Lecture 16: GCD and Bézout coefficients

inductive proof gives $\forall n \in \mathbb{N}, P(n)$

- **Defn:** $a \mid b$ means there exists k such that $ka = b$
- **Defn:** $g(a, 0) := a$, and $g(a, b) := g(b, r)$ where $r = rem(a, b)$ (so $a = qb + r$)

Claim: For all $a \in \mathbb{N}, b \in \mathbb{N}$, $g(a, b) \mid a$ and $g(a, b) \mid b$

Proof: By induction on b. Let $P(b)$ be "for all $a \in \mathbb{N}$, $g(a, b) \mid a$ and $g(a, b) \mid b$"

To see $P(0)$, choose an arbitrary a; we have $g(a, 0) = a$. Clearly $a \mid a$ (since $1 \cdot a = a$) and $a \mid 0$ (since $0 \cdot a = 0$).

Now we will show $P(b)$ for an arbitrary $b > 0$, assuming $P(b')$ for all $b' < b$. ($P(b-1), P(b-2), \ldots, P(0)$)
Choose an arbitrary a. We want to show that $g(a, b) \mid a$ and $g(a, b) \mid b$.

A. I'm making progress
B. I have a next step
C. I have a question
D. I'm lost
E. I'm done

know	WTS
$\forall b' < b,\ P(b')$	$g(a,b) \mid a$ ~~and $g(a,b) \mid b$~~
$g(a,b) = g(b,r)$	$g(b,r) \mid a$ and $g(b,r) \mid b$.
$a = qb + r$	
$r = a - qb$	
$g(b,r) \mid b$, $g(b,r) \mid r$	

Well, $g(a,b) = g(b,r)$ by def^n, so WTS $g(b,r) \mid a$, $g(b,r) \mid b$.

by $P(r)$, we have $\forall a', g(a', r) \mid a'$ and $g(a', r) \mid r$

so $g(b,r) \mid b$ and $g(b,r) \mid r$.

So $g(a,b) = g(b,r) \mid b$. ✓

all that's left: $g(b,r) \mid a$. ← $t \cdot g(a,b) = a$ for some t.

we know $g(b,r) \mid b$, so $k \cdot g(b,r) = b$ for some k

$g(b,r) \mid r$, so $l \cdot g(b,r) = r$ for some l

$$a = qb + r = qkg(b,r) + lg(b,r)$$
$$= (qk + l)\, g(b,r).$$

So a is a multiple of $g(b,r)$ ✓

So $g(b,r) \mid a$ so $g(a,b) \mid a$

GCD is the greatest common divisor

- **Defn:** $a \mid b$ means there exists k such that $ka = b$
- **Defn:** $g(a, 0) := a$, and $g(a, b) := g(b, r)$ where $r = rem(a, b)$ (so $a = qb + r$)

Claim : For all $a, b, c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$ then $c \leq g(a, b)$

Claim': For all $a, b, c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$ then $c \mid g(a, b)$

Proof: By induction on b. Let $P(b)$ be the statement "$\forall a, \forall c$, if $c \mid a$ and $c \mid b$ then $c \mid g(a, b)$"

(skip P(0))

WTS P(b), assuming P(b') for all b'<b (strong ind.)

WTS if c|a and c|b then c|g(a,b).

Assume c|a and c|b, WTS: c|g(a,b).

so a=kc and b=lc for some l,k.

Know g(a,b) = g(b,r). So done if c|g(b,r).

by P(r), if c|b and c|r then c|g(b,r)

so we'd be done.

we know c|b by assumption,

so done if we can show c|r.

want to write r = t·c for some t.

a=qb+r so r=a-qb

=kc - qlc = (k-ql)c.

So c|r, so by P(r), c|g(b,r) = g(a,b)

Bézout coefficients; inductive proofs as algorithms

Defn: integers s and t are called "Bézout coefficients" of a and b if $g(a,b) = sa + tb$.

Claim: For all a and b, there exist s and t with $g(a,b) = sa + tb$.

Proof: By induction on b. Let $P(b)$ be the statement "$\forall a, \exists s, t$ such that $g(a,b) = sa + tb$."

To see $P(0)$, choose an arbitrary a. Let $s =$ 1 and $t =$ 0 (or anything). Then

$g(a,0) = a =$ $1 \cdot a + 0 \cdot 0$ $= s \cdot a + t \cdot 0$ ✓

Now we will show $P(b)$ for an arbitrary $b > 0$, assuming $P(b')$ for all $b' < b$. Choose an arbitrary a. We want to find s, t with $g(a,b) = sa + tb$. We have

$g(a,b) = g(b,r)$ where $a = qb + r$

$= s'b + t'r$ for some s', t', by $P(r)$.

$= s'b + t'(a - qb)$

$= (s' - t'q)b + t'a$

$= sa + tb$ ✓

since $a = qb + r$, $r = a - qb$

let $s = t'$ and $t = s' - t'q$.