Worksheet:

$$S = \{ 6m + 10n : m, n \in \mathbb{Z} \}$$

found that $S = \{$ multiples of $2 \}$

and $2 = \gcd(6, 10)$

Q: if $6m + 10n = 0$, what can you say?

$3m + 5n = 0$

$3m = -5n$

$\hookrightarrow 3 \mid n$ write $n = 3l$

$3m = -15l$

$m = -5l$

then $n = 3l$ and $m = -5l$

for some $l \in \mathbb{Z}$

Euclidean Algorithm

Theorem: Let $a, b \in \mathbb{Z}$, not both zero

Let $S = \{ ma + nb : m, n \in \mathbb{Z} \}$

Then there is a pos. int. d

such that $S = \{ kd : k \in \mathbb{Z} \}$

moreover, $d \mid a$, $d \mid b$

and if $e \mid a$ and $e \mid b$ then $e \mid d$.
for any int. e.

take as this def of gcd

Proof: Let d be the smallest positive element of S.

Write $d = m_0 a + n_0 b$.

(1) every multiple of d is in S.

Why? $kd = km_0 a + kn_0 b \in S$

(2) d divides a. Why? If not, do long division.

$a = qd + r$ where $0 < r < d$

then r is a $\mathbb{Z}$-linear combo of a and b:

$$r = a - qd$$
$$= a - qm_0 a - qn_0 b$$
$$= (1 - qm_0)a + (-qn_0)b$$

so $r \in S$. but this contradicts our choice of d as the smallest pos. elt. of S.

(3) similarly, $d \mid b$.

(4) thus every element of S is a mult of d.

$ma + nb$ if $a = kd$ and $b = ld$
then $ma + nb = mkd + nld = (mk + nl)d$.

(5) if $e \mid a$ and $e \mid b$ then $e \mid d$.

bec. $d = m_0 a + n_0 b$ .. same idea as here

This proof suggests an algorithm for finding $\gcd(a, b)$:

Euclidean algorithm.

much faster than "factor them both."

Example: $d = \gcd(87, 717)$

is the smallest pos. elt. of

$S = \{ 87m + 717n : m, n \in \mathbb{Z} \}$

divide any two elts of S

$\Rightarrow$ remainder is a smaller elt of S.

$$\begin{array}{r} 8 \\ 87 \overline{)\,717} \\ \underline{696} \\ 21 \end{array}$$

So $21 = 8 \cdot 87 - 717 \in S$

$$\begin{array}{r} 4 \\ 21 \overline{)\,87} \\ \underline{84} \\ 3 \end{array}$$

So $3 \in S$ too.

$$\begin{array}{r} 7 \\ 3 \overline{)\,21} \end{array}$$

now $3 \mid 21$ no remainder.

So $\gcd = 3$.