Math 4460
2/13/23

The Euclidean algorithm can also be used to find a solution to the equation

$$ax + by = \gcd(a, b)$$

Ex: Last time we saw that $\gcd(578, 153) = 17$.

Let's find x, y where

$$578x + 153y = 17$$

Step 1: Use the Euclidean algorithm

$$\boxed{\begin{aligned} 578 &= 3 \cdot 153 + 119 \\ 153 &= 1 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}}$$

From Weds last week

Step 2: Disregard the last equation that has remainder $r=0$. Rewrite the other equations so that the remainder is on the left-hand side, that is solve for the remainder in each equation.

$$\boxed{\begin{aligned} 119 &= 1\cdot 578 - 3\cdot 153 \\ 34 &= 1\cdot 153 - 1\cdot 119 \\ 17 &= 1\cdot 119 - 3\cdot 34 \end{aligned}}$$

Step 3: Now start at the bottom equation (the one with the gcd) and back-substitute in using the equations above it until you are left with an expression of the form $ax+by$

$$17 = 1\cdot\boxed{119} - 3\cdot\boxed{34}$$

$$119 = 1\cdot 578 - 3\cdot 153$$
$$34 = 1\cdot 153 - 1\cdot 119$$
$$17 = 1\cdot 119 - 3\cdot 34$$

previous page

$$= 1\cdot\left(1\cdot\boxed{578} - 3\cdot\boxed{153}\right)$$
$$- 3\cdot\left(1\cdot\boxed{153} - 1\cdot\boxed{119}\right)$$

$$= 1\cdot\boxed{578} - 3\cdot\boxed{153} - 3\cdot\boxed{153} + 3\cdot\boxed{119}$$

$$= 1\cdot\boxed{578} - 6\cdot\boxed{153} + 3\cdot\boxed{119}$$

$$= 1\cdot\boxed{578} - 6\cdot\boxed{153} + 3\cdot\left(1\cdot\boxed{578} - 3\cdot\boxed{153}\right)$$

$$= 1\cdot\boxed{578} - 6\cdot\boxed{153} + 3\cdot\boxed{578} - 9\cdot\boxed{153}$$

$$= 4\cdot\boxed{578} - 15\cdot\boxed{153}$$

So, $\boxed{4\cdot 578 - 15\cdot 153 = 17}$

Thus,

$$\boxed{578(4)+153(-15)=17}$$

So, a solution to

$$578x+153y=17$$

is $x=4$ and $y=-15$.

Ex: Let

$$a = 60 = 10 \cdot 6$$
$$b = 350 = 10 \cdot 35$$

$$d = \gcd(a, b) = \gcd(60, 350) = 10$$

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \gcd\left(\frac{60}{10}, \frac{350}{10}\right)$$
$$= \gcd(6, 35)$$
$$= 1$$

Idea: If you divide a & b by their gcd, the resulting numbers have gcd 1. You're removing all the common factors.

Theorem: Let $a_1, a_2, \ldots, a_n$ be integers, not all equal to zero.
Let $d = \gcd(a_1, a_2, \ldots, a_n)$.
Then, $\gcd\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1$

Special case when $n=2$:

Let $a, b \in \mathbb{Z}$, not both zero.
Let $d = \gcd(a,b)$.
Then, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Proof: We will prove the $n=2$ case.
Look at the online notes if you want to see the general proof.

Let $a, b \in \mathbb{Z}$, not both zero.
Let $d = \gcd(a,b)$.
Let $d' = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$.

Our goal is to show that $d'=1$.

Since $d=\gcd(a,b)$ we know $d \mid a$ and $d \mid b$.

So, $\boxed{a=dx}$ and $\boxed{b=dy}$ where $x,y \in \mathbb{Z}$

Then, $d'=\gcd\left(\frac{a}{d},\frac{b}{d}\right) = \gcd(x,y)$

$a=dx$
$b=dy$

Consequently, $d' \mid x$ and $d' \mid y$.

since $d'=\gcd(x,y)$

Hence, $\boxed{x=d's}$ and $\boxed{y=d't}$ where $s,t \in \mathbb{Z}$.

Thus,

$$a = dx = dd's$$

$$b = dy = dd't$$

So, dd' is a common factor of a and b.

Note $\underbrace{d \geq 1}_{\text{def of gcd}}$ and $\underbrace{\boxed{d' \geq 1}}_{\text{def of gcd}}$ and so $\underbrace{dd' \geq 1}_{dd' \text{ is a positive integer}}$.

However, d is the greatest common divisor of a and b.

Ergo, $\boxed{dd' \leq d}$

Divide by d to get $\boxed{d' \leq 1}$

Since $1 \leq d'$ and $d' \leq 1$

We know $d' = 1$. $\blacksquare$

Theorem: Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$.

If $\gcd(c, a) = 1$ and $c \mid ab$,

then $c \mid b$.

Ex: $3 \mid 30$

$3 \mid 5 \cdot 6 \longrightarrow 3 \mid 6$

c a b

$\gcd(3,5) = 1$

proof: Suppose $\gcd(c, a) = 1$ and $c \mid ab$.

Since $\gcd(c, a) = 1$ we know there exist $x_0, y_0 \in \mathbb{Z}$ where

$$\boxed{1 = c x_0 + a y_0}$$

Since $c \mid ab$ there exists $k \in \mathbb{Z}$ where $\boxed{ab = ck}$.

Multiply $1 = cx_0 + ay_0$ by b to get $\boxed{b = cbx_0 + aby_0}$

Sub in $ab = ck$ to get $\boxed{b = cbx_0 + cky_0}$.

Thus,

$$b = c[\underbrace{bx_0 + ky_0}_{\text{this is an integer}}]$$

Therefore, $c \mid b$. $\blacksquare$

$\boxed{\text{GCD METHODS}}$

$\boxed{d = \gcd(a,b)}$

1. $d \mid a$, $d \mid b$
2. If $d' \mid a$ and $d' \mid b$ then $d' \leq d$
3. $ax_0 + by_0 = d$ for some $x_0, y_0 \in \mathbb{Z}$