Math 4460
2/8/23

We want an algorithm to calculate $\gcd(a,b)$.

The next theorem will be the basis for the Euclidean Algorithm

---

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

Then,

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

We replace this problem with a smaller problem

Ex: Calculate gcd(138, 62)

$$\boxed{138 = 62(2) + 14}$$

$$\begin{array}{r} 2 \\ 62\overline{)\,138} \\ -124 \\ \hline 14 \end{array}$$

$\boxed{r}$

Theorem says:

$\gcd(138, 62) = \gcd(62, 14)$

Repeat the process:

$$\boxed{62 = 14(4) + 6}$$

$$\begin{array}{r} 4 \\ 14\overline{)\,62} \\ -56 \\ \hline 6 \end{array}$$

$\boxed{r}$

Theorem says:

$\gcd(62, 14) = \gcd(14, 6)$

Repeat the process:

$$\boxed{14 = 6(2) + 2}$$

$$\begin{array}{r} 2 \\ 6\overline{)\,14} \\ -12 \\ \hline 2 \end{array}$$

$\boxed{r}$

Theorem says:

$\gcd(14, 6) = \gcd(6, 2)$

Repeat the process:

$$\boxed{6 = 2(3) + 0}$$

$$\begin{array}{r} 3 \\ 2\overline{)\,6} \\ -6 \\ \hline 0 \end{array}$$

$\boxed{r}$

Theorem says:

$$\gcd(6,2) = \gcd(2,0)$$

Summary:

$$\gcd(138,62) = \gcd(62,14) = \gcd(14,6)$$
$$= \gcd(6,2) = \gcd(2,0) = 2$$

$$\boxed{\text{Answer: } \gcd(138,62) = 2}$$

proof of theorem:

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

Use the division algorithm to write $b = aq + r$ with $0 \leq r < a$.

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

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

Step 1: Let's show $d' \leq d$.

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

So, $a = d'm$ and $r = d'n$ where $m, n \in \mathbb{Z}$.

Ergo,

$$\begin{aligned} b &= aq + r \\ &= d'mq + d'n \\ &= d'\underbrace{[mq+n]}_{\substack{\text{this is an integer} \\ \text{because } m,\, q,\, n \\ \text{are integers.}}} \end{aligned}$$

Consequently, $d' \mid b$.

Thus, $d' \mid b$ and $d' \mid a$.

So, d' is a positive common divisor of b and a.

But d is the greatest positive

common divisor of b and a.

Thus, $\boxed{d' \leq d}$.

Step 2: Let's show $d \leq d'$

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

$d \mid a$ and $d \mid b$.

Hence,

$a = ds$ and $b = dt$

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

It follows that

$$\begin{aligned} r &= b - aq \\ &= dt - dsq \end{aligned}$$

$$= d\underbrace{[t - sq]}_{\text{this is an integer since } t,s,q\in\mathbb{Z}}$$

So, $d \mid r$.

Hence, $d \mid a$ and $d \mid r$.

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

Therefore, since $d' \le d$ and $d \le d'$, we may conclude that $d = d'$. $\blacksquare$

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

Let a and b be positive integers with $0 < a \leq b$.

Step 1: Divide a into b to get

$$b = aq + r$$

with $0 \leq r < a$.

Step 2:

If $r = 0$, then you're done. The answer is a.

If $r \neq 0$, then repeat step 1 but with b replaced by a and a replaced by r.

$\boxed{\text{While loop}}$

```
a = #;
b = #;
r = remainder[b, a];
While[r ≠ 0,
    b = a;
    a = r;
    r = remainder[b, a];
];
Print[r];
```

Recursion method

```
gcd(b, a) := [

    r = remainder[b, a];
  If [r = 0,
      return[a];
    else
      return[gcd(a, r)];
    ];
];
```

Ex: Find gcd(578, 153)

$$578 = 3 \cdot 153 + 119$$
$$153 = 1 \cdot 119 + 34$$
$$119 = 3 \cdot 34 + 17$$
$$34 = 2 \cdot 17 + 0$$

Answer

$$\boxed{\gcd(578,153) = 17}$$

$$\gcd(578,153)$$
$$= \gcd(153,119)$$
$$= \gcd(119,34)$$
$$= \gcd(34,17)$$
$$= \gcd(17,0)$$
$$= 17$$

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

Hw 1 # 7(a) $n \in \mathbb{Z}, n > 1$.

n is composite iff $n = ab$ where $1 < a < n, 1 < b < n$.

proof:

($\Leftarrow$) Suppose $n = ab$ where $1 < a < n$, $1 < b < n$, $a, b \in \mathbb{Z}$.

So, a is a divisor of n with $a \neq 1$, $a \neq n$.

Thus, n is not prime (ie composite)

($\Rightarrow$) Suppose n is composite.

This means n is not prime.

Thus there exists a positive divisor a of n where $a \neq 1$ and $a \neq n$.

So, $1 < a < n$ since $a \mid n$.

Since $a \mid n$ we know

$n = ab$ where $b \in \mathbb{Z}$.

Since a & n are positive, so is b.

We have $b = \frac{n}{a}$.

Then, $1 < \frac{n}{a} = b$

because $a < n$

And, $b = \frac{n}{a} < n$

because $1 < a$
so $\frac{1}{a} < \frac{1}{1}$.

So, $1 < b < n$.

So, $n = ab$ where

$1 < a < n$, $1 < b < n$. ▨