Proofs About Numbers

Reading: EC 2.2

Peter J. Haas

INFO 150
Fall Semester 2019

Overview

Goal: Use prior skills to reason about numbers

- Learn some standard definitions related to number
- Develop a clear style (a different kind of poetry)
- Apply what you know in increasingly abstract settings

Divisibility

Definition

An integer n is divisible by a nonzero integer k if there is an integer q (called the quotient) such that $n = k \cdot q$.

Equivalent terms

- "k divides n"
- "k is a factor of n"
- "n is a multiple of k"

Propositions About Divisibility - 1

Proposition 1

If the integers m and n are both divisible by 3, then $m + n$ is divisible by 3.

Proof (existence proof):

1. Let m and n be integers divisible by 3
2. Then there exist integers K and L such that $m = 3K$ and $n = 3L$
3. $m + n = 3K + 3L = 3(K + L)$
4. $K + L$ is an integer (the integers are closed under addition)
5. Hence $m + n$ is divisible by 3

Propositions About Divisibility - 2

Proposition 2

If the integers m and n are both divisible by 3, then $m \cdot n$ is divisible by 9.

Proof:

1. Let m and n be integers divisible by 3
2. Then there exist integers K and L such that $m = 3K$ and $n = 3L$
3. $m \cdot n = 3K \cdot 3L = 9(K \cdot L)$
4. $K \cdot L$ is an integer (the integers are closed under multiplication)
5. Hence $m \cdot n$ is divisible by 9

Propositions about Divisibility - 3

Proposition 3

If the integer n is divisible by 3, then $n^2 + 3n$ is divisible by 9.

Proof (building on earlier results):

1. Let n be an integer divisible by 3
2. By Proposition 1, $n + 3$ is divisible by 3
3. By Proposition 2, $n \cdot (n + 3)$ is divisible by 9
4. Since $n^2 + 3n = n \cdot (n + 3)$, it follows that $n^2 + 3n$ is divisible by 9

Logical Notation Revisited

$\mathbb{Z}_{\neq 0}$: set of non-zero integers

Proposition 4

For any nonzero integer d, if the integers m and n are both divisible by d, then $m + n$ is divisible by d.

Exercise: Let $Q(x, d) =$ "x is divisible by d"

- Write a logical formula corresponding to Proposition 4

$\forall d \in \mathbb{Z}_{\neq 0}, m \in \mathbb{Z}, n \in \mathbb{Z}, \quad Q(m,d) \wedge Q(n,d) \rightarrow Q(m+n,d)$

- Write the contrapositive

$\neg Q(m+n, d) \rightarrow \neg Q(m,d) \vee \neg Q(n,d)$

- Write the converse (is it true?)

$Q(m+n, d) \rightarrow Q(m,d) \wedge Q(n,d)$ ✗ counterexample: $d=2, m=3, n=5$

- Write the inverse (is it true?)

$\neg Q(m,d) \vee \neg Q(n,d) \rightarrow \neg Q(m+n,d)$ ✗ same counterexample

Rational Numbers

Definitions

A real number r is rational if there exist integers a and b ($b \neq 0$) such that $r = a/b$.
A real number is irrational if it is not rational.

Definition

Two integers having no common divisor great than 1 are called relatively prime.

Rational Numbers

Definitions

A real number r is rational if there exist integers a and b ($b \neq 0$) such that $r = a/b$.
A real number is irrational if it is not rational.

Definition

Two integers having no common divisor great than 1 are called relatively prime.

Observations about rational numbers

- Also called fractions
- Can be expressed in many equivalent ways: $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$
- It is always possible to choose a and b so that they are relatively prime

Rational Numbers

Definitions

A real number r is rational if there exist integers a and b ($b \neq 0$) such that $r = a/b$.
A real number is irrational if it is not rational.

Definition

Two integers having no common divisor great than 1 are called relatively prime.

Observations about rational numbers

- Also called fractions
- Can be expressed in many equivalent ways: $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$
- It is always possible to choose a and b so that they are relatively prime

Existence proofs about rational numbers

- To show that r is a rational number, you must show that it can be written as

$$\frac{\text{some integer}}{\text{some nonzero integer}}$$

A Proposition About Rational Numbers

Proposition 5

For any rational number r, the number $r + 1$ is also rational.

Proof

1. Let r be a rational number
2. Then r can be written as $\frac{a}{b}$ for some integers a and b with $b \neq 0$
3. Then
$$r + 1 = \frac{a}{b} + 1 = \frac{a}{b} + \frac{b}{b} = \frac{a+b}{b}.$$
4. Since $a + b$ and b are integers with $b \neq 0$, $r + 1$ is rational

(a+b is an integer by closure property of integers under addition)

A Proposition About Rational Numbers

Proposition 5

For any rational number r, the number $r + 1$ is also rational.

Proof

1. Let r be a rational number
2. Then r can be written as $\frac{a}{b}$ for some integers a and b with $b \neq 0$
3. Then
$$r + 1 = \frac{a}{b} + 1 = \frac{a}{b} + \frac{b}{b} = \frac{a+b}{b}.$$
4. Since $a + b$ and b are integers with $b \neq 0$, $r + 1$ is rational

This is another example of an existence proof

- Find integers c and d such that $r + 1 = \frac{c}{d}$
- The proof simply shows that $c = a + b$ and $d = b$ satisfy the conditions

Another Proposition About Rational Numbers

Proposition

For any real number x, if $2x$ is irrational then x is irrational

Prove this! $Q(x) =$ "x is rational"

[Hint: for a negative conclusion, it can be easier to prove the contrapositive]

original: $\neg Q(2x) \to \neg Q(x)$.

contrapositive: $Q(x) \to Q(2x)$ "if x is rational, then $2x$ is rational"

Proof

1. Let x be a given rational number
2. We can write $x = \frac{a}{b}$ for some integers a, b with $b \neq 0$
3. $2x = 2 \cdot \frac{a}{b} = \frac{2 \cdot a}{b}$, where $2 \cdot a$ is an integer (by closure) and b is a nonzero integer by assumption
4. By definition of "rational", $2x$ is rational

Proving by Cases

Proposition 5

For any integer n, $n^2 + n$ is even.

Proof

1. Case 1: n is even
   1.1 $n = 2L$ for some integer L
   1.2 Then
   $$n^2 + n = (2L)^2 + (2L) = 4L^2 + 2L = 2(2L^2 + L)$$
   1.3 Since $2L^2 + L$ is an integer, $n^2 + n$ is even
2. Case 2: n is odd
   2.1 $n = 2M + 1$ for some integer M
   2.2 Then
   $$\begin{aligned} n^2 + n &= (2M+1)^2 + (2M+1) = 4M^2 + 4M + 1 + 2M + 1 \\ &= 4M^2 + 6M + 2 = 2(2M^2 + 3M + 1) \end{aligned}$$
   2.3 Since $2M^2 + 3M + 1$ is an integer, $n^2 + n$ is even
3. Thus, in either case, we have shown that $n^2 + n$ is even

Another Proof Using Cases

Proposition 5

Every perfect square is either a multiple of 4 or of the form $4q + 1$ for some integer q

Proof

1. Given a perfect square n, write $n = m^2$
2. Case 1: m is even
   - 2.1 $m = 2k$ for some integer k
   - 2.2 Then
   $$n = m^2 = (2k)^2 = 4k^2$$
   - 2.3 Since k^2 is an integer, n is divisible by 4
3. Case 2: m is odd
   - 3.1 $m = 2k + 1$ for some integer k
   - 3.2 Then
   $$n = m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$
   - 3.3 So $n = 4 \cdot q + 1$, where $q = k^2 + k$ (an integer)

Note: we used the variable k for both cases,but not a problem (2 separate "mini-proofs")

The Division Theorem

We used the fact that every integer is even or odd

- Equivalently, whenever you divide an integer n by 2, you get some quotient q and a remainder r that equals 0 or 1
- Formally, every integer n can be written $n = 2 \cdot q + r$ for some integer q, where $r = 0$ or 1
- This is why we do not, e.g., define odd as "not even": it is more useful to say something positive

The Division Theorem

We used the fact that every integer is even or odd

- Equivalently, whenever you divide an integer n by 2, you get some quotient q and a remainder r that equals 0 or 1
- Formally, every integer n can be written $n = 2 \cdot q + r$ for some integer q, where $r = 0$ or 1
- This is why we do not, e.g., define odd as "not even": it is more useful to say something positive

This point of view generalizes to any divisor

- Whenever you divide an integer n by a positive integer d, you get a unique integer quotient q and a unique remainder r from the set $\{0, 1, \ldots, d-1\}$

Divisor $= 5$:

n	1	23	49	0	-13
Quotient	0	4	9	0	-3
Remainder	1	3	4	0	2
Equation $n =$	$0 \cdot 5 + 1$	$4 \cdot 5 + 3$	$9 \cdot 5 + 4$	$0 \cdot 5 + 0$	$-3 \cdot 5 + 2$

The Division Theorem, Continued

The Division Theorem

For all integers a and b (with $b > 0$), there is an integer q (the quotient) and an integer r (the remainder) such that

1. $a = b \cdot q + r$; and
2. $0 \leq r < b$.

Furthermore, q and r are the only numbers satisfying those conditions.

The Division Theorem, Continued

The Division Theorem

For all integers a and b (with $b > 0$), there is an integer q (the quotient) and an integer r (the remainder) such that

1. $a = b \cdot q + r$; and
2. $0 \leq r < b$.

Furthermore, q and r are the only numbers satisfying those conditions.

Example: $73 \div 5$

- Quotient of 14 and remainder of 3 (or $= 14\frac{3}{5}$ or $= 14.6$)
- Check the answer by checking that $73 = 5 \cdot 14 + 3$

The Division Theorem, Continued

The Division Theorem

For all integers a and b (with $b > 0$), there is an integer q (the quotient) and an integer r (the remainder) such that

1. $a = b \cdot q + r$; and
2. $0 \leq r < b$.

Furthermore, q and r are the only numbers satisfying those conditions.

Example: $73 \div 5$

- Quotient of 14 and remainder of 3 (or $= 14\frac{3}{5}$ or $= 14.6$)
- Check the answer by checking that $73 = 5 \cdot 14 + 3$

~ i.e., $b=5$

Example: for a divisor of 5, the Division Theorem says that

1. For any integer a, we can find a quotient q such that $a = 5 \cdot q + r$, and r is either 0, 1, 2, 3, or 4
2. That is, we can find q so that a can be written as one of the following:

$$a = 5 \cdot q, \quad a = 5 \cdot q + 1, \quad a = 5 \cdot q + 2, \quad a = 5 \cdot q + 3, \quad \text{or} \quad a = 5 \cdot q + 4$$

Using the Division Theorem in a Proof

Proposition

If n is any integer not divisible by 5, then n has a square of the form $5k+1$ or $5k+4$.

Don't need to consider case where $n = 5 \cdot q + 0$

Examples: $13^2 = 5 \cdot 33 + 4$ **and** $9^2 = 5 \cdot 16 + 1$

Proof

1. Let n be an integer not divisible by 5
2. By the Division Theorem, dividing n by 5 leaves a remainder of 0, 1, 2, 3, or 4
3. Since n is not divisible by 5, the remainder must equal 1, 2, 3, or 4
4. Case 1: $n = 5q + 1$
   4.1 $n^2 = 25q^2 + 10q + 1 = 5 \cdot (5q^2 + 2q) + 1 = 5 \cdot (\text{integer}) + 1$
5. Case 2: $n = 5q + 2$
   5.1 $n^2 = 25q^2 + 20q + 4 = 5 \cdot (5q^2 + 4q) + 4 = 5 \cdot (\text{integer}) + 4$
6. Case ~~1~~ 3: $n = 5q + 3$
   6.1 $n^2 = 25q^2 + 30q + 9 = 5 \cdot (5q^2 + 6q + 1) + 4 = 5 \cdot (\text{integer}) + 4$
7. Case ~~1~~ 4: $n = 5q + 4$
   7.1 $n^2 = 25q^2 + 40q + 16 = 5 \cdot (5q^2 + 8q + 3) + 1 = 5 \cdot (\text{integer}) + 1$
8. Therefore n is of the form $5k+1$ or $5k+4$ in every possible case

The MOD Operator

Definition

By the Division Theorem, we can write any integer a in the form $a = b \cdot q + r$, where $0 \leq r < b$. We then write $a \bmod b = r$.

Notes

- Thus a mod b is the remainder after dividing a by b
- In, e.g., C++ and Java, we write $a\%b$ (for "branching" statements)
- Previous proposition: "if n mod $5 \neq 0$, then n^2 mod $5 = 1$ or 4"

Example: Compute each of the following

- 73 mod 5 $\quad 73 = 14 \cdot 5 + 3 \quad 73 \bmod 5 = \boxed{3}$
- -22 mod 6 $\quad -22 = -4 \cdot 6 + 2 \quad -22 \bmod 6 = \boxed{2}$
- 8 mod 11 $\quad 8 = 11 \cdot 0 + 8 \quad 8 \bmod 11 = \boxed{8}$
- $(4n^2 - 12n + 3)$ mod 4 for any integer n

$4n^2 - 12n + 3 = 4(n^2 - 3n) + 3 = 4(\text{integer}) + 3$, so $(4n^2 - 12n + 3) \bmod 4 = \boxed{3}$

- $(4n^2 - 12n + 9)$ mod 4 for any integer n

$4n^2 - 12n + 9 = 4(n^2 - 3n + 2) + 1$, so $(4n^2 - 12n + 9) \bmod 4 = \boxed{1}$

Excursion: Pseudorandom Number Generation

To simulate a random event on a computer, you need "random numbers"

- E.g., The number of barbarian invaders who attack you
- E.g., the number of patients arriving at hospital
- Hard to generate truly random numbers (radioactive decay, atmospheric noise)
- Come up with numbers that "look" random (pass statistical tests)

A simple "linear congruential" pseudorandom number generator

- $x_1 = 7$ $\quad x_2 = (5 \cdot 7 + 3) \bmod 16$ $\quad x_3 = 1$ $\quad x_4 = 8$

  $= 38 \bmod 16$

  $= 3$