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 $|a| \leq |b|$.

Divisibilty 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 is an integer mk so that $c = amk$, we know tht $a|c$.

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. $bx + cy = amx + aky = a(mx + ky)$. Therefore there is an integer, $s = mk + ky$, 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 $b > 0$.

- Divison is repeated subtraction so consider $a, a-b, a-2b, a-3b, \ldots$. 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 only solutions to the equation $a = qb + r$ with $0 \leq r < b$.

The condition that a be positive is not necessary. Can you re-do the proof if $a < 0$? You have to fix a few steps.

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?)

Some examples:

- $\gcd(145, 55) = 5$. (The divisors of 145 are $1, 5, 29, and 145$; of 55 are $1, 5, 11, 55$; the common divisors are $1, 5$.
- $\gcd(64, 12) = 4$.

- $\gcd(100, 49) = 1$.

To prove that an integer d is a common divisor of a and b, you must show that $d|a$ and $d|b$.

To prove that it is the greatest common divisor of a and b, you must prove:

- that it is a common divisor, and
- if x is another common divisor, then $x \leq d$.

Euclid's Algorithm

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.

```
Euclidean Algorithm
Enter a: 1230
Enter b>0: 54
1230    =   22*54   +   42
54  =   1*42    +   12
42  =   3*12    +   6
12  =   2*6 +   0
GCD = 6
```

Example 2

```
Euclidean Algorithm
Enter a: 1029381029
Enter b>0: 1201233111
          1029381029=                  0*          1201233111 +          1029381029
          1201233111=                  1*          1029381029 +           171852082
          1029381029=                  5*           171852082 +           170120619
           171852082=                  1*           170120619 +             1731463
           170120619=                 98*             1731463 +              437245
             1731463=                  3*              437245 +              419728
              437245=                  1*              419728 +               17517
              419728=                 23*               17517 +               16837
               17517=                  1*               16837 +                 680
               16837=                 24*                 680 +                 517
                 680=                  1*                 517 +                 163
                 517=                  3*                 163 +                  28
                 163=                  5*                  28 +                  23
                  28=                  1*                  23 +                   5
                  23=                  4*                   5 +                   3
                   5=                  1*                   3 +                   2
                   3=                  1*                   2 +                   1
                   2=                  2*                   1 +                   0
GCD = 1
```

Why does Euclid's Algorithm work?

In each step in Euclid's algorithm, we replace a pair of numbers (a, b) with (b, r), where r is the remainder when a is divided by b. The point is that the greatest common divisor of this new, smaller pair of numbers is the same. Since each time we do this, the numbers get smaller, eventually one of them has to become zero. But the greatest common divisor of x and 0 is x, so at the last step the greatest common divisor is visible.

The key idea is that the replacement of a and b by b and r does not change the greatest common divisor.

Proposition: Let a and b be two integers with $b \neq 0$. Let q and r be integers so that $a = qb + r$. Then

$$\gcd(a, b) = \gcd(b, r)$$

.

Proof:

1. Let $d = \gcd(a, b)$.
2. Since $d|a$ and $d|b$, we know that $d|r$ because $r = a - qb$. (Property ii of divisibility).
3. d is a common divisor of b and r.
4. Let x be any common divisor of b and r. Then x divides a because $a = qb + r$. (Property ii of divisibility).
5. x is a common divisor of a and b. Therefore $x \leq d$.
6. Any common divisor of b and r is less than or equal to d so d is the greatest common divisor of b and r.
7. $d = \gcd(a, b) = \gcd(b, r)$.

Proof of Euclid's algorithm

Given a and b with $b \neq 0$, construct the sequence of remainders where r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, and r_k is the remainder when r_{k-2} is divided by r_{k-1}.

Proposition: There exists an N so that $r_N \neq 0$ and $r_{N+1} = 0$, and this $r_N = \gcd(a, b)$.

Proof:

1. The sequence of remainders is (strictly) decreasing and and all remainders are greater than or equal to zero, so the sequence must eventually reach zero.
2. By the proposition on the previous slide (2.21 in the book) the greatest common divisor of r_i and r_{i+1} is the same as that of a and b.

3. The greatest common divisor of r_N and r_{N+1} is r_N since $r_{N+1} = 0$.

The extended euclidean algorithm

See page 31. Given integers a and b, construct a table:

a	b		q
1	0	a	
0	1	b	

The next row of the table is constructed by 1: divide a by b to get q and r, and write them as follows:

a	b		q
1	0	a	
0	1	b	
		r	q

Then fill in the two left most columns by calculating (row-2)-q(row-1).

a	b	r	q
1	0	a	
0	1	b	
1	-q	r	a

Then repeat this process until you get a zero in the r column.

An example

a	b	r	q
1	0	1534	0
0	1	87	0
1	-17	55	17
-1	18	32	1
2	-35	23	1
>	-3	53	9
8	-141	5	2
-11	194	4	1

a	b	r	q
19	-335	1	1

Linear Combinations

Theorem: Let a and b be integers with $b \neq 0$. Then there are integers x and y so that $ax + by = d$ where d is the greatest common divisor of a and b. Conversely, if d is a common divisor of a and b so that there exist integers x and y such that $ax + by = d$, then d is the greatest common divisor of a and b.

Proof: Each row of the extended GCD algorithm has x, y in the columns headed a, b. And each row satisfies $ax + by = r$ where r is the entry in that column. The last row has the greatest common divisor in the r column, so those x and y give the solution. (Strictly speaking this is a proof by induction).

Conversely, suppose d is a common divisor of a and b and $ax + by = d$ for some x and y. Let f be any other common divisor. Then f divides $ax + by$ so f divides d so $d \geq f$. Thus d must be the greatest common divisor.

A more complete proof

Proposition: Let a and b be integers with $b \neq 0$ and let d be the greatest common divisor of a and b. Then there exist integers x and y so that

$$ax + by = d.$$

Proof: Let

$$S = \{ax + by : x, y \in \mathbb{Z}\}.$$

Both b and $-b$ belong to S, and therefore the subset of S consisting of positive elements is non-empty. Let d be the smallest positive element of S, which exists by the well-ordering principle. I will show first that d is a common divisor of a and b, and then that it is the greatest common divisor.

Use the division algorithm to write $a = qd + r$ with $0 \leq r < d>$ Then $a = q(ax+by)+r$ and so $(1-qx)a+bqy = r$. This shows that $r \in S$. Since $0 \leq r < d$, and d is the smallest positive element of S, we must have $r = 0$ and therefore $d|a$. Repeating the argument with b shows that $d|b$, so d is a common divisor of a and b.

To show that d is the greatest common divisor, let $s > 0$ be any common divisor. Then since $s|a$ and $s|b$, we know that $s|(ax + by)$ and so $s|d$. Therefore $s \leq d$, so d is the largest common divisor.

Other consequences.

Let a and b be integers with $b \neq 0$ and let d be their greatest common divisor.

- $d = 1$ if and only if there are x and y so that $ax + by = 1$.
- The greatest common divisor of a/d and b/d is 1.
- Let u be any common divisor of a and b. Then $a|d$.

Also the following important fact.

Proposition: Suppose a, b, c are integers and $\gcd(a, c) = 1$. If $a|bc$ then $a|b$.

Proof: $ax + cy = 1$ so $abx + bcy = b$. Since a divides ab and a divides bc we have $a|b$.