Lecture 07

Elementary Number Theory and Methods of Proof

CSE173: Discrete Mathematics

Direct Proof and Counterexample II: Rational Numbers

Sums, differences, and products of integers are integers. But most quotients of integers are not integers. Quotients of integers are, however, important; they are known as *rational numbers*.

• Definition

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 **irrational.** More formally, if r is a real number, then

$$r \text{ is rational } \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

The word *rational* contains the word *ratio*, which is another word for quotient. A rational number can be written as a ratio of integers.

Example 1 – *Determining Whether Numbers Are Rational or Irrational*

a. Is 10/3 a rational number?

b. Is $-\frac{5}{39}$ a rational number?

c. Is 0.281 a rational number?

d. Is 7 a rational number?

e. Is 0 a rational number?

Example 1 – *Determining Whether Numbers Are Rational or Irrational* cont'd

f. Is 2/0 a rational number?

g. Is 2/0 an irrational number?

h. Is 0.12121212 . . . a rational number (where the digits 12 are assumed to repeat forever)?

i. If m and n are integers and neither m nor n is zero, is $(m + n)/mn$ a rational number?

Example 1 – *Solution*

a. Yes, 10/3 is a quotient of the integers 10 and 3 and hence is rational.

b. Yes, $-\frac{5}{39} = \frac{-5}{39}$, which is a quotient of the integers –5 and 39 and hence is rational.

c. Yes, 0.281 = 281/1000. Note that the real numbers represented on a typical calculator display are all finite decimals.

An explanation similar to the one in this example shows that any such number is rational. It follows that a calculator with such a display can represent only rational numbers.

Example 1 – *Solution* cont'd

d. Yes, 7 = 7/1.

e. Yes, 0 = 0/1.

f. No, 2/0 is not a number (division by 0 is not allowed).

g. No, because every irrational number is a number, and 2/0 is not a number.

Example 1 – *Solution* cont'd

h. Yes. Let $x = 0.12121212\ldots$. Then $100x = 12.12121212\ldots$.

Thus $100x - x = 12.12121212\ldots - 0.12121212\ldots = 12.$

But also $100x - x = 99x$ by basic algebra

Hence $99x = 12,$

And so $x = \frac{12}{99}.$

Therefore, 0.12121212…. = 12/99, which is a ratio of two nonzero integers and thus is a rational number.

Example 1 – *Solution* cont'd

Note that you can use an argument similar to this one to show that any repeating decimal is a rational number.

i. Yes, since *m* and *n* are integers, so are *m* + *n* and *mn* (because sums and products of integers are integers). Also $mn \neq 0$ by the *zero product property*.

One version of this property says the following:

Zero Product Property

If neither of two real numbers is zero, then their product is also not zero.

Example 1 – *Solution* cont'd

It follows that $(m + n)/mn$ is a quotient of two integers with a nonzero denominator and hence is a rational number.

More on Generalizing from the Generic Particular

Some people like to think of the method of generalizing from the generic particular as a challenge process.

If you claim a property holds for all elements in a domain, then someone can challenge your claim by picking any element in the domain whatsoever and asking you to prove that that element satisfies the property.

To prove your claim, you must be able to meet all such challenges. That is, you must have a way to convince the challenger that the property is true for an *arbitrarily chosen* element in the domain.

More on Generalizing from the Generic Particular

For example, suppose "A" claims that every integer is a rational number. "B" challenges this claim by asking "A" to prove it for $n = 7$.

"A" observes that

$$7 = \frac{7}{1}$$ which is a quotient of integers and hence rational.

"B" accepts this explanation but challenges again with $n = -12$. "A" responds that

$$-12 = \frac{-12}{1}$$ which is a quotient of integers and hence rational.

More on Generalizing from the Generic Particular

Next "B" tries to trip up "A" by challenging with $n = 0$, but "A" answers that

$$0 = \frac{0}{1}$$ which is a quotient of integers and hence rational.

As you can see, "A" is able to respond effectively to all "B"s challenges because "A" has a general procedure for putting integers into the form of rational numbers: "A" just divides whatever integer "B" gives by 1.

That is, no matter what integer n "B" gives "A", "A" writes

$$n = \frac{n}{1}$$ which is a quotient of integers and hence rational.

More on Generalizing from the Generic Particular

This discussion proves the following theorem.

Theorem 4.2.1

Every integer is a rational number.

Proving Properties of Rational Numbers

The next example shows how to use the method of generalizing from the generic particular to prove a property of rational numbers.

Example 2 – *A Sum of Rationals Is Rational*

Prove that the sum of any two rational numbers is rational.

Solution:
Begin by mentally or explicitly rewriting the statement to be proved in the form "∀_____, if _____ then _____."

Formal Restatement: ∀ real numbers r and s, if r and s are rational then $r + s$ is rational.

Next ask yourself, "Where am I starting from?" or "What am I supposing?" The answer gives you the starting point, or first sentence, of the proof.

Example 2 – *Solution* cont'd

Starting Point: Suppose r and s are particular but arbitrarily chosen real numbers such that r and s are rational; or, more simply, Suppose r and s are rational numbers.

Then ask yourself, "What must I show to complete the proof?"

To Show: $r + s$ is rational.

Finally ask, "How do I get from the starting point to the conclusion?" or "Why must $r + s$ be rational if both r and s are rational?" The answer depends in an essential way on the definition of rational.

Example 2 – *Solution* cont'd

Rational numbers are quotients of integers, so to say that r and s are rational means that

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d} \quad \text{for some integers } a, b, c, \text{ and } d \text{ where } b \neq 0 \text{ and } d \neq 0.$$

It follows by substitution that

$$r + s = \frac{a}{b} + \frac{c}{d}.$$

Example 2 – *Solution* cont'd

You need to show that $r + s$ is rational, which means that $r + s$ can be written as a single fraction or ratio of two integers with a nonzero denominator.

But the right-hand side of equation (4.2.1) in

$$\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd}$$ rewriting the fraction with a common denominator

$$= \frac{ad + bc}{bd}$$ adding fractions with a common denominator.

Example 2 – *Solution* cont'd

Is this fraction a ratio of integers? Yes. Because products and sums of integers are integers, $ad + bc$ and bd are both integers.

Is the denominator $bd \neq 0$? Yes, by the zero product property (since $b \neq 0$ and $d \neq 0$). Thus $r + s$ is a rational number.

This discussion is summarized as follows:

Theorem 4.2.2

The sum of any two rational numbers is rational.

Example 2 – *Solution* cont'd

Proof:
Suppose r and s are rational numbers. *[We must show that $r + s$ is rational.]*

Then, by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$.

Thus

$$r + s = \frac{a}{b} + \frac{c}{d}$$ by substitution

$$= \frac{ad + bc}{bd}$$ by basic algebra.

Example 2 – *Solution* cont'd

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, and d are all integers.

Also $q \neq 0$ by the zero product property.

Thus

$$r + s = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } q \neq 0.$$

Therefore, $r + s$ is rational by definition of a rational number. *[This is what was to be shown.]*

Deriving New Mathematics from Old

In the future, when we ask you to **prove something directly from the definitions,** we will mean that you should restrict yourself to this approach.

However, once a collection of statements has been proved directly from the definitions, another method of proof becomes possible.

The statements in the collection can be used to derive additional results.

Example 3 – *Deriving Additional Results about Even and Odd Integers*

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.

2. The sum and difference of any two odd integers are even.

3. The product of any two odd integers is odd.

4. The product of any even integer and any odd integer is even.

Example 3 – *Deriving Additional Results about Even and Odd Integers* cont'd

5. The sum of any odd integer and any even integer is odd.

6. The difference of any odd integer minus any even integer is odd.

7. The difference of any even integer minus any odd integer is odd.

Use the properties listed above to prove that if a is any even integer and b is any odd integer, then $\frac{a^2+b^2+1}{2}$ is an integer.

Example 3 – *Solution*

Suppose *a* is any even integer and *b* is any odd integer. By property 3, b^2 is odd, and by property 1, a^2 is even.

Then by property 5, $a^2 + b^2$ is odd, and because 1 is also odd, the sum $(a^2 + b^2) + 1 = a^2 + b^2 + 1$ is even by property 2.

Hence, by definition of even, there exists an integer *k* such that $a^2 + b^2 + 1 = 2k$.

Dividing both sides by 2 gives $\frac{a^2+b^2+1}{2} = k$, which is an integer.

Thus $\frac{a^2+b^2+1}{2}$ is an integer *[as was to be shown]*.

Deriving New Mathematics from Old

A **corollary** is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Example 4 – *The Double of a Rational Number*

Derive the following as a corollary of Theorem 4.2.2.

Corollary 4.2.3

The double of a rational number is rational.

Solution:
The double of a number is just its sum with itself.

But since the sum of any two rational numbers is rational (Theorem 4.2.2), the sum of a rational number with itself is rational.

Hence the double of a rational number is rational.

Example 4 – *Solution* cont'd

Here is a formal version of this argument:

Proof:
Suppose *r* is any rational number. Then $2r = r + r$ is a sum of two rational numbers.

So, by Theorem 4.2.2, $2r$ is rational.

Direct Proof and Counterexample III: Divisibility

The notion of divisibility is the central concept of one of the most beautiful subjects in advanced mathematics: **number theory**, the study of properties of integers.

• Definition

If n and d are integers and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Example 1 – *Divisibility*

a. Is 21 divisible by 3?

b. Does 5 divide 40?

c. Does 7 | 42?

d. Is 32 a multiple of –16?

e. Is 6 a factor of 54?

f. Is 7 a factor of –7?

Example 1 – *Solution*

a. Yes, $21 = 3 \cdot 7$.

b. Yes, $40 = 5 \cdot 8$.

c. Yes, $42 = 7 \cdot 6$.

d. Yes, $32 = (-16) \cdot (-2)$.

e. Yes, $54 = 6 \cdot 9$.

f. Yes, $-7 = 7 \cdot (-1)$.

Direct Proof and Counterexample III: Divisibility

Two useful properties of divisibility are (1) that if one positive integer divides a second positive integer, then the first is less than or equal to the second, and (2) that the only divisors of 1 are 1 and –1.

Theorem 4.3.1 A Positive Divisor of a Positive Integer

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

Theorem 4.3.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Example 1 – *Divisibility of Algebraic Expressions*

a. If a and b are integers, is $3a + 3b$ divisible by 3?

b. If k and m are integers, is $10km$ divisible by 5?

Solution:

a. Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

b. Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers.

Direct Proof and Counterexample III: Divisibility

When the definition of divides is rewritten formally using the existential quantifier, the result is

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Since the negation of an existential statement is universal, it follows that d does not divide n (denoted $d \nmid n$) if, and only if, $\forall$ integers k, $n \neq dk$, or, in other words, the quotient n/d is not an integer.

For all integers n and d, $\quad d \nmid n \quad \Leftrightarrow \quad \dfrac{n}{d}$ is not an integer.

Example 4 – *Checking Nondivisibility*

Does 4 | 15?

Solution:

No, $\frac{15}{4} = 3.75$, which is not an integer.

Proving Properties of Divisibility

One of the most useful properties of divisibility is that it is transitive. If one number divides a second and the second number divides a third, then the first number divides the third.

Example 6 – *Transitivity of Divisibility*

Prove that for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Solution:
Since the statement to be proved is already written formally, you can immediately pick out the starting point, or first sentence of the proof, and the conclusion that must be shown.

Starting Point: Suppose a, b, and c are particular but arbitrarily chosen integers such that $a \mid b$ and $b \mid c$.

Example 6 – *Solution* cont'd

To Show: $a \mid c$.

You need to show that $a \mid c$, or, in other words, that

$$c = a \cdot (\text{some integer}).$$

But since $a \mid b$,

$$b = ar \quad \text{for some integer } r. \qquad 4.3.1$$

And since $b \mid c$,

$$c = bs \quad \text{for some integer } s. \qquad 4.3.2$$

Equation 4.3.2 expresses c in terms of b, and equation 4.3.1 expresses b in terms of a.

Example 6 – *Solution* cont'd

Thus if you substitute 4.3.1 into 4.3.2, you will have an equation that expresses c in terms of a.

$$c = bs \qquad \text{by equation 4.3.2}$$

$$= (ar)s \qquad \text{by equation 4.3.1.}$$

But $(ar)s = a(rs)$ by the associative law for multiplication. Hence

$$c = a(rs).$$

Now you are almost finished.

Example 6 – *Solution* cont'd

You have expressed c as $a \cdot$ (something). It remains only to verify that that something is an integer. But of course it is, because it is a product of two integers.

This discussion is summarized as follows:

Theorem 4.3.3 Transitivity of Divisibility

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

Example 6 – *Solution* cont'd

Proof:
Suppose *a*, *b*, and *c* are *[particular but arbitrarily chosen]* integers such that *a* divides *b* and *b* divides *c*. *[We must show that a divides c.]* By definition of divisibility,

$$b = ar \quad \text{and} \quad c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \qquad \text{by basic algebra.} \end{aligned}$$

Example 6 – *Solution* cont'd

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore

$$c = ak \quad \text{where } k \text{ is an integer.}$$

Thus *a* divides *c* by definition of divisibility. *[This is what was to be shown.]*

Proving Properties of Divisibility

Theorem 4.3.4 Divisibility by a Prime

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

Counterexamples and Divisibility

To show that a proposed divisibility property is not universally true, you need only find one pair of integers for which it is false.

Example 7 – *Checking a Proposed Divisibility Property*

Is the following statement true or false? For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Solution:

This statement is false. Can you think of a counterexample just by concentrating for a minute or so?

The following discussion describes a mental process that may take just a few seconds. It is helpful to be able to use it consciously, however, to solve more difficult problems.

Example 7 – *Solution* cont'd

To discover the truth or falsity of the given statement, start off much as you would if you were trying to prove it.

Starting Point: Suppose a and b are integers such that $a \mid b$ and $b \mid a$.

Ask yourself, "Must it follow that $a = b$, or could it happen that $a \neq b$ for some a and b?" Focus on the supposition. What does it mean? By definition of divisibility, the conditions $a \mid b$ and $b \mid a$ mean that

$$b = ka \quad \text{and} \quad a = lb \quad \text{for some integers } k \text{ and } l.$$

Example 7 – *Solution* cont'd

Must it follow that $a = b$, or can you find integers a and b that satisfy these equations for which $a \neq b$? The equations imply that

$$b = ka = k(lb) = (kl)b.$$

Since $b \mid a$, $b \neq 0$, and so you can cancel b from the extreme left and right sides to obtain

$$1 = kl.$$

In other words, k and l are divisors of 1. But, by Theorem 4.3.2, the only divisors of 1 are 1 and –1. Thus k and l are both 1 or are both –1. If $k = l = 1$, then $b = a$.

Example 7 – *Solution* cont'd

But if $k = l = -1$, then $b = -a$ and so $a \neq b$.

This analysis suggests that you can find a counterexample by taking $b = -a$.

Here is a formal answer:

Proposed Divisibility Property: For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then

$a \mid b$ since $2 \mid (-2)$ and $b \mid a$ since $(-2) \mid 2$, but $a \neq b$ since $2 \neq -2$.

Therefore, the statement is false.

The Unique Factorization of Integers Theorem

The most comprehensive statement about divisibility of integers is contained in the *unique factorization of integers theorem*.

Because of its importance, this theorem is also called the *fundamental theorem of arithmetic*.

The unique factorization of integers theorem says that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order in which the primes are written.

The Unique Factorization of Integers Theorem

Theorem 4.3.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist 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

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

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.

The Unique Factorization of Integers Theorem

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right.

• Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example 9 – *Using Unique Factorization to Solve a Problem*

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

Does $17 \mid m$?

Solution:

Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem).

But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large). Hence 17 must occur as one of the prime factors of m, and so $17 \mid m$.