Next theorem says: if we divide out by gcd we're left w/ #'s w/ no common factors

Theorem Fix $m, n \in \mathbb{Z}$ (not both 0) and let $d = \gcd(m,n)$

Then: $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$

Pf: - Let $a = \gcd\left(\frac{m}{d}, \frac{n}{d}\right)$ WTS: $a = 1$

- So $a \geq 1$ and $a \mid \frac{m}{d}$ and $a \mid \frac{n}{d}$

- i.e. $\exists k, \ell \in \mathbb{Z}$ s.t. $\frac{m}{d} = ak$ $\frac{n}{d} = a\ell$

$\Rightarrow m = (ad)k$ $n = (ad)\ell$

$\Rightarrow ad$ is a common divisor of m, n.

since d is greatest common divisor of m, n must be: $ad \leq d$.

$\Rightarrow a \leq 1 \Rightarrow a = 1$. ✓

---

ex: $\gcd\left(\frac{42}{6}, \frac{60}{6}\right) = \gcd(7, 10)$

$= 1$, as expected from theorem.

Q: is there a better way of finding $\gcd(m,n)$ than writing out all divisors of m,n?

A: Yes! The Euclidean Algorithm (will cover later)

First: Theorem (Division Algorithm)

- Fix $b \in \mathbb{Z}$ and $a \in \mathbb{N}$
- then: there exist unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < a$ s.t.

$$b = aq + r$$

(q is the quotient of b when divided by a, r is the remainder)

---

before proving: ex illustrating proof:

if $b = 14$ $a = 3$

Consider:

$3 \cdot 1 = 3$ $\quad$ $14 - 3 \cdot 1 = 11 > 3$

$3 \cdot 2 = 6$ $\quad$ $14 - 3 \cdot 2 = 8 > 3$

$3 \cdot 3 = 9$ $\quad$ $14 - 3 \cdot 3 = 5 > 3$

$3 \cdot 4 = 12$ $\quad$ $14 - 3 \cdot 4 = 2 < 3$

$$14 = 3 \cdot 4 + 2$$

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

Pf: Define $S = \{n \in \mathbb{N} \cup \{0\} \mid (\exists k \in \mathbb{Z})(n = b - ak)\}$ (196)

(e.g. if $b = 14$ $a = 3$ then $S = \{2, 5, 8, 11, \ldots\}$)

Observe: - $S \neq \emptyset$ since $b - ak \geq 0$ whenever $b \geq ak$ (and k can be negative)

- but $S \subseteq \mathbb{N} \cup \{0\}$, hence by WOP, S has a least elt r.

- Let $q \in \mathbb{Z}$ be the integer s.t.

$$b - aq = r$$

$$\Rightarrow b = aq + r$$

Claim: $r < a$

Pf: - if not, $r \geq a$

- so: $r = a + r_1$ with $r_1 \geq 0$ and $r_1 < r$

- but then: $b = aq + r = aq + a + r_1$

$$= a(q+1) + r_1$$

- so: $r_1 \in S$.

↳ contradiction as r is least in S. ✓

- so: we've proved existence of r, q s.t. $b = aq + r$ and $r < a$.

- need to prove uniqueness of r, q.

- So suppose $q', r' \in \mathbb{Z}$ with $0 \leq r' < a$ and $b = aq' + r'$

WTS: $q = q'$ and $r = r'$

will: either $r \geq r'$ or $r' \geq r$. Let's assume $r \geq r'$ - other case similar.

then: $r - r' = aq' - aq$

$= a(q' - q)$ (nonnegative)

$\Rightarrow a \mid r - r'$. But $0 \leq r - r' < a$.

Only way this is possible is if $r - r' = 0$

i.e. $r = r'$

But then: $b = aq + r = aq' + r$

$\Rightarrow aq = aq' \Rightarrow q = q'$ ✓

Ex's ① if $b = 107$, $a = 15$

then $107 = 15 \cdot 7 + 2$ $(q = 7, r = 2)$

② if $b = -29$, $a = 6$

then $-29 = 6(-5) + 1$ $(q = -5, r = 1)$

③ if $b = 12$, $a = 3$

then $b = 3 \cdot 4 + 0$ $(q = 4, r = 0)$

Next theorem is the fundamental result about divisibility.

Bezout's Theorem: Fix $a, b \in \mathbb{Z}$ (not both 0) and let $d = \gcd(a,b)$

then $\exists m, n \in \mathbb{Z}$ s.t. $d = am + bn$ — "d can be written as a linear combination of a, b"

note: m, n not unique

Furthermore: d is the least natural number that can be so written.

Example before proof: Consider $a = 27$, $b = 21$

Q: If we add/subtract 21's and 27's in any combination: how small a positive # can we get?

e.g. $27 - 21 = 6$ (i.e. $21(-1) + 27(1) = 6$)

better yet: $21(4) + 27(-3) = 3$

Can we do better than 3? Doesn't seem so, but we can get 3 in more than one way: e.g. $21(-5) + 27(4) = 3$.

Notice: $\gcd(21, 27) = 3$. Bezout says: this is no accident.