Week 1 (Friday)

Euclidean Algorithm

inputs: $a, b \in \mathbb{Z}$

output: $\gcd(a,b)$

Recursive

p. 288

1. Let $c = a \bmod b$
2. If $c = 0$, then gcd is b
3. Otherwise, then answer is $\gcd(b, c)$

Uses the following thm:

Let $a = bq + r$

(a, b, q, r obtained using Div. Alg.)

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

$\gcd(360, 84)$

① $24 = 360 \bmod 84$

② $12 = 84 \bmod 24$

$0 = 24 \bmod \underline{12}$

$\therefore \gcd(360, 84) = 12$

gcd(a,b) as a linear combination of a,b:

gcd(a,b) = d can be written as

$$d = ax + by \qquad x,y \in \mathbb{Z}$$

Continuing ex. from prev. page, we want:

$$\boxed{12 = 360x + 84y}$$

① $360 = 84(4) + 24 \Rightarrow 24 = 360 + 84(-4)$

② $84 = 24(3) + 12 \Rightarrow 12 = 84 + 24(-3)$

② $12 = 84 + [360 + 84(-4)](-3)$

$= 84 + 360(-3) + 84(12)$

$= 84(13) + 360(-3)$

$x = -3,\ y = 13$

Ex. $\gcd(1205, 37)$

(1) $1205 = 37(32) + 21 \rightarrow 21 = 1205 + 37(-32)$

(2) $37 = 21(1) + 16 \rightarrow 16 = 37 + 21(-1)$

(3) $21 = 16(1) + 5 \rightarrow 5 = 21 + 16(-1)$

(4) $16 = 5(3) + 1 \rightarrow 1 = 16 + 5(-3)$

(5) $5 = 1(5) + 0$

$\gcd(1205, 37) = 1$

1205 and 37 are <u>relatively prime</u>

Find x, y s.t. $1 = 1205x + 37y$?

$$1 = 16 + 5(-3)$$

$$= [37 + 21(-1)] + [21 + 16(-1)](-3)$$

$$= 37 + [1205 + 37(-32)](-4) + 16(3)$$

$$= 37 + 1205(-4) + 37(128) + 16(3)$$

$$= 37(129) + 1205(-4) + [37 + 21(-1)](3)$$

$$= 37(129) + 1205(-4) + 37(3) + [1205 + 37(-32)](-3)$$

$$= 37(228) + 1205(-7)$$

Doing two substitutions in the same step as I did in class unnecessarily overcomplicates the subsequent steps. Instead, take it slow and one step at a time like on the next page.

Let's try this again more carefully and only one substitution at a time:

$$
\begin{aligned}
1 &= 16 + 5(-3) \\
&= 16 + [21 + 16(-1)](-3)
\end{aligned}
$$

Better idea to start by substituting 5 (not 16), since we see from eqn. 3 on prev. page that the expression contains 16, which we can then collect with the 16 term that is already here.

Similarly, we will substitute 16 first (not 21) because we see from eqn 2 on prev. page that the expression for 16 contains 21, which we can then collect with the 21 term that is already here.

$$
\begin{aligned}
&= 16(4) + 21(-3) \\
&= [37 + 21(-1)](4) + 21(-3) \\
&= 37(4) + 21(-7) \\
&= 37(4) + [1205 + 37(-32)](-7) \\
&= 37(228) + 1205(-7)
\end{aligned}
$$

So, $y = 228$ and $x = -7$