Math 4460
2/10/25

Test 1 study guide and practice tests are online

We are going to learn the Euclidean algorithm which calculates $\gcd(a,b)$

<u>Theorem:</u> Let a and b be positive integers and $0 < a \leq b$.
Suppose $b = aq + r$ where $r, q \in \mathbb{Z}$ and $0 \leq r < a$.

Then,
$$\gcd(b,a) = \gcd(a,r)$$

<u>proof:</u> Let $a, b \in \mathbb{Z}$ with

$0 < a \le b$. And,

$b = aq + r$ with $0 \le r < a$.

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

$d' = \gcd(a, r)$

Goal: Show $d = d'$.

Part 1: Let's show $d' \le d$.

Since $d' = \gcd(a, r)$ we know

that $d' \mid a$ and $d' \mid r$.

Then, $a = d'k$ and $r = d'l$

where $k, l \in \mathbb{Z}$.

So, $b = aq + r = d'kq + d'l$

$= d'[kq + l]$

an integer

Consequently, $d'|b$.

Since $d'|a$ and $d'|b$ we have that d' is a positive common divisor of a and b.

But, $d = \gcd(b,a)$ is the greatest positive common divisor of a and b.

Therefore, $d' \leq d$.

Part 2: Let's show $d \leq d'$.

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

So, $b = dm$ and $a = dn$ where $m, n \in \mathbb{Z}$.

Then,

$$\begin{aligned} r &= b - qa \\ &= dm - qdn \\ &= d\underbrace{(m - qn)}_{\text{an integer}} \end{aligned}$$

Thus, $d \mid r$.

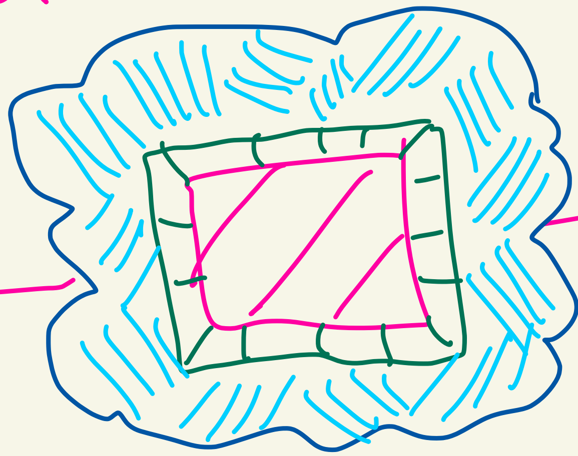
Since $d \mid a$ and $d \mid r$ we know d is a positive common divisor of a and r.

Since $d' = \gcd(a, r)$ this implies that $d \leq d'$.

Parts 1 and 2 showed

$d' \leq d$ and $d \leq d'$.

Thus, $d = d'$.



Euclidean Algorithm (Finds $\gcd(b,a)$)

Let $a, b \in \mathbb{Z}$ with $0 < a \leq b$.

<u>Step 1:</u> Divide a into b to get

$$b = aq + r$$

with $0 \leq r < a$

<u>Step 2:</u>

- If $r = 0$, then you are done. The answer is a.
- If $r > 0$, then repeat step 1 but with b replaced by a and a replaced by r.

Ex: Calculate gcd(138, 62)

$$138 = 62(2) + 14$$
$$62 = 14(4) + 6$$
$$14 = 6(2) + 2$$
$$6 = 2(3) + 0$$

$$\boxed{\begin{aligned} &\gcd(138, 62) \\ &= \gcd(62, 14) \\ &= \gcd(14, 6) \\ &= \gcd(6, 2) \\ &= \gcd(2, 0) \\ &= 2 \end{aligned}}$$

Thus, $\gcd(138, 62) = 2$

$\begin{array}{r} 2 \\ 62\overline{)138} \\ -124 \\ \hline 14 \end{array}$	$\begin{array}{r} 4 \\ 14\overline{)62} \\ -56 \\ \hline 6 \end{array}$	$\begin{array}{r} 2 \\ 6\overline{)14} \\ -12 \\ \hline 2 \end{array}$	$\begin{array}{r} 3 \\ 2\overline{)6} \\ -6 \\ \hline 0 \end{array}$

Ex: Find $\gcd(578, 153)$

$$578 = 153(3) + 119$$
$$153 = 119(1) + 34$$
$$119 = 34(3) + 17$$
$$34 = 17(2) + 0$$

$$\boxed{\begin{aligned} &\gcd(578,153) \\ &= \gcd(153,119) \\ &= \gcd(119,34) \\ &= \gcd(34,17) \\ &= \gcd(17,0) \\ &= 17 \end{aligned}}$$

Thus,

$$\gcd(578, 153) = 17$$

$\begin{array}{r} 3 \\ 153\overline{)578} \\ -459 \\ \hline 119 \end{array}$	$\begin{array}{r} 1 \\ 119\overline{)153} \\ -119 \\ \hline 34 \end{array}$	$\begin{array}{r} 3 \\ 34\overline{)119} \\ -102 \\ \hline 17 \end{array}$	$\begin{array}{r} 2 \\ 17\overline{)34} \\ -34 \\ \hline 0 \end{array}$

Hw 1 - 7(a)

Let $n > 1$ be an integer.
n is composite if and only if there exist positive integers a and b where $n = ab$ and $1 < a < n$ and $1 < b < n$

proof: Let $n > 1$.

($\Rightarrow$) Assume n is composite.
So n is not prime.
Thus, there is a positive divisor a of n where $a \neq 1$ and $a \neq n$.
From class day 1 and $a \neq n$ this implies $a < n$.
Since $a \neq 1$ we get $1 < a$.

Since $a|n$ we know $n = ab$ where $b \in \mathbb{Z}$.

We know $1 < a < n$.

Then, $1 > \frac{1}{a} > \frac{1}{n}$.

So, $n > \underbrace{\frac{n}{a}}_{b} > 1$

Thus, $n > b > 1$.

So, $n = ab$ with $1 < a < n$ and $1 < b < n$.

($\Leftarrow$) Suppose $n = ab$ with $1 < a < n$ and $1 < b < n$.

Then, $a|n$ and $a \neq 1$ and $a \neq n$ and a is positive.

So, n is not prime.

So, n is composite.

$\blacksquare$