Math 4460

2/3/25

Topic 2 - GCD

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	$\pm 1, \pm 2, \pm 3, \pm 6$

Ex: 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	$\pm 1, \pm 2, \pm 3, \pm 4, \ldots$
common divisors	$\pm 1, \pm 3$

Every non-zero integer divides 0.

For example, Why does $3 \mid 0$?

Because $0 = (3)(0)$

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 is written $\gcd(a_1, a_2, \ldots, a_n)$

Ex: Find $\gcd(12, 18)$

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

So, $\gcd(12,18)=6$

Ex: Calculate $\gcd(12,27,9)$

positive divisors of 12	1, 2, 3, 4, 6, 12
p.d. of 27	1, 3, 9, 27
p.d. of 9	1, 3, 9
common positive divisors	1, 3

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

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

positive divisors of 0	1, 2, 3, 4, 5, 6, 7, 8, ...
positive divisors of 5	1, 5
common positive divisors	1, 5

So, $\gcd(0,5) = 5$

Facts: If $a > 0$, then

$$\gcd(a,0) = a$$

If $a < 0$, then

$$\gcd(a,0) = |a|$$

Ex: What about gcd(0,0)?

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

There is no largest common positive divisor

gcd(0,0) is undefined

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

Proof: On Weds ▨

Ex: $a = 33$

$b = 11$

$$11 \overline{)\,33} \quad 3 \leftarrow q$$

$$-33$$

$$0 \leftarrow r$$

$$33 = (3)(11) + 0$$

$$a = qb + r$$

Ex: $a = 213$
$b = 7$

$$\begin{array}{r} 30 \leftarrow q \\ 7\overline{)213} \\ -21 \\ \hline 03 \\ -\ 0 \\ \hline 3 \leftarrow r \end{array}$$

$213 = (30)(7) + 3$

$a = qb + r$

$0 \leq 3 < 7$

$0 \leq r < b$

Ex: $a = -120$
$b = 50$

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

$-120 = (-2)(50) + (-20)$

$a = qb + r$

$0 \leq r < b$

but r doesn't satisfy $0 \leq r < 50$

You need to "over divide"

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

q ← −3

r ← 30

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

$$a = qb + r$$

Now: $0 \leq r < b$

$0 \leq 30 < 50$

Theorem: Let a and b be integers, not both zero.

Then there exist integers x_0 and y_0 where

$$\gcd(a,b) = ax_0 + by_0$$

---

proof: On Weds. 

Ex: $a = 2$, $b = 3$

$\gcd(a,b) = \gcd(2,3) = 1$

Thm says we can find $x_0, y_0 \in \mathbb{Z}$ where

$$\underbrace{1}_{\gcd(2,3)} = 2x_0 + 3y_0$$

Can use $x_0 = -1, y_0 = 1$.

Get:

$$1 = 2(-1) + 3(1)$$

Ex: $a = 42, b = 72$

p.d. of 42	1, 2, 3, 6, 7, 14, 21, 42
p.d. of 72	1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72
c.p.d.	1, 2, 3, 6

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

Theorem says there exist x_0, y_0 where

$$\underbrace{6}_{\gcd(42,72)} = 42x_0 + 72y_0$$

Set $x_0 = -5$, $y_0 = 3$ it works:

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

Another sol. is $x_0 = 7$, $y_0 = -4$

$$6 = 42(7) + 72(-4)$$

We will learn later how to find formulas for x_0, y_0.