Math 4460

3/13/23

$\boxed{\text{HW 2}}$

(12) Let $a, b \in \mathbb{Z}$, not both zero.
Suppose there exist $x, y \in \mathbb{Z}$
with $ax + by = 1$.

Prove: $\gcd(a,b) = 1$

proof: Let $d = \gcd(a,b)$.
We know $ax+by=1$ for some $x, y \in \mathbb{Z}$.
Since $d = \gcd(a,b)$ we know $d \mid a$ and $d \mid b$.
So, $a = dk$, $b = d\ell$ where $k, \ell \in \mathbb{Z}$.
Thus, $1 = ax + by = dkx + d\ell y = d[kx + \ell y]$.
So, $d \mid 1$.
Thus, $d = \pm 1$.
Since $d = \gcd(a,b)$ we know $d > 0$, so $d = 1$.
$\blacksquare$

$\boxed{\text{HW 2 \#8}}$

Let $a,b \in \mathbb{Z}$ where $\gcd(a,4)=2$ and $\gcd(b,4)=2$.

$\boxed{4=2^2}$

Prove, $\gcd(a+b,4)=4$.

<u>proof:</u>

Since $\gcd(a,4)=2$ we know $2|a$ but $4 \nmid a$.
Since $\gcd(b,4)=2$ we know $2|b$ but $4 \nmid b$.

Since $2|a$ we know $a=2k$ where $k \in \mathbb{Z}$.
We must have that k is odd, for otherwise if k was even and $k=2s$, then $a=2k=2(2s)=4s$ and $4|a$ which isn't the case.

Thus, $a=2k$ where k is odd.

Similarly, since $2|b$ and $4 \nmid b$, we know $b=2l$ where l is odd.

Since k and l are odd we know
$k=2n+1$ and $l=2m+1$
where $n,m \in \mathbb{Z}$.

Thus,

$$\begin{aligned} a+b = 2k+2l &= 2(k+l) \\ &= 2(2n+1+2m+1) \\ &= 2(2n+2m+2) \\ &= 4(n+m+1). \end{aligned}$$

So, $4 \mid (a+b)$.

Thus, $\gcd(a+b, 4) = 4$. $\blacksquare$

$\boxed{\text{HW 1 7}}$

Let $n > 1$ where $n \in \mathbb{Z}$.

(a) n is composite iff there exist $a, b \in \mathbb{Z}$ where $n = ab$ and $1 < a < n$, $1 < b < n$

did in class

(b) n is composite iff there exist $a, b \in \mathbb{Z}$ where $n = ab$ and $1 < a$, $1 < b$.

<u>proof of (b):</u>

($\Rightarrow$) Suppose n is composite. Then from (a) we know $n = ab$ where $a, b \in \mathbb{Z}$ and $1 < a < n$, $1 < b < n$.

Thus, $n = ab$ where $1 < a$ and $1 < b$.

($\Leftarrow$) Suppose $n = ab$ where $a, b \in \mathbb{Z}$ and $1 < a$ and $1 < b$.
We must show that n is composite.

Since $1 < b$ and $1 < a$ we

Know $a(1) < \underbrace{ab}_{n}$.

Thus, $a < n$

Thus a is a positive divisor of n and $a \neq 1$ and $a \neq n$ (because $1 < a < n$).
So, n is composite (ie not prime). $\blacksquare$

HW 2

④ (f) Find <u>all</u> the solutions, if there are any, to

$$39x + 17y = 22$$

Euclidean algorithm time.

$$39 = 2 \cdot 17 + 5$$
$$17 = 3 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$\gcd(39, 17) = 1$

Since $1 \mid 22$ there exist integer solutions to $39x + 17y = 22$

Let's find an integer solution.

Solve equations for remainders.

$$5 = 1\cdot\boxed{39} - 2\cdot\boxed{17}$$
$$2 = 1\cdot\boxed{17} - 3\cdot\boxed{5}$$
$$1 = 1\cdot\boxed{5} - 2\cdot\boxed{2}$$

Thus,

$$\begin{aligned}
1 &= 1\cdot\boxed{5} - 2\cdot\boxed{2} \\
&= 1\cdot\left(1\cdot\boxed{39} - 2\cdot\boxed{17}\right) - 2\cdot\left(1\cdot\boxed{17} - 3\cdot\boxed{5}\right) \\
&= 1\cdot\boxed{39} - 2\cdot\boxed{17} - 2\cdot\boxed{17} + 6\cdot\boxed{5} \\
&= 1\cdot\boxed{39} - 4\cdot\boxed{17} + 6\cdot\boxed{5} \\
&= 1\cdot\boxed{39} - 4\cdot\boxed{17} + 6\cdot\left(1\cdot\boxed{39} - 2\cdot\boxed{17}\right) \\
&= 7\cdot\boxed{39} - 16\cdot\boxed{17}
\end{aligned}$$

$\boxed{\underline{\text{Check:}}\ 7\cdot 39 - 16\cdot 17 = 273 - 272 = 1}$ ✓

Thus,

$$\boxed{39(7) + 17(-16) = 1}$$

multiply by 22 to get

$$\boxed{39(154) + 17(-352) = 22}$$

Particular solution to

$$39x + 17y = 22$$

is $x_0 = 154$, $y_0 = -352$

All solutions:

$$\boxed{\begin{array}{c} ax + by = c \\ 39x + 17y = c \end{array}}$$

$$x = x_0 - t\frac{b}{d} = 154 - t\frac{17}{1} = 154 - 17t$$

$$y = y_0 + t\frac{a}{d} = -352 + t\frac{39}{1} = -352 + 39t$$

Some solutions:

$t=1$: $x = 154 - 17 = 137$
$y = -352 + 39 = -313$

$t=0$: $x = 154 - 0 = 154$
$y = -352 + 0 = -352$

Hw 2

⑦ Let $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$.
Let $d = \gcd(a, b)$.
Prove: $a | b$ iff $d = a$

($\Leftarrow$) Suppose $d = a$.

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

Since $d = a$ and $d | b$ we know $a | b$.

($\Rightarrow$) Let $d = \gcd(a, b)$, $a > 0$, $b > 0$.

Suppose $a | b$.

Thus, $a | a$ and $a | b$, so a is

a positive common divisor of a and b.

Thus, since $d = \gcd(a,b)$ we know $\boxed{a \leq d}$.

But also, $d > 0$, $a > 0$ and $d \mid a$, thus by a theorem in class we know $\boxed{d \leq a}$.

Since $a \leq d$ and $d \leq a$ we know $a = d$. $\blacksquare$

($\Rightarrow$) Method 2

Suppose m is a positive common

divisor of a and b.

Since $a > 0$, $b > 0$ and
$m \mid a$ and $m \mid b$,
we know $m \leq a$ and $m \leq b$.

Since $a \mid b$ we know $a \leq b$.

Thus, $m \leq a \leq b$.

And since $a \mid a$ and $a \mid b$
we know a is a positive
common divisor of a and b.

Thus, a is the greatest
common divisor of a & b.

Ie $a = \gcd(a, b)$. $\blacksquare$