TOPIC 2 -

Greatest common divisor

Greatest Common Divisor (HW 2)

Def: Let $a_1, a_2, \ldots, a_n$ be n integers.

If x is a non-zero integer that divides each of $a_1, a_2, \ldots, a_n$ then x is called a common divisor of $a_1, a_2, \ldots, a_n$

Ex: Find the common divisors of 12 and 18.

divisors of 12	$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$
divisors of 18	$\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$
common divisors of 12 and 18	$\pm 1, \pm 2, \pm 3, \pm 6$

Ex: Let's find the common divisors of 12, 27, and 0.

divisors of 12	$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$
divisors of 27	$\pm 1, \pm 3, \pm 9, \pm 27$
divisors of 0	$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots$
common divisors of 12, 27, 0	$\pm 1, \pm 3$

$2 \mid 0$ because $(2)\overbrace{(0)}^{k} = 0$

$-10 \mid 0$ because $(-10)\underbrace{(0)}_{k} = 0$

Def: Let $a_1, a_2, \ldots, a_n$ be integers, not all zero. The largest positive common divisor of $a_1, a_2, \ldots, a_n$ is called the greatest common divisor of $a_1, a_2, \ldots, a_n$ and we denote this integer by $\gcd(a_1, a_2, \ldots, a_n)$

Note: The gcd of $a_1, a_2, \ldots, a_n$ exists if the integers are not all zero. This is because at least one of the a_i is not zero and so there is an upper bound on the positive common divisors of $a_1, a_2, \ldots, a_n$, namely $|a_i|$

Ex: $\gcd(12, 18) = 6$

positive divisors of 12	1, 2, 3, 4, 6, 12
positive divisors of 18	1, 2, 3, 6, 9, 18
common positive divisors	1, 2, 3, 6 ← gcd

Ex: $\gcd(12, 27, 9) = 3$

positive divisors of 12	1, 2, 3, 4, 6, 12
positive divisors of 27	1, 3, 9, 27
positive divisors of 9	1, 3, 9
common positive divisors	1, 3 ← gcd

Ex: $\gcd(0,5) = 5$

positive divisors of 5	1, 5
positive divisors of 0	1, 2, 3, 4, 5, 6, ...
common positive divisors	1, 5 ← gcd

Fact: If $a > 0$, $a \in \mathbb{Z}$, then
$$\gcd(a, 0) = a$$

Ex: What is $\gcd(0,0)$?

Not defined. There is no positive greatest common divisor when all the numbers are zero.

positive divisors of 0	1, 2, 3, 4, 5, ...
positive divisors of 0	1, 2, 3, 4, 5, ...
common positive divisors	1, 2, 3, 4, 5, ...

no largest common divisor

Theorem (The division algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Then there exist unique integers q and r where

$$a = qb + r$$

and $0 \leq r < b$.

We are dividing b into a with quotient q and remainder r

$\boxed{\text{Ex:}}$ $b = 12$
$a = 24$

$$\begin{array}{r} 2 \leftarrow \boxed{q} \\ 12\overline{)24} \\ -24 \\ \hline 0 \leftarrow \boxed{r} \end{array}$$

$$24 = 2(12) + 0$$

$$\boxed{a = qb + r}$$

$$0 \leq r < 12$$

Ex: $b = 5$

$a = 123$

$$\begin{array}{r} 24 \\ 5\,\overline{)\,123} \\ -10 \\ \hline 23 \\ -20 \\ \hline 3 \end{array}$$

$\boxed{q}$ $\boxed{r}$

$$123 = (24)(5) + 3$$
$$a = q\,b + r$$
$$0 \leq r < 5$$

Ex: $b = 50$

$a = -120$

Easier (from chat):

$$\begin{array}{r} -3 \\ 50\,\overline{)\,-120} \\ -(-150) \\ \hline 30 \end{array}$$

$-120 =$
$(-3)(50) + 30$

$$\begin{array}{r} -2 \\ 50\,\overline{)\,-120} \\ -(-100) \\ \hline -20 \end{array}$$

negative! can't be r

need to make positive

The division gives: $-120 = \underbrace{(-2)(50)}_{\text{take a 50 from here and put it}} - 20$

Get:

$$\begin{array}{l} -120 = (-3)(50) + 30 \\ \;\;\;a \;\;=\;\; q \;\;\; b \;\;+\; r \end{array} \Bigg\}\; 0 \leq r < 50$$

Proof of the division algorithm:

Let a and b be integers with $b>0$.
Consider the set

$$T = \{ a - xb \mid x \in \mathbb{Z} \text{ and } a - xb \geq 0 \}$$

Claim: T is not empty.

pf of claim:

case 1: Suppose $a=0$

Then setting $x=-1$ into $a-xb$ gives

$$a - xb = 0 - (-1)b = b > 0$$

So, $b>0$ and $b \in T$.

case 2: Suppose $a \neq 0$

If $a>0$, then set $x=0$ to get

$$a = a - 0b \in T.$$

If $a<0$, then set $x=2a$ to get that

$$a - (2a)b = \underbrace{a}_{<0}\underbrace{(1-2b)}_{\substack{b \geq 1 \\ -2b \leq -2 \\ 1-2b \leq -1 < 0}} > 0$$

So, $a-(2a)b \in T$

$\boxed{\text{Claim}}$

L9

Since $T \neq \emptyset$ and every element of T is non-negative, T must have a smallest element.

Let r be the smallest element of T [that is $r \in T$ and $r \leq t$ for all $t \in T$].

Since $r \in T$, there exists $q \in \mathbb{Z}$ with $r = a - qb$.

[q is the x variable]

$$\boxed{\text{Thus, } a = qb + r}$$

Let's show $0 \leq r < b$.

We know $0 \leq r$ because $r \in T$.

Let's show $r < b$.

What if $r \geq b$?

If so, then

$$r - b = (a - qb) - b = a - (q+1)b$$

which is in T because $a-(q+1)b$ is of the form $a - xb$ and we know $r - b \geq 0$ if $r \geq b$.

But, $r - b < r$ since $b > 0$.

This would then contradict r being the smallest element of T.

Therefore, $r < b$.

Now for the uniqueness of r and q.

Suppose that $a = qb + r$ and $a = q'b + r'$ where $0 \leq r < b$ and $0 \leq r' < b$.

Without loss of generality assume $r' \leq r$

[This means a similar proof works if $r \leq r'$]

Subtract $a = qb + r$ and $a = q'b + r'$ to get

$$0 = (q - q')b + (r - r')$$

So,

$$r - r' = (q' - q)b$$

Then, b divides $r - r'$.

Recall that $0 \leq r' \leq r < b$.

So, $0 \leq r - r' < b - r' < b$

So, $0 \le r - r' < b$

But $r-r'$ is a multiple of b because b divides $r-r'$.
There are no positive multiples of b that are less than b.
The only way this can happen is if $r-r'=0$.

So, $\boxed{r=r'}$.

Replace $r-r'=0$ into
$$0 = (q-q')b + (r-r')$$
to get $0 = (q-q')b$.
Since $b>0$ this implies $q-q'=0$. Thus, $\boxed{q=q'}$

So we get uniqueness. ◺

Theorem: Let a and b be integers, not both equal to zero. There exist integers x_0 and y_0 where $\gcd(a,b) = ax_0 + by_0$

Ex: $a = 42$ $b = 72$

positive divisors of 42	1, 2, 3, 6, 7, 14, 21, 42
positive divisors of 72	1, 2, 3, 4, 6, 8, 9, 12, 18, 36, 72
common positive divisors	1, 2, 3, 6

$$\gcd(42, 72) = 6$$

$$6 = 42 \cdot (-5) + 72 \cdot (3)$$

$$\underset{\gcd}{} = 42x_0 + 72y_0$$

$$\boxed{\begin{array}{c} 6 = 42x + 72y \\ \text{we solved for } x, y \end{array}}$$

proof of theorem:

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

Let

$$S = \{ ax + by \mid x, y \in \mathbb{Z} \}$$

$$= \{ 10a - b,\ a \cdot 1 + b \cdot 0,\ a \cdot 0 + b \cdot 1,\ 100a + 0b, \ldots \}$$

infinitely many more

Note that $a, -a, b, -b$ are all in S because $a = a \cdot 1 + b \cdot 0$, $-a = a(-1) + b \cdot 0$, $b = a \cdot 0 + b \cdot 1$, and $-b = a \cdot 0 + b(-1)$.

Since a and b are not both zero and $a, -a, b, -b \in S$, we know S contains at least one positive integer.

Let d be the smallest positive integer in S.

Since d is in S, we can write
$$d = ax_0 + by_0 \quad \text{for some } x_0, y_0 \in \mathbb{Z}.$$

We will now show that $d = \gcd(a,b)$. Then we will be done with the proof.

First let's show that d is a common divisor of a and b.

Let's start, by showing d divides a.

By the division algorithm we can write $a = dq + r$ where $0 \leq r < d$.

We want to show that $r = 0$.

Notice that

$$\left.\begin{aligned} r &= a - dq \\ &= a - (ax_0 + by_0)q \\ &= a(1 - x_0 q) + b(-y_0 q) \end{aligned}\right\} \begin{array}{l} r = \\ ax+by \\ \text{for some} \\ x,y \in \mathbb{Z} \end{array}$$

Thus, $r \in S$.

But $0 \leq r < d$ and d is the smallest positive integer in S.

Therefore, $r = 0$.

Thus, $a = dq + r = dq + 0 = dq$.

So, $d \mid a$.

A similar argument will show that $d \mid b$.] Try for practice

Therefore, d is a common divisor of a and b.

We now show that d is the greatest common divisor of a & b.

Suppose d' is another positive common divisor of a and b.

We will show $d' \leq d$.

Since d' is a common divisor of a and b, we know
$d'k = a$ and $d'l = b$
for some $k, l \in \mathbb{Z}$.

Thus,

$$d = ax_0 + by_0 = (d'k)x_0 + (d'l)y_0$$
$$= d'[kx_0 + ly_0]$$

So, $d' \mid d$.

Since d' and d are both positive and $d' \mid d$, we know $d' \leq d$.

Therefore $d = \gcd(a, b)$. ▨

We are going to learn a new way to calculate $\gcd(a,b)$. It's called the Euclidean algorithm.

Here's the main idea behind the Euclidean algorithm.

<u>Theorem:</u> Let a and b be positive integers and $0 < a \leq b$. Suppose $b = aq + r$ where $q, r \in \mathbb{Z}$ with $0 \leq r < a$.

Then,

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

We replace $\boxed{\text{this problem}}$ with a $\boxed{\text{smaller problem}}$

$(0 \leq r < a \leq b)$

Proof: Suppose $a, b \in \mathbb{Z}$ with $0 < a \leq b$.

Suppose $b = aq + r$ with $q, r \in \mathbb{Z}$ with $0 \leq r < a$.

Let $d = \gcd(b, a)$ and $d' = \gcd(a, r)$.

Our goal is to show $d = d'$.

Since $d' = \gcd(a, r)$ we know $d' \mid a$ and $d' \mid r$.

So, $d' k_1 = a$ and $d' k_2 = r$ where $k_1, k_2 \in \mathbb{Z}$.

Then,

$$\begin{aligned} b &= aq + r \\ &= (d'k_1)q + d'k_2 \\ &= d'[k_1q + k_2]. \end{aligned}$$

So, $d' \mid b$.

Thus, d' is a positive common divisor of both a and b.

Since d is the greatest common divisor of a and b, we have $\boxed{d' \leq d}$.

Now let's show $d \leq d'$.

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

Thus, $b = d\ell_1$ and $a = d\ell_2$
where $\ell_1, \ell_2 \in \mathbb{Z}$.

So,

$$
\begin{aligned}
r &= b - qa \\
&= d\ell_1 - q(d\ell_2) \\
&= d[\ell_1 - q\ell_2].
\end{aligned}
$$

So, $d \mid r$.

Since $d \mid r$ and $d \mid a$, we know
d is a positive common divisor
of a and r.

Since $d' = \gcd(a,r)$ we know $\boxed{d \le d'.}$

Therefore, since $d' \le d$ and $d \le d'$
we have $d = d'$. $\blacksquare$

Ex: Find $\gcd(138, 61)$

$$138 = 2\cdot 61 + 16$$

$$\begin{array}{r} 2 \\ 61\overline{)138} \\ -122 \\ \hline 16 \end{array}$$

So,
$\gcd(138,61) = \gcd(61,16)$

Repeat idea:

$$61 = 3\cdot 16 + 13$$

$$\begin{array}{r} 3 \\ 16\overline{)61} \\ -48 \\ \hline 13 \end{array}$$

So,
$\gcd(61,16) = \gcd(16,13)$

Repeat idea:

$$16 = 1\cdot 13 + 3$$

$$\begin{array}{r} 1 \\ 13\overline{)16} \\ -13 \\ \hline 3 \end{array}$$

So,
$\gcd(16,13) =$
$\gcd(13,3)$

$$13 = 4 \cdot 3 + 1$$

$$\begin{array}{r} 4 \\ 3 \overline{)13} \\ -12 \\ \hline 1 \end{array}$$

$\gcd(13,3)$
$= \gcd(3,1)$

$$3 = 3 \cdot 1 + 0$$

$$\begin{array}{r} 3 \\ 1 \overline{)3} \\ -3 \\ \hline 0 \end{array}$$

So,
$\gcd(3,1)$
$= \gcd(1,0)$

So,

$$\gcd(138,61) = \gcd(61,16) = \gcd(16,13)$$
$$= \gcd(13,3) = \gcd(3,1)$$
$$= \gcd(1,0) = 1$$

Euclidean Algorithm

Finds $\gcd(a,b)$

Let a and b be positive integers, with $a \leq b$.

Step 1: Divide a into b to get

$$b = aq + r$$

with $0 \leq r < a$.

Step 2:
If $r = 0$, then you're done. The gcd will be a.
If $r \neq 0$, you repeat step 1 but with b replaced by a and a replaced by r.

Ex: Find gcd(578, 153)

From 2/8 Thm

$$578 = 3\cdot 153 + 119$$
$$153 = 1\cdot 119 + 34$$
$$119 = 3\cdot 34 + 17$$
$$34 = 2\cdot \underbrace{17}_{\text{answer}} + \underset{\text{done}}{0}$$

$$\begin{aligned} &\gcd(578,153) \\ &= \gcd(153,119) \\ &= \gcd(119,34) \\ &= \gcd(34,17) \\ &= \gcd(17,0) \\ &= 17 \end{aligned}$$

$$\boxed{\text{So, } \gcd(578,153) = 17}$$

Calculations

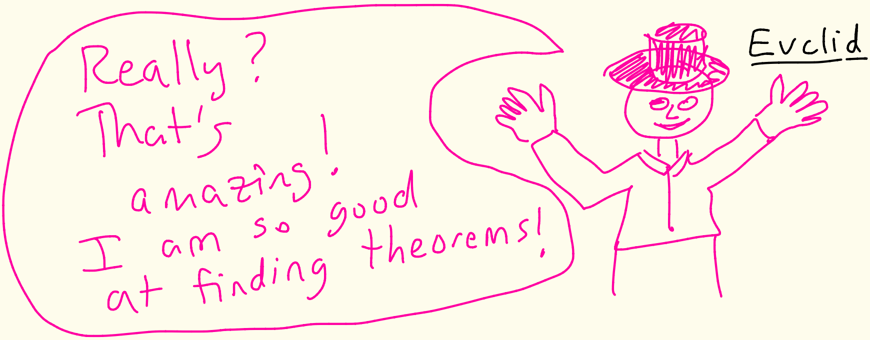
$$\begin{array}{r} 3 \leftarrow \boxed{q} \\ 153\,\overline{)\,578} \\ -459 \\ \hline 119 \leftarrow \boxed{r} \end{array}
\qquad
\begin{array}{r} 1 \leftarrow \boxed{q} \\ 119\,\overline{)\,153} \\ -119 \\ \hline 34 \leftarrow \boxed{r} \end{array}
\qquad
\begin{array}{r} 2 \\ 17\,\overline{)\,34} \\ -34 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 3 \leftarrow \boxed{q} \\ 34\,\overline{)\,119} \\ -102 \\ \hline 17 \leftarrow \boxed{r} \end{array}$$

The Euclidean algorithm can also be used to solve the equation

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

for x and y.



Ex: Recall $\gcd(578, 153) = 17$.

Solve $578x + 153y = 17$

Step 1: Do the Euclidean algorithm.

$$\boxed{\begin{aligned} 578 &= 3 \cdot 153 + 119 \\ 153 &= 1 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}}$$

Step 2: Disregard the last equation with $r = 0$ in it. Rewrite the other equations so that the remainder is on the left-hand side.

$$\boxed{\begin{aligned} 119 &= 578 - 3 \cdot 153 \\ 34 &= 153 - 1 \cdot 119 \\ 17 &= 119 - 3 \cdot 34 \end{aligned}}$$

Step 3: Now start at the bottom equation and back-subsitute in using the equations above it until you are left with an expression of the form $ax+by = 578x+153y$

Previous page

$$\boxed{119} = 578 - 3\cdot 153$$
$$\boxed{34} = 153 - 119$$
$$17 = 119 - 3\cdot 34$$

$$
\begin{aligned}
17 &= \boxed{119} - 3\cdot\boxed{34} \\
&= (578 - 3\cdot 153) - 3\cdot(153 - 119) \\
&= \boxed{578} - 6\cdot\boxed{153} + 3\cdot\boxed{119} \\
&= 578 - 6\cdot 153 + 3\cdot(578 - 3\cdot 153) \\
&= 578 - 6\cdot 153 + 3\cdot 578 - 9\cdot 153 \\
&= 4\cdot\boxed{578} - 15\cdot\boxed{153}
\end{aligned}
$$

Answer: $578(4) + 153(-15) = 17$

$x = 4$ and $y = -15$ is a solution to $578x + 153y = 17$

Ex: $a = 60$
$b = 350$

$$a = 60 = 2^2 \cdot 3 \cdot 5$$
$$b = 350 = 2 \cdot 5^2 \cdot 7$$

$$\gcd(a,b) = \gcd(60,350) = 2 \cdot 5 = 10$$

$$\gcd\left(\frac{a}{10}, \frac{b}{10}\right) = \gcd\left(\frac{2^2 \cdot 3 \cdot 5}{2 \cdot 5}, \frac{2 \cdot 5^2 \cdot 7}{2 \cdot 5}\right)$$
$$= \gcd(2 \cdot 3, 5 \cdot 7) = 1$$

So, $d = \gcd(a,b)$

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Idea: If you remove all the common factors of a & b the result has gcd 1

Theorem: Let $a_1, a_2, \ldots, a_n$ be integers, not all equal to zero. Let $d = \gcd(a_1, a_2, \ldots, a_n)$. Then $\gcd\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1$

Special case when $n=2$: Let $a, b \in \mathbb{Z}$, not both equal to zero. Let $d = \gcd(a,b)$. Then, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

proof:

We will prove the special case when $n=2$. You can generalize this proof if you want practice. I'll put the general case proof online with the notes.

proof: Let $a, b \in \mathbb{Z}$, not both equal to zero.

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

Then $d \mid a$ and $d \mid b$, since d is a common divisor of a and b.

So, $a = dx$ and $b = dy$ for some $x, y \in \mathbb{Z}$.

Let $d' = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \gcd(x, y)$.

Our goal is to show $d' = 1$.

Since $d' = \gcd(x, y)$, we know $d' \mid x$ and $d' \mid y$.

So, $x = d'r$ and $y = d's$ where $r, s \in \mathbb{Z}$.

Thus,

$$a = dx = dd'r$$
$$b = dy = dd's$$

So, $dd' \mid a$ and $dd' \mid b$.

Also, since d and d' are both gcd's we know $d \geq 1$ and $d' \geq 1$.

Thus, $dd' \geq 1$.

Therefore, dd' is a positive common divisor of a and b.

Since d is the greatest common divisor of a and b we know that $dd' \leq d$.

Dividing by d gives $d' \leq 1$.

Since $d' \geq 1$ and $d' \leq 1$ we have $d' = 1$. Thus, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = d' = 1$. $\blacksquare$

~~Ex: Let $a=60$ and $b=350$.~~
~~Then $\gcd(a,b)=\gcd(60,350)=10$.~~
~~Note that $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=\gcd(6,35)=1$.~~
~~This always happens!~~

Here's a more general version of the lemma

<u>Lemma:</u> Let $a_1, a_2, \ldots, a_n$ be integers, not all zero. Let $d=\gcd(a_1,a_2,\ldots,a_n)$. Then $\gcd\left(\frac{a_1}{d},\frac{a_2}{d},\ldots,\frac{a_n}{d}\right)=1$.

In particular, for two integers $a,b\in\mathbb{Z}$ not both zero with $d=\gcd(a,b)$, then $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$.

<u>proof:</u> Since $d=\gcd(a_1,a_2,\ldots,a_n)$ we have that $d \mid a_i$ for each i. Hence there exist integers $k_i\in\mathbb{Z}$ with $dk_i=a_i$ for $i=1,2,\ldots,n$.

Let $d'=\gcd\left(\frac{a_1}{d},\frac{a_2}{d},\ldots,\frac{a_n}{d}\right)$.

Then $d' \mid \frac{a_i}{d}$ for all i, so there exist $l_i\in\mathbb{Z}$ with $d'l_i=\frac{a_i}{d}$ for $i=1,2,\ldots,n$.

Thus, $a_i=(dd')l_i$ for $i=1,2,\ldots,n$.

So, dd' is a positive common divisor of the a_i.

Hence $dd'\le d$ (since d is the greatest positive common divisor of the a_i).

Thus, $d'\le 1$ (by dividing by d).

Since d' is positive, $d'=1$. ∎

Theorem: Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$. Suppose also that $\gcd(c, a) = 1$. If $c \mid ab$, then $c \mid b$.

Ex: $c = 3$, $3 \mid 30$,

$\underset{c}{3} \mid \underset{a}{5} \cdot \underset{b}{6}$ and $\underset{c}{3} \mid \underset{b}{6}$

$\gcd(3,5) = 1$

proof:

Suppose $\gcd(c, a) = 1$ and $c \mid ab$.

Since $\gcd(c, a) = 1$ we know that

$$c x_0 + a y_0 = 1$$

for some $x_0, y_0 \in \mathbb{Z}$.

Since $c \mid ab$ we know $ab = ck$
for some integer k.

Multiply $cx_0 + ay_0 = 1$ by b to get

$$cbx_0 + aby_0 = b.$$

Substituting $ab = ck$ into the above gives

$$cbx_0 + cky_0 = b.$$

Thus, $c\left[bx_0 + ky_0\right] = b.$

Since $bx_0 + ky_0 \in \mathbb{Z}$, we see
that $c \mid b$. $\blacksquare$

Corollary: Let $a, b, p \in \mathbb{Z}$ where p is prime.
If $p \mid ab$, then $p \mid a$ or $p \mid b$.

you could have both $p \mid a$ and $p \mid b$ since in math "A or B" is only false when both A and B are false

proof:

Suppose $p \mid ab$.

Since p is prime the only divisors of p are 1 and p.

Thus, either

$\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

If $\gcd(p, a) = 1$, then by the previous theorem $p \mid b$.

If $\gcd(p, a) = p$, then p is a common divisor of a & p and so $p \mid a$. $\blacksquare$

One area of number theory is the study of <u>Diophantine equations</u>. These are polynomials in one or more variables whose coefficients are integers.

<u>Examples of Diophantine equations:</u>

$578x + 153y = 17$ ← linear eqn

$x^2 + y^2 = z^2$ ← Pythagorean formula

$5 = x^2 + y^2$ ← prime = sum of squares

$x^2 - ny^2 = 1$ ← Pell-Fermat equation

where $n > 1$ and square-free

(see HW for what square-free means)

We won't solve this one, but you can solve it with continued fractions

$$x^n + y^n = z^n, \quad n \geq 3$$

$$x^3 + y^3 = z^3$$

$$x^4 + y^4 = z^4$$

$$\vdots \qquad \vdots$$

We will show Fermat's proof for $n=3$

Fermat claimed to have a proof that these equations have no trivial solutions with $x, y, z \in \mathbb{Z}$

[where trivial means one of the variables is 0, like $3^3 + 0^3 = 3^3$]

This is called "Fermat's Last Theorem" and wasn't proved till 1995 by Andrew Wiles. There is a Nova PBS movie about this called "The proof"

Suppose we have the equation

$$ax + by = c$$

where a, b, and c are integers.

Q1: Does $ax+by=c$ have integer solutions? For example, $578x+153y=17$ has the integer solution $(x,y)=(4,-15)$ that we found in the last class. If you tried to solve $578x+153y=1$ you wouldn't be able to find integer solutions. [$x=\frac{2}{578}$, $y=-\frac{1}{153}$ is a solution but those numbers aren't integers.]

Q2: If $ax+by=c$ has integer solutions, how many are there? Finitely many or infinitely many? Is there an equation or formulas that describes the solutions?

Theorem: Let a, b, c be integers with a and b not both equal to zero. Let $d = \gcd(a,b)$.

has integer solutions means $\exists x, y \in \mathbb{Z}$ with $ax+by=c$

① $ax+by=c$ has integer solutions if and only if $d \mid c$.

② If $ax+by=c$ has integer solutions and (x_0, y_0) is an integer solution [that is, $ax_0+by_0=c$] then the formula

$$x = x_0 - t\left(\frac{b}{d}\right)$$
$$y = y_0 + t\left(\frac{a}{d}\right)$$

proof is later after a few examples

gives all the integer solutions where t ranges over all integers.

③ So either $ax+by=c$ has no integer solutions or infinitely many.

Ex: Consider

$$21x + 33y = 5 \leftarrow \boxed{ax+by=c}$$

Does the equation have integer solutions?

Let $d = \gcd(21, 33) = 3$.

Since $3 \nmid 5$, there are no integer solutions to $21x + 33y = 5$.

Note: There are rational solutions, such as:

$$21\left(\frac{5}{21}\right) + 33(0) = 5$$

Ex: Consider

$$578x + 153y = 17 \leftarrow \boxed{ax+by=c}$$

Here $d = \gcd(578, 153) = 17$.

And $17 \mid 17$. $\leftarrow \boxed{d \mid c}$

So there are integer solutions.

We found one last time, it was $(x_0, y_0) = (4, -15)$

So, all integer solutions are of the form:

$$x = x_0 - t\left(\frac{b}{d}\right) = 4 - t\left(\frac{153}{17}\right) = 4 - 9t$$

$$y = y_0 + t\left(\frac{a}{d}\right) = -15 + t\left(\frac{578}{17}\right) = -15 + 34t$$

Where t can be any integer.

Some example integer solutions to $578x + 153y = 17$

t	$x = 4 - 9t$	$y = -15 + 34t$
0	4	−15
1	−5	19
−1	13	−49
2	−14	53
−2	22	−83
⋮	⋮	⋮

proof of theorem:

Let $a, b, c \in \mathbb{Z}$ with a, b not both zero.

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

① ($\Rightarrow$) Suppose $ax + by = c$ has integer solutions.

We want to show $d \mid c$.

We are given that there exists $x_0, y_0 \in \mathbb{Z}$ with $ax_0 + by_0 = c$.

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

By HW 1 #6, $d \mid (ax_0 + by_0)$.

So, $d \mid c$.

① ($\Leftarrow$) Suppose $d \mid c$.

So, $c = dk$ where $k \in \mathbb{Z}$.

Since $d = \gcd(a,b)$ we know there exist $x_0, y_0 \in \mathbb{Z}$ where $ax_0 + by_0 = d$.

Thm from class

FOR HW 2

Note: This proof tells you how to find the solution. First solve $ax+by=d$ via the Euclidean alg. then multiply by k to solve $ax+by=c$

Multiplying by k we get

$$ax_0k + by_0k = dk$$

which becomes

$$a(x_0k) + b(y_0k) = c$$

So, $x = x_0k$, $y = y_0k$ is an integer solution to

$$ax + by = c.$$

$\boxed{①}$

(2) We now deal with the problem of constructing all the integer solutions to $ax+by=c$ when $d \mid c$ where $d = \gcd(a,b)$

We saw in part (1) that since $d \mid c$, there exist $x_0, y_0 \in \mathbb{Z}$ where $ax_0 + by_0 = c$.

Let $t \in \mathbb{Z}$ and set

$$x = x_0 - t\left(\frac{b}{d}\right)$$

$$y = y_0 + t\left(\frac{a}{d}\right)$$

Let's check that this is indeed a solution to $ax+by=c$ by plugging it in.

Plugging in we get

$$ax+by = a\left(x_0 - t\left(\frac{b}{d}\right)\right) + b\left(y_0 + t\left(\frac{a}{d}\right)\right)$$

$$= \underbrace{ax_0 + by_0}_{c} \underbrace{- t\frac{ab}{d} + t\frac{ab}{d}}_{\text{cancel}}$$

$$= c$$

Hence, $x = x_0 - t\left(\frac{b}{d}\right)$, $y = y_0 + t\left(\frac{a}{d}\right)$ is a solution to $ax+by=c$ for every t.

The question remains: Is every solution of $ax+by=c$ in the above form?

Let $x_0, y_0 \in \mathbb{Z}$ satisfy

$$\boxed{ax_0 + by_0 = c}$$

Suppose that $x, y \in \mathbb{Z}$ is another solution, that is $\boxed{ax + by = c}$

Subtracting the two above equations gives

$$a(x - x_0) + b(y - y_0) = 0$$

So,

$$\frac{a}{d}(x - x_0) = \frac{-b}{d}(y - y_0)$$

Multiplying by -1 gives

$$\boxed{\frac{a}{d}(x_0 - x) = \frac{b}{d}(y - y_0)} \quad (*)$$

(*) tells us that $\frac{a}{d} \mid \frac{b}{d} \cdot (y - y_0)$

We know $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ and

so since $\frac{a}{d} \mid \frac{b}{d} \cdot (y - y_0)$

this implies $\frac{a}{d} \mid (y - y_0)$.

Therefore, $y - y_0 = t\left(\frac{a}{d}\right)$ for some $t \in \mathbb{Z}$.

So, $\boxed{y = y_0 + t\left(\frac{a}{d}\right)}$.

Plug this back into (*) to get

$$\frac{a}{d}(x_0 - x) = \frac{b}{d}\Big(\underbrace{y_0 + t\left(\tfrac{a}{d}\right) - y_0}_{y - y_0}\Big)$$

So, $\frac{a}{d}(x_0 - x) = \frac{b}{d} \cdot \left(\frac{a}{d} t\right)$

Thus, $x_0 - x = \frac{b}{d} t$

So, $\boxed{x = x_0 - \frac{b}{d} t.}$

Thus, every solution to $ax+by=c$ is of the form

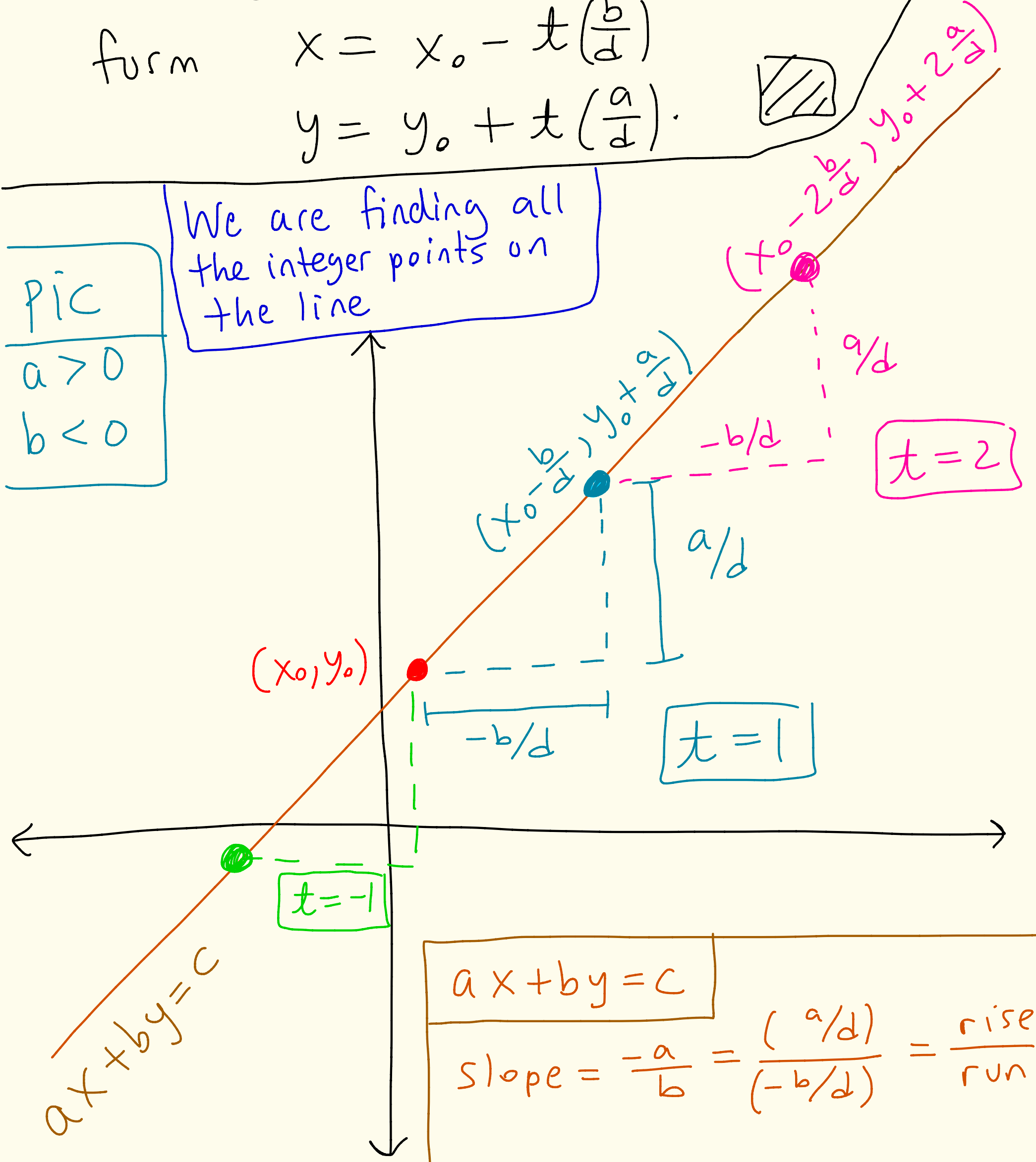
$$x = x_0 - t\left(\frac{b}{d}\right)$$
$$y = y_0 + t\left(\frac{a}{d}\right).$$

pic

$a>0$

$b<0$

We are finding all the integer points on the line



$ax+by=c$

$$\text{slope} = \frac{-a}{b} = \frac{(a/d)}{(-b/d)} = \frac{\text{rise}}{\text{run}}$$