Day 15 - Topics in Number Theory #2:
GCD, Euclid's Lemma

Vocabulary

- linear combination - gcd - prime	- Euclid's Lemma

Definitions

- Definition. Given two integers a,b, a **linear combination** of a and b is an expression of the form ax+by, for some integers x,y.
- **Proposition NT1.2**: Suppose a,b,c are integers. If c|a and c|b and $ax + by$ is a linear combination of a and b, then c divides $ax + by$.
- Definition. A natural number n is **prime** if it has exactly two distinct positive divisors, 1 and n.
- Definition. If a and b are integers and are not both zero, then the **greatest common divisor** or gcd of a and b is the largest integer d such that $d|a$ and $d|b$. It is written $d = gcd(a, b)$.
- HINT: To prove that a number x is the gcd of a and b, show two things:
    1. x is a common divisor of a and b (that is, $x|a$ and $x|b$)
    2. x is the greatest common divisor (if $y|a$ and $y|b$, then $x \geq y$)

Example 1. a) gcd(15,20) b) gcd(9,27) c) gcd(15,28) d) gcd(-6,21)

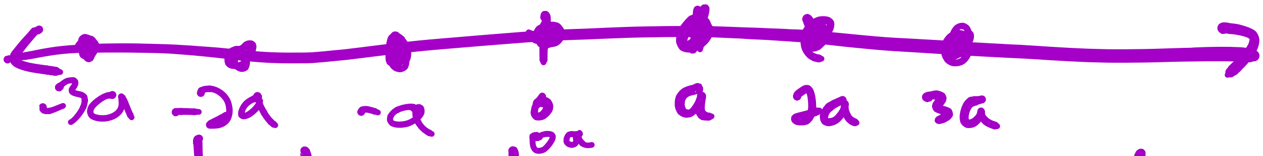
"The gcd of two numbers can be written as a linear combination."

Proposition NT 2.1: Suppose $a, b \in \mathbb{Z}$ are not both zero. Then there exist $x, y \in \mathbb{Z}$ such that $gcd(a, b) = ax + by$.

Proposition NT 2.2: (Euclid's Lemma) Let p be prime and a,b integers with $p|ab$. Then $p|a$ or $p|b$.

Linear Combinations, GCD, and Euclid's Lemma

$a \in \mathbb{Z}$

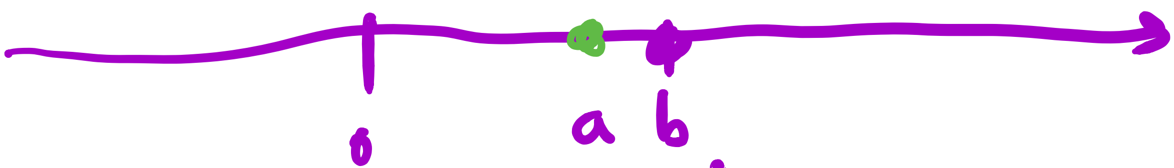


what numbers can you reach by moving distance $\underline{a}$ repeatedly

Multiples of a.

$\{x \in \mathbb{Z} : x = ay \text{ for some } y \in \mathbb{Z}\}$

$a, b \in \mathbb{Z}$



what can we reach by moving distance a or b? (can repeat, can go either direction)

<u>Ex</u> $a = 3, \quad b = 6$

(Desmos)

<u>Defn</u> if $a, b \in \mathbb{Z}$, not both 0, then a <u>linear combination</u> of a and b is a number

of the form $\underline{a \cdot x + by}$, for some $x, y \in \mathbb{Z}$.

$a=4, \quad b=6$

is 0 a linear combo of a, b?

$2b - 3a = 2 \cdot 6 - 3 \cdot 4 = 12 - 12 = 0$

$x=2, \quad y=-3$

$4 \cdot 0 + 6 \cdot 0$ – is it a linear combo

$a \; x + b \; y$

Are the linear combos just multiples of the difference a-b?

$a=4, \quad b=10$

is 24 a linear combo? $2b + a$

is 6 a linear combo? $b-a$

$b - a = 10 - 4 = 6.$

Q: is every linear combo of 4, 10 a multiple of 6?

$b + 2a = 10 + 2\cdot 4 = 18$ ✓

$4\cdot 0 + 10\cdot 1 = 10$ not a multiple of 6!

$4 + 10 = 14$ "

All even numbers!

Is it because 2 is a common factor?

$2 \mid a$ and $2 \mid b$

Theorem if $a, b, f \in \mathbb{Z}$, and $f \mid a$ and $f \mid b$, then $f \mid ax+by$ for any linear combination of a and b.

Proof (Direct) Spoze $a, b, f \in \mathbb{Z}$ and $f \mid a$ and $f \mid b$.

then $a = fm$ and $b = fn$ for some $m, n \in \mathbb{Z}$

by defn of divides.

Suppose $ax+by$ is a linear combo of a and b, $x,y \in \mathbb{Z}$,

then $ax+by = fmx + fny$ (substitution)

$ax+by = f(mx+ny)$

Note $mx+ny \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under addition and mult.

so $f \mid ax+by$ by defn of divides $\square$

ex: $a=4$, $b=12$

any linear combo of 4, 12 will be divisible by

-2

-4

2

4

$4x+12y$ ______

Is it possible 24 is a linear combo of 4, 12?

Is 6 a linear comb of

4, 12?
NO

$2 \cdot 12 - 4 \cdot 5 =$

$24 - 20 = 4.$

test 104 – is it divisible by $-2, -4, 2, 4$?

Just check if div. by 4

4, 12

divisors: $-2, -4, 2, 4$

$104 = 12 \cdot 10 - 4 \cdot 4$ ✓

from $a = 4$, $b = 12$ get 4

"linear combos" = "multiples of 4"

from $a = 4$, $b = 6$

"linear combos" = multiples of 2

from $a = 30$, $b = 45$

"linear combos of 30, 45" = multiples of 15

15 is the <u>greatest</u> common divisor of 30, 45

<u>Theorem</u>: Suppose $a, b \in \mathbb{Z}$, not both zero. then $\gcd(a,b) = ax + by$ for some $x, y \in \mathbb{Z}$

"the gcd is a linear combination"

$$\boxed{\text{\underline{Defn} a natural number } p \text{ is \underline{prime} if it has exactly 2 positive divisors (1 and } p)}$$

Theorem Euclid's Lemma Let p be

prime and $a, b \in \mathbb{Z}$ such that $p \mid ab$ then $p \mid a$ or $p \mid b$. $\square$

$4 \mid 12$

2 6

3 4

$3 \mid 12$

2 6

3 4

1 12