Algebra in-class exams on weeks 7 and 11 on Thursdays.

Examples of Euclid's alg.

<u>Ex:</u> $\gcd(\overset{b}{144}, \overset{a}{360})$

$$360 = 2 \cdot 144 + 72$$

$$144 = 2 \cdot 72 + 0$$

So our seq. of remainders is $b = 144 > \underline{72} > 0$.

Thus, $\gcd(144, 360) = 72$.

<u>Ex:</u> $\gcd(242, 1870) = 22$.

$$1870 = 7(242) + 176$$

$$242 = 1(176) + 66$$

$$176 = 2(66) + 44$$

$$66 = 1 \cdot \underline{44} + \boxed{22}$$

$$44 = 2 \cdot 22 + 0$$

Linear equations with integer solutions.

A linear Diophantine equation has the form (in 2 vars):

$$\boxed{ax + by = c}$$

where $a, b, c \in \mathbb{Z}$ and one seeks $x, y \in \mathbb{Z}$ that satisfy

The existence of a solution is controlled by $\gcd(a,b)$

Theorem (Bezout's theorem). Let $a, b \in \mathbb{N}$. There exist $x, y \in \mathbb{Z}$ such that
$$ax + by = \gcd(a,b).$$

Corollary: The equation $\boxed{ax+by=c}$ has a solution if and only if
$$\gcd(a,b) \mid c.$$

Suppose we found $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a,b).$$

Take $\tilde{x} = \frac{c \cdot x}{\gcd(a,b)}$, $\tilde{y} = \frac{c \cdot y}{\gcd(a,b)}$: (assuming $\gcd(a,b) \mid c$)

new var. looks like x

integers

$$a\tilde{x} + b\tilde{y} = \frac{c}{\gcd(a,b)} ax + \frac{c}{\gcd(a,b)} by$$

$$= \frac{c}{\gcd(a,b)} (ax + by)$$

$$= c.$$

So $\tilde{x}, \tilde{y} \in \mathbb{Z}$ ~~are~~ is a solution to the Diophantine eq.

Use Euclid's alg. to solve for (x,y)

$$ax + by = \gcd(a,b).$$

From ex: $\gcd(242, 1870) = 22$:

$$1870 = 7\,(242) + 176$$
$$242 = 1(176) + 66$$
$$176 = 2\cdot(66) + 44$$
$$66 = 1(44) + 22$$

Use "back-substitution" to get (x,y) for above

$$22 = 66 - 1\cdot(44)$$
$$= 66 - 1\cdot(176 - 2\cdot(66))$$
$$= 3\cdot 66 - 1\cdot 176$$

$\boxed{22 = 3\cdot 66 - 1\cdot 176}$

If $a=66$, $b=176$

$$= 3\cdot(242 - 1\cdot(176)) - 1\cdot 176$$
$$= 3\cdot 242 - 4\cdot 176$$
$$= 3\cdot 242 - 4\cdot(1870 - 7\cdot(242)) = \boxed{31}\cdot 242 \boxed{-4}\cdot 1870$$

17