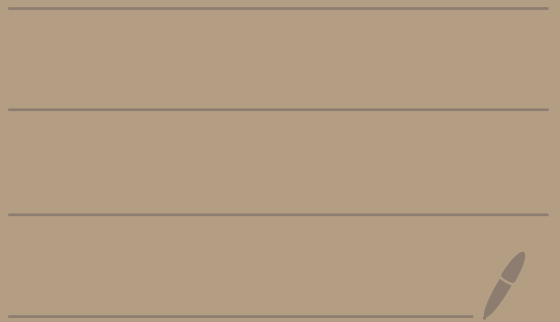


Math 4460

2/12/25



Last time we learned
the Euclidean algorithm.
We can also use it to
find x_0, y_0 that solve

$$ax_0 + by_0 = \gcd(a, b)$$

Ex: Last time we found
that $\gcd(578, 153) = 17$.
Let's find x_0, y_0 where

$$578x_0 + 153y_0 = 17$$

Step 1: Use the Euclidean
algorithm.

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

From
Monday

Step 2: Disregard the last equation where $r=0$.

Rewrite the other equations by solving for the r in each of them.

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

$$34 = 1 \cdot \boxed{153} - 1 \cdot \boxed{119} \quad \textcircled{2}$$

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

Step 3: Start with the last equation and backsubstitute until only 578's and 153's are left.

We get

$$\begin{aligned} 119 &= 1 \cdot 578 - 3 \cdot 153 & \textcircled{1} \\ 34 &= 1 \cdot 153 - 1 \cdot 119 & \textcircled{2} \\ 17 &= 1 \cdot 119 - 3 \cdot 34 & \textcircled{3} \end{aligned}$$

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

$$\stackrel{\textcircled{1}/\textcircled{2}}{=} 1 \cdot \left(1 \cdot 578 - 3 \cdot 153 \right)$$

119

$$- 3 \cdot \left(1 \cdot 153 - 1 \cdot 119 \right)$$

34

consolidate terms

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

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

{consolidate terms}

$$= 4 \cdot 578 - 15 \cdot 153$$

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

Thus,

$$578 \underbrace{(4)}_{x_0=4} + 153 \underbrace{(-15)}_{y_0=-15} = 17$$

Ex: Let

$$a = 60 = 10 \cdot 6$$

$$b = 350 = 10 \cdot 35$$

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

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

$$= \gcd(6, 35) = 1$$

If you divide a & b by their \gcd , the resulting numbers have $\gcd 1$.

You're removing the common factor

I
D
E
A

Theorem: Let a_1, a_2, \dots, a_n
be integers, not all zero.

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

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

Specific case $n=2$:

Let $a, b \in \mathbb{Z}$, not both zero.

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

Then, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

We will prove the specific
case. In my notes online
it has the general case.

proof when $n = 2$:

Let $d = \gcd(a, b)$
and $d' = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$.

Goal is to show $d' = 1$.

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

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

Then,

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

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

Thus, $x = d'r$ and $y = d's$

where $r, s \in \mathbb{Z}$.

So,

$$a = dx = dd'r$$

$$b = dy = dd's$$

Thus, dd' is a positive common divisor of a and b .

But d is the greatest common divisor of a and b .

Thus, $dd' \leq d$.

So, $d' \leq 1$.

But $d' = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$ so

$$1 \leq d'$$

Thus, $d' = 1$.



Second proof:

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

We know there exists

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

$$ax_0 + by_0 = d.$$

Thus,

$$\left(\frac{a}{d}\right)x_0 + \left(\frac{b}{d}\right)y_0 = 1$$

these are integers
because $d|a$ and $d|b$

Let $d' = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$.

So, $d' \mid \frac{a}{d}$ and $d' \mid \frac{b}{d}$

Thus, $\frac{a}{d} = d'r$ and $\frac{b}{d} = d's$

where $r, s \in \mathbb{Z}$.

So, $d'r x_0 + d's y_0 = 1$

Thus, $d'[r x_0 + s y_0] = 1$.

So, $d' \mid 1$. \leftarrow $d' = \pm 1$

Since d' is a gcd we know $d' \geq 1$.

Thus, $d' = 1$.



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: $3 \mid 30$

$$\begin{array}{ccc} 3 \mid 5 \cdot 6 & \xrightarrow{\gcd(3,5)=1} & 3 \mid 6 \\ \uparrow \quad \uparrow \quad \uparrow & & \\ c \quad a \quad b & & \end{array}$$

proof:

Since $\gcd(a, c) = 1$ we get

$$ax_0 + cy_0 = 1 \quad (1)$$

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

Since $c \mid ab$ we get

$$ab = ck \quad (2)$$

for some $k \in \mathbb{Z}$

Multiply (1) by b to get

$$abx_0 + cby_0 = b$$

Then use (2) $ab = ck$ to get

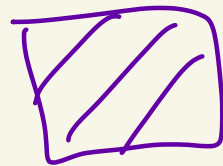
$$ckx_0 + cby_0 = b$$

So,

$$c \underbrace{[kx_0 + by_0]} = b$$

is an integer

Thus, $c|b$.



GCD proof methods

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

Facts to use:

① $ax_0 + by_0 = d$

where x_0, y_0
are integers

② $d|a$ and $d|b$

d is a
common
divisor

③ If $d'|a$ and $d'|b$
then $d' \leq d$

d is the
greatest
common
divisor

