e. $1 + 2 + 2^2 + \ldots + 2^k = 2^{k+1} - 1$. Then, we wish to show S_{k+1} holds:

$$\begin{aligned} 1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} \\ &= 2\left(2^{k+1}\right) - 1 \\ &= 2^{k+2} - 1 \end{aligned}$$

Thus, the inductive step holds and we have proven the claim.

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

We could try the clever direct proof by noting that $3|n^3 - n$ is the same as saying $3|(n-1)n(n+1)$ if we factor the polynomial. Since $n - 1$, n, and $n + 1$ are consecutive one of them must be divisible by three meaning that we have a factor of three multiplied into the polynomial and thus we have our proof.

We could alternatively write an inductive proof. Then, S_n is the statement $3|n^3 - n$. The base case is S_1, i.e. $3|1^3 - 1$. We can let $k = 0$ to satisfy $0 = 3k$ and prove the base case holds.

Now suppose the inductive hypothesis of $3|k^3 - k$. We wish to prove the inductive step S_{k+1}. Note:

$$\begin{aligned} (k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k) \end{aligned}$$

We know that $3|k^3 - k$ by the inductive hypothesis and thus $\exists m \in \mathbb{Z}$ such that $3m = k^3 - k$. So by substitution we get $3m + 3(k^3 + k)$ which factors to $3(m + k^3 + k)$. Since integers are closed under multiplication and addition $m + k^3 + k$ is an integer and we have shown that $(k+1)^3 - (k+1)$ is indeed divisible by 3.