GREATEST COMMON DIVISOR
EUCLIDEAN ALGORITHM

6/23/17

<u>Euclid's Algorithm</u> for find the gcd is of the form

$$gcd(x, y) = gcd(y, rem(x, y))$$

for example,

$$gcd(72, 26) = gcd(26, \underbrace{72 - \lfloor 72/26 \rfloor \cdot 26}_{r=20})$$

one way to find remainder or use a%b

$$= gcd(20, \underbrace{26 \% 20}_{r=6})$$

$$= gcd(6, \underbrace{rem(20, 6)}_{r=2})$$

$$= gcd(2, \underbrace{r(6, 2)}_{r=0})$$

Stop when b of gcd(a,b) is 0, then a is final gcd

so $\boxed{gcd(72, 26) = 2}$

It is interesting to note that each iteration of the gcd is exactly equal to its predecessor, for instance

$$gcd(72, 26) = gcd(26, 20) = gcd(6, 2) = 2$$

Recursive Implementation

```
gcd(a,b) {
    while b ≠ 0
        gcd(b, a%b)
    end while
    return a
}
```

Iterative Implementation

```
gcd(a,b) {
    while b ≠ 0
        temp_a = a
        a = b
        b = temp_a % b
    end while
    return a
```

6/23/17

EXTENDED EUCLIDEAN ALGORITHM FOR GCD
PULVERIZER / BEZOUT'S IDENTITY

The <u>Extended Euclidean Algorithm</u> (Bezout's Identity) not only calculates the gcd as done using the general Euclidean Algorithm $gcd(x,y) = gcd(y, rem(x,y))$ until $y_i = 0$, then x_i is the gcd, but additionally computes scalars c, d at each step such that we can express the current terms of the gcd x_i, y_i as a linear combination of the original x_0, y_0 as $x_i = c x_0 + d y_0$ and similarly we express y_i as $y_i = e x_0 + f y_0$

<u>Example</u>

	i	a , b	q	r	c , d	e , f	linear combinations
gcd (899, 493)	0	899, 493	1	406	1 0	0 1	$899 = 1 \cdot 899 + 0 \cdot 493$
gcd (493, 406)	1	493, 406	1	87	0 1	1 -1	$493 = 0 \cdot 899 + 1 \cdot 493$
gcd (406, 87)	2	406, 87	4	58	1 -1	-1 2	$406 = 1 \cdot 899 + -1 \cdot 493$
gcd (87, 58)	3	87, 58	1	29	-1 2	5 -9	$87 = -1 \cdot 899 + 2 \cdot 493$
gcd (58, 29)	4	87, 29	2	0	5 -9	-6 11	$58 = 5 \cdot 899 + -9 \cdot 493$
gcd (29, 0)	5	29, 0					b=0 so STOP a=29 this is gcd

<u>Pseudo code</u>

Current step
$$\begin{cases} a_i = c_i X + d_i Y \\ b_i = e_i X + f_i Y \\ q_i = \lfloor a_i / b_i \rfloor \\ r_i = a_i - q_i b_i \end{cases}$$

update steps
$$\begin{cases} a_i = b_{i-1} \\ b_i = r_{i-1} \\ c_i = e_{i-1} \\ d_i = f_{i-1} \\ e_i = c_{i-1} - q_{i-1} \cdot e_{i-1} \\ f_i = d_{i-1} - q_{i-1} \cdot f_{i-1} \end{cases}$$

$$b_{i+1} = r_i = a_i - q_i b_i$$
$$= (c_i X + d_i Y) - q_i (e_i X + f$$
$$= X\underbrace{(c_i - q_i e_i)}_{e_{i+1}} + Y\underbrace{(d_i - q_i f_i}_{f_{i+1}}$$

Initial values
$$\begin{cases} C[0] = 1 \\ d[0] = 0 \\ e[0] = 0 \\ f[0] = 1 \end{cases}$$