CSCI 2824 - CU Boulder, 2019 Summer

Lecture 6: Rational Number Proofs, Divisibility

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.

Theorem 3.1. *For all integers a and b, if a and b are positive and $a|b$, then $a \leq b$.*

Proof. 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.

Theorem 3.2. *The only divisors of 1 are 1 and -1.*

Proof. 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 iteself, 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. □

Theorem 3.3. *For all integers a, b, and c if a divides b and b divides c, then a divides c.*

Proof. Suppose a, b, and c are integers such that a divides b and b divides c. By definition of dividisibility $\exists r, s \in \mathbb{Z}$ 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. □

Theorem 3.4. *Any integer $n > 1$ is divisible by a prime number.*

Proof. 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 3.5. *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.

References