Math 312, lecture 2, 16/5/2018

- Webwork: Click "webwork link", close ww, click "ww1".
- PS1 updated

Today: The GCD

Last time: $\mathbb{Z}$, induction (& well-ordering)
divisibility, division thm.

Easy observation: if $a|b$, and $a|c$ then $a|b \pm c$

Pf: $b \pm c = a\left(\frac{b}{a} \pm \frac{c}{a}\right)$.

Cor: Only positive common divisor of $n, n+1$ is 1:
if $a|n$ and $a|n+1$ then $a|(n+1)-n$ i.e. $a|1$.

$\Rightarrow |a| \leq 1$ so $a = 1$

Aside: $a|b$ iff $-a|b$ so only study positive divisors.

Problems: (1) Find all divisors of n
(2) Find the common divisors of n, m.
(3) Find the greatest common divisor of n, m

Note: (1) currently hard, (2) is the divisors of the $\gcd(n,m)$
(3) can be done efficiently

Notation: $(a,b) = \gcd(a,b) = \gcd(\{a,b\}) =$ greatest common divisor of a,b (if both $a=b=0$, set $\gcd(a,b)=0$)

$[a,b] = \operatorname{lcm}(a,b) = \operatorname{lcm}(\{a,b\}) =$ least positive common multiple of a,b. (undef if $a=0$ or $b=0$)

Why do they exist? gcd: $1 \mid a$, $1 \mid b$ and if $d \mid a$ then $d \le |a|$

lcm: $|a| \cdot |b|$ is a common multiple

Lemma: (Euclid): $(a,b) = (a-b, b)$

Pf: the pairs $\{a,b\}$, $\{a-b, b\}$ have same sets of common divisors: if $d \mid a$ and $d \mid b$ then $d \mid a-b$
if $d \mid a-b$ and $d \mid b$ then $d \mid a = (a-b)+b$

Also, $(a,0) = |a|$ for all a, and changing sign of a,b has no effect.

Algorithm: (Euclid) Given $a,b \in \mathbb{Z}$ output their gcd:

(1) Replace a with $|a|$, b with $|b|$.
(2) If $a<b$, exchange a,b
(3) If $b=0$, output a, terminate
(4) If not replace a with $a-b$, go to step 2

Thm: The algorithm terminates in finitely many steps, outputting gcd(input)

Pf: the quantity $|a|+|b|$ strictly decreases every time we pass step 4. (by at least $b \geq 1$)

If we passed step 4 infinitely many times, the set of values this quantity takes would not have a least member.

Also, gcd(a,b) is unchanged as algorithm replaces a,b (Euclid's lemma), so output is correct.

Corollary: (Bezout's theorem): there are $x, y \in \mathbb{Z}$ s.t. $\gcd(a,b) = xa + yb$

Pf: Every value considered by algorithm has this form. True by induction on steps of algorithm:

say a,b initial values.

step (1): $|a| = (\pm 1)a + 0 \cdot b$, $|b| = 0 \cdot a + (\pm 1) \cdot b$

(2): swapping not a problem

(3): — (proves gcd has desired form)

(4): say we had a', b' : $a' = xa + yb$

$b' = za + wb$

then $a' - b' = (x-z)a + (y-w)b$ of desired form

Since $(a,0)=a$ for all a, and since changing the signs of a,b does not change their gcd (why?) we get a method for calculating the gcd of any two integers. For example:

$$\begin{aligned}
(24,-153) &= (153,24) \\
&= (129,24) \\
&= (105,24) \\
&= (81,24) \\
&= (57,24) \\
&= (33,24) \\
&= (24,9) \\
&= (15,9) \\
&= (9,6) \\
&= (6,3) \\
&= (3,3) \\
&= (3,0) \\
&= 3.
\end{aligned}$$

$153 = (-1)\cdot 153$

$129 = 153 - 24 = -1(153) + 1\cdot 24$

$9 = 153 - 6\cdot 24 = (-1)\cdot(-153) + (-6)\cdot 24$

$15 = 24 - 9 = 24 - ((-1)\cdot(-153) + (-6)\cdot 24)$
$= 1\cdot(-153) + 7\cdot 24$

$6 = 15 - 9 = (1\cdot(-153) + 7\cdot 24)$
$- (-1(-153) + (-6)\cdot 24)$
$= 2\cdot(-153) + 13\cdot 24$

So $3 = 9 - 6 = -3\cdot(-153) - 19\cdot 24$

ALGORITHM 24. *(Euclid) Given two integers a,b, output their* gcd*:*

(1) *Replace a with $|a|$, b with $|b|$.*
(2) *If $a<b$ exchange a and b.*
(3) *If $b=0$, terminate and output a.*
(4) *Else, replace a with $a-b$ and go to step 2.*

THEOREM 25. *The algorithm terminates after finitely many steps and outputs the* gcd *of (a,b).*

PROOF. Consider the changes in the quantity $|a|+|b|$ during the course of the algorithm. Every time we reach step 4, we know that $a \geq b > 0$. It follows that at the conclusion of step 4, the quantity has decreased by at least $b \geq 1$. Since there is no infinite strictly decreasing sequence of natural numbers (well-ordering), we can reach step 4 only finitely many times. In particular, at some point $b=0$ and we terminate. Finally, by Lemma 23, the replacements and exchanges never change the gcd of the two numbers. □

In fact, more can be said.

CLAIM 26. (Bezout) Every intermediate value considered by Euclid's Algorithm is of the form $xa+yb$ for some $x,y \in \mathbb{Z}$.

PROOF. We prove this by induction on the steps of the algorithm. Certainly this is true at the start, and also changing signs and exchanging a,b doesn't matter. Now assume that at the nth time we reach step 3, we are looking at the numbers $a' = xa+yb > b' = za+wb \geq 0$, where a,b are the initial values and $x,y,z,w \in \mathbb{Z}$. At step 4 we will then replace a' with

$$a'-b' = (x-z)a+(y-w)b$$

which is indeed also of this form, so the situation will hold when we reach step 3 for the $(n+1)$st time. □

We have thus proven (by algorithm) the following fact:

Alternative pf: Set $A = \{m > 0 \mid m = xa + yb \text{ for some } x, y\}$

show min A is the gcd

Prop: Every common divisor divides gcd

Pf: let d be a common divisor of a, b.

Then $d \mid xa$, $d \mid yb$ for any $x, y \in \mathbb{Z}$

so $d \mid xa + yb$, but $\gcd(a,b)$ has this form

so $d \mid \gcd(a,b)$.

Conversely, if $d \mid \gcd(a,b)$ then $d \mid \gcd(a,b) \mid a$ so $d \mid a$,

similarly $d \mid b$