Math 4460
2/1/23

TOPIC 2 - Greatest common divisor

<u>Def:</u> 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 <u>common divisor</u> of $a_1, a_2, \ldots, a_n$.

<u>Ex:</u> Find all 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: Find all the common divisors of 12, 27, and 0.

divisors of 12	±1, ±2, ±3, ±4, ±6, ±12
divisors of 27	±1, ±3, ±9, ±27
divisors of 0	±1, ±2, ±3, ±4, ±5, ...
common divisors of 12, 27, 0	±1, ±3

$5 \mid 0$ because $0 = (5)\overbrace{(0)}^{k}$

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

0 has an infinite # of divisors

<u>Def:</u> 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 <u>greatest common divisor of $a_1, a_2, \ldots, a_n$</u> and we denote this integer by $\gcd(a_1, a_2, \ldots, a_n)$

<u>Note:</u> 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 them, say 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: 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 ← gcd

$$\boxed{\gcd(12,18)=6}$$

Ex: Find gcd(12, 27, 9)

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

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

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 ← gcd

$\gcd(0,5) = 5$

Fact: If $a > 0$, $a \in \mathbb{Z}$

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

If $a < 0$, $a \in \mathbb{Z}$, 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 positive common divisor.

So, 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 $0 \leq r < b$.

dividing b into a q times with remainder r

$\boxed{\text{Ex:}}$ $b = 7$

$a = 21$

$$\begin{array}{rl} 3 & \leftarrow \boxed{q} \\ 7\overline{)21} & \\ -21 & \\ \hline 0 & \leftarrow \boxed{r} \end{array}$$

$$21 = (3)(7) + 0$$

$$a = q\,b + r$$

$$0 \leq r < b$$

$$0 \leq 0 < 7 \checkmark$$

__Ex:__ $b = 7$

$a = 213$

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

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

$$a = qb + r$$

$$\boxed{\begin{array}{c} 0 \le r < b \\ 0 \le 3 < 7 \ \checkmark \end{array}}$$

__Ex:__ $b = 50, \ a = -120$

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

$$0 \le r < b$$

$$\cancel{0 \le -20 < 50} \ \times$$

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

This doesn't work

You have to "over divide"

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

$-3 \leftarrow q$

$30 \leftarrow r$

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

$a = qb + r$

$0 \le r < b$

$0 \le 30 < 50$ ✓

Answer: $q = -3$, $r = 30$

Next Monday we will prove the division algorithm

Theorem: Let a and b be integers, not both equal to zero. Then there exist integers x_0 and y_0 where

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

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

pos. div. of 42	1, 2, 3, 6, 7, 14, 21, 42
pos. div. of 72	1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72
pos. common div.	1, 2, 3, 6

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

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

$$\gcd(42,72) = 42x_0 + 72y_0$$

We will learn how to find x_0, y_0 at a later time.

Need the Euclidean alg.

Next Mon. we will prove the above theorem.