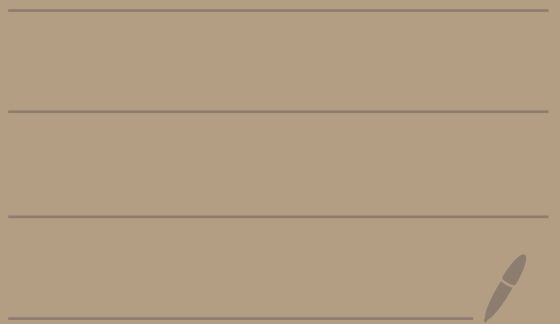


Math 4460

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

$$578 = 3 \cdot 153 + 119$$

$$153 = 1 \cdot 119 + 34$$

$$119 = 3 \cdot 34 + 17$$

$$34 = 2 \cdot 17 + 0$$

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.

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

$$34 = 1 \cdot 153 - 1 \cdot 119$$

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

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 $ax+by$

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

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

previous page

$$\begin{aligned} &= 1 \cdot 578 - 3 \cdot 153 - 3 \cdot 153 + 3 \cdot 119 \\ &= 1 \cdot 578 - 6 \cdot 153 + 3 \cdot 119 \\ &= 1 \cdot 578 - 6 \cdot 153 + 3 \cdot (1 \cdot 578 - 3 \cdot 153) \\ &= 1 \cdot 578 - 6 \cdot 153 + 3 \cdot 578 - 9 \cdot 153 \\ &= 4 \cdot 578 - 15 \cdot 153 \end{aligned}$$

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

Thus,

$$578(4) + 153(-15) = 17$$

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, \dots, a_n be integers, not all equal to zero.

Let $d = \gcd(a_1, a_2, \dots, a_n)$.

Then, $\gcd\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = 1$

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 $d|a$
and $d|b$.

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

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

$$\begin{array}{l} a = dx \\ b = dy \end{array}$$

Consequently, $d'|x$ and $d'|y$.

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

Hence, $x = d's$ and $y = d't$ 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 $d \geq 1$ and $d' \geq 1$ and so $dd' \geq 1$.

def of
gcd

def of
gcd

dd' is a
positive integer

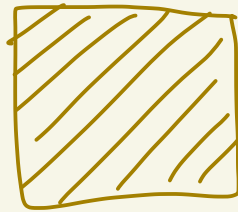
However, d is the greatest common divisor of a and b .

Ergo, $dd' \leq d$

Divide by d to get $d' \leq 1$

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

We know $d' = 1$.



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: $3 \mid 30$

$$3 \mid 5 \cdot 6 \rightarrow 3 \mid 6$$

$$\begin{array}{ccc} \uparrow & \uparrow & \uparrow \\ c & a & b \end{array}$$

$$\gcd(3, 5) = 1$$

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

$$1 = cx_0 + ay_0$$

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

Multiply $1 = cx_0 + ay_0$ by b
to get $b = cbx_0 + aby_0$

Sub in $ab = ck$ to get

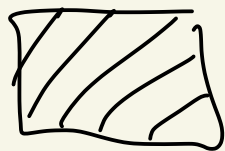
$$b = cbx_0 + cky_0.$$

Thus,

$$b = c \left[bx_0 + ky_0 \right]$$

this is an integer

Therefore, $c \mid b$.



GCD METHODS

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

- 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 $x_0, y_0 \in \mathbb{Z}$