

Math 2710

Sep 9-13

Catch-up

Discussion problems

By groups, look at:

- ▶ page 21, prob. 57
- ▶ page 21, prob. 58
- ▶ page 21: prob. 60
- ▶ page 22: prob. 66

Section 1.6: Counterexamples

Counterexamples: disproving for all statements

Suppose have a proposition that makes a “for all” assertion.

Proposition: All odd numbers are prime.

More formally, the proposition says: For all integers x , if x is odd then x is prime.

This statement is FALSE if we can find *one* odd integer x that is not prime. In other words, if we can show the negation:

There exists an x such that x is odd and x is not prime.

Notice that the negation of “If x is odd then x is prime” is “ x is odd and x is not prime” as we’ve seen before.

Disproving existence statements

Suppose we have a proposition that makes a “there exists” statement.

Proposition: There exist integers x , y , and z so that

$$114 = x^3 + y^3 + z^3$$

To DISPROVE this statement, we need to rule out ALL triples (x, y, z) because the negation would be

Proposition: For all integers x, y, z , we have

$$x^3 + y^3 + z^3 \neq 114.$$

In fact the answer to this question is unknown; after the solution of 42, 114 is the smallest number where the answer is not known.

Chapter 2

Section 2.1: The division algorithm

Definition: Given two integers d and n , we say that d divides n (or n is divisible by d) if there exists an integer m so that $n = dm$. We write $d|n$ to mean “ d divides n ”.

Proposition: Let a , b , and c be integers.

1. if $a|b$ and $b|c$ then $a|c$.
2. if $a|b$ and $a|c$ then $a|(bx + cy)$ for any integers x and y . In particular $a|(b + c)$ and $a|(b - c)$.
3. if $a|b$ and $b|a$ then $a = \pm b$.
4. If $a|b$ and $b \neq 0$ then $|a| \leq |b|$.

Divisibility property 1

Proposition: if $a|b$ and $b|c$ then $a|c$.

1. $a|b$ means there exists an integer m so that $b = am$.
2. $b|c$ means there exists an integer k so that $c = bk$.
3. $c = bk = amk$. Since there is an integer mk so that $c = amk$, we know that $a|c$.

Property 2

Proposition: if $a|b$ and $a|c$ then $a|(bx + cy)$ for any integers x and y . In particular $a|(b + c)$ and $a|(b - c)$.

1. $a|b$ means that there is an integer m so that $b = am$.
2. $a|c$ means that there is an integer k so that $c = ak$.
3. $bx + cy = amx + ak y = a(mx + ky)$. Therefore there is an integer, $s = mx + ky$, so that $bx + cy = as$. Therefore $a|(bx + cy)$

Property 3

Proposition: if $a|b$ and $b|a$ then $a = b$ or $a = -b$.

1. $a|b$ means $b = am$ for some integer m .
2. $b|a$ means $a = bk$ for some integer k .
3. $b = am = bmk$ so $b(1 - km) = 0$. There three possibilities:
 - ▶ $b = 0$, in which case $a = bk = 0$, and $a = b$.
 - ▶ $k = m = 1$ in which case $b = a$.
 - ▶ $k = m = -1$, in which case $b = -a$.

Question: We are using this fact. Let k and m be integers such that $km = 1$. Then either $k = m = 1$ or $k = m = -1$. Why is this true? Prove it.

Property 4

Proposition: If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

1. Since $a|b$, we have $b = am$. Therefore $b^2 = a^2m^2$.
2. If $b \neq 0$, then neither a nor m is zero. Then $m^2 \geq 1$, so $b^2 \geq a^2$.
3. Since $b^2 \geq a^2$, we have $|b| \geq |a|$.

Division Algorithm (division with remainder)

Proposition: Let a and b be integers, and suppose $b > 0$. Then there are integers q and r so that

$$a = qb + r$$

and

$$0 \leq r < b.$$

Furthermore, there is only one q and one r satisfying these conditions. (We say q and r are *unique*).

Division algorithm examples

Examples:

Suppose $b = 2$. Then this proposition says that any integer a can be written

$$a = 2q + r$$

with $r = 0$ or $r = 1$. So this proposition tells us that every number is either even or of the form $2q + 1$ for some integer q .

Suppose $b = 3$. Then this proposition says that any integer a can be written

$$a = 3q + r$$

with $r \in \{0, 1, 2\}$. In other words, there are three kinds of numbers: those that are divisible by 3; those that are of the form $3q + 1$ (meaning they are one more than a multiple of 3) and those of the form $3q + 2$ (meaning they are two more than, or one less than, a multiple of 3).

Grade School

In grade school, we called q the quotient and r the remainder when dividing a by b .

For example, dividing 7 into 25 gives 3 with remainder 4. In other words, $25 = 7 * 3 + 4$.

We want the remainder to be less than the divisor (or we could take more into the quotient)

Proof of Division Algorithm

The Well-ordering principle: Every non-empty set S of positive integers has a smallest element: that is, there exists (exactly one) $x \in S$ so that, for all $y \in S$, $x \leq y$.

- ▶ If S is nonempty,
- ▶ then there exists $x \in S$
- ▶ such that, for all $y \in S$
- ▶ $x \leq y$.

THIS IS AN AXIOM!

Another version: Let S be a set of positive integers. Suppose that, for every $y \in S$, there exists $x \in S$ so that $x < y$. Then S is empty.

Negation of the original statement: If, for all $x \in S$, there exists $y \in S$ so that $y < x$, then S is empty.

Proof of Division Algorithm 2

We have a and b ; we want to divide a by b and identify the remainder.

- ▶ First suppose $a > 0$ and $b > 0$.
- ▶ Division is repeated subtraction so consider $a, a - b, a - 2b, a - 3b, \dots$. Call this set A .
- ▶ Let S be the set of positive elements of A .
- ▶ S is nonempty because $a \in S$.
- ▶ S has a least element. Let r be that element. Then $r = a - qb$ for some q in \mathbb{Z} .
- ▶ $r \geq 0$ because $r \in S$ and S consists of positive elements.
- ▶ $a - (q + 1)b < 0$ because r is the smallest positive element of the set A .
- ▶ $r - b = a - qb - b = a - (q + 1)b < 0$ so $r < b$

Now suppose $a = xb + s$ and $0 \leq s < b$. Then $qb + r = xb + s$ so $(q - x)b = s - r$. This tells us that b divides $s - r$. Since $0 \leq r < b$ and $0 \leq s < b$, we know that $0 \leq |r - s| < b$. Therefore $r - s = 0$ so $r = s$, and then $q = x$. In other words, q and r are the

Some examples

What is the remainder when -257 is divided by 11 ? What is the quotient.

Recall that a number is '5-ish' if it is divisible by 5 . What does the division algorithm tell you about numbers that are NOT 5-ish?

Greatest common divisor

Definition: Let a and b be integers, at least one of which is not zero. An integer d is a *common divisor* of a and b if $d|a$ and $d|b$. The *greatest common divisor* $\gcd(a, b)$ of a and b is the largest integer among all common divisors of a and b .

Note that a common divisor of a and b must be smaller than $|a|$ and $|b|$. So there must be a greatest one. (How is this related to the well ordering principle?)

The **Euclidean Algorithm** is a method for finding the greatest common divisor. It is the prototypical example of a “method of descent” in which you take a problem and systematically transform it into easier, but equivalent, problems until the solution becomes obvious.

Examples of Euclid's Algorithm

Euclidean Algorithm

Enter a: 1230

Enter b>0: 54

$$1230 = 22 \cdot 54 + 42$$

$$54 = 1 \cdot 42 + 12$$

$$42 = 3 \cdot 12 + 6$$

$$12 = 2 \cdot 6 + 0$$

$$\text{GCD} = 6$$

Example 2

Euclidean Algorithm

Enter a: 1029381029

Enter b>0: 1201233111

1029381029=	0*	1201233111
1201233111=	1*	1029381029
1029381029=	5*	171852082
171852082=	1*	170120619
170120619=	98*	1731463
1731463=	3*	437245
437245=	1*	419728
419728=	23*	17517
17517=	1*	16837
16837=	24*	680
680=	1*	517
517=	3*	163
163=	5*	28
28=	1*	23
23=	4*	

Why does Euclid's Algorithm work?