MATH 115, SUMMER 2012
LECTURE 2
TUESDAY, JUNE 19TH

JAMES MCIVOR

– Review of last time
- remind course website
- HW1 due next Tuesday
- Quiz 1 on Thursday
- Just call me "James" - I'm not a professor or doctor (yet!)
What we discussed last time:

(1) Defined divisibility
(2) Defined ideals
(3) Relation between divisibility and ideals: $a|b$ iff $b \in (a)$
(4) Division Alg. Note $a|b$ iff remainder is zero when you divide b by a.
(5) Finally, we proved that every ideal in $\mathbb{Z}$ is principal.

We also defined the gcd of two integers. Now we see how this relates to ideals.

1. Ideals and the gcd

– NOTE: this section contains material not covered in the book –

Theorem 1. *For a, b any two integers, the set of all $\mathbb{Z}$-linear combinations $ax+by$ (where $x, y \in \mathbb{Z}$) is an ideal, and it's generated by the gcd of a and b.*

We saw yesterday that it's an ideal, call it I. By the theorem about principal ideals, I is generated by some g, which therefore divides everything in I, so in particular it's a common divisor of a and b. But why is it the *greatest*? Well, since g is in I, it can be written in the form $g = ax + by$ (by def of I). If g' is any other common divisor of a and b, then since $g'|a$ and $g'|b$, we have $g'|ax + by = g$, so $g' \leq g$. So g is the biggest of all the common divisors.

We can generalize the gcd to more than two numbers as follows. If $a_1, \ldots, a_n$ are any integers, not all zero, then a common divisor of the a_i is any integer which divides each of them. Their gcd is the largest of these. It is expressible as a linear combination

$$a_1x_1 + \ldots + a_nx_n$$

since the set of such linear combinations forms an ideal, and we can use the same type of argument as above.

This is the standard type of question you will be asked concerning gcds:

Example 1.1 (Typical Exam Question!). Find integers x and y for which

$$1236x + 417y = -6$$

The first thing you should ask is: how do we even know that such x and y exist? Well, what do we know? For each choice of x and y, we get a $\mathbb{Z}$-linear combination

of 1236 and 417. By the theorem above, the set of all such linear combination is an ideal, generated by the gcd $(1236, 417)$. So this thing will only have a solution if -6 is in the ideal generated by the gcd of 1236 and 417. Let us first find this gcd, as follows. Divide 1236 by 417:

$$1236 = 2 \cdot 417 + 402$$

Now divide 417 by the first remainder, 402:

$$417 = 1 \cdot 402 + 15$$

Now divide 402 by the second remainder, 15:

$$402 = 26 \cdot 15 + 12$$

Keep going...

$$15 = 1 \cdot 12 + 3$$
$$12 = 4 \cdot 3 + 0$$

Eventually you will get a remainder zero. The gcd is the remainder from the previous line, in this case 3. And since $-6 \in (3)$, we will be able to find a solution. To actually get the x and y, we first write the gcd as a linear combination of 1236 and 417, by backtracking through the above calculations. Starting with the final remainder, 3, you solve for the remainder, and substitute in the smaller of the other two terms by solving the equation immediately above. Here's how it looks in this example. I'll boldface the things I'm substituting:

$$\begin{aligned} 3 &= 15 - 1 \cdot \mathbf{12} \\ &= 15 - 1 \cdot (\mathbf{402} - \mathbf{26} \cdot \mathbf{15}) \\ &= 27 \cdot \mathbf{15} - 1 \cdot 402 \\ &= 27 \cdot (\mathbf{417} - \mathbf{402}) - 1 \cdot 402 \\ &= 27 \cdot 417 - 28 \cdot \mathbf{402} \\ &= 27 \cdot 417 - 28 \cdot (\mathbf{1236} - \mathbf{2} \cdot \mathbf{417}) \\ &= -28 \cdot 1236 + 83 \cdot 417 \end{aligned}$$

Notice that at every other step we're substituting out the smaller of the two terms which appear above. Anyway, we can build the gcd, 3, of 1235 and 417 using the scalars -28 and 83, respectively. But the question asks us to build -6, not 3! Since -6 is -2 times 3, we just take the scalars -28 and 83, and multiply them by -2. Thus our solution is

$$x = 56, \quad y = -166$$

In fact, there are many other choices of x and y that work - infinitely many! To see why, just notice that we're looking for points (x, y) on a certain line in $\mathbb{R}^2$, but we're only interested in the pairs where x and y are integers (as opposed to arbitrary real numbers). But its slope is a rational number, so if there's one such point there will be infinitely many.

2. Properties of GCD

We can use ideals to quickly verify some useful properties of the gcd.

Proposition 1. *Let a, b be any two integers not both zero, m any positive integer, and set $g = (a, b)$. Then*

(1) $(ma, mb) = mg$.
(2) *If* $d > 0$ *divides both* a *and* b*, then* $(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}g$.
(3) *In particular,* $(\frac{a}{g}, \frac{b}{g}) = 1$
(4) *If* $(a, m) = (b, m) = 1$*, then* $(ab, m) = 1$.
(5) $(a, b) = (b, a) = (a, -b) = (a, b + ax)$*, where* x *can be any integer.*

- 2 and 3 say we can "divide through" by any common divisors of a and b (including the greatest common divisor).

- 4 is very useful - it says we need only consider positive integers when computing gcd, and also that we can "translate" b by some multiples of a and get the same result.

- for part 5, we'll need the following observation. Every ideal is principal, as we've seen, so there's a generator, which could be positive or negative - both will work. But there's exactly one positive generator. That's the gcd.

Proof. We use ideals. See your book for a treatment without the use of ideals. The arguments are basically the same, though, just in a different language.

(1) Put $I = \{\mathbb{Z}\text{-linear combos of } a, b\}$. Then $\{\mathbb{Z}\text{-linear combos of } ma, mb\} = m\{\mathbb{Z}\text{-linear combos of } a, b\} = mI$, and $I = (g)$, so $mI = (mg)$.
(2) Same as above, but with $\frac{1}{d}$ instead of m. This makes sense, since multiplying either a or b by $\frac{1}{d}$ always gives an integer.
(3) Special case of 2
(4) Define three ideals $I_1 = \{ax + my | x, y \in \mathbb{Z}\}$, $I_2 = \{bx + my | x, y \in \mathbb{Z}\}$, $I_3 = \{abx + my | x, y \in \mathbb{Z}\}$. We're given that $I_1 = I_2 = \mathbb{Z}$, ie, they're as big as possible. We want $I_3 = \mathbb{Z}$, so can show I_3 contains I_1. Only thing that contains $\mathbb{Z}$ is $\mathbb{Z}$ itself!

    To show $I_1 \subseteq I_3$, we know $m \in I_3$, so just need $a \in I_3$. Since $I_2 = \mathbb{Z}$, we have

    $$bx + my = 1$$

    for some x, y. Multiply by a and find that a is a linear combo of ab and m, so $a \in I_3$.
(5) Any $\mathbb{Z}$-linear combination of a and b is also a $\mathbb{Z}$-linear combination of b and a is also a $\mathbb{Z}$-linear combination of a and $-b$ is also a $\mathbb{Z}$-linear combination of a and $b + ax$. These ideals are all the same, so their unique positive generators are the same.

□

When the gcd of two integers is 1, we say they are **coprime**, or **relatively prime**, or sometimes **prime to each other**.