Today:
- Existence proofs
- Proving equivalent statements
- Disproof

} proofs topics

"Math" topics:
- congruences
- inequalities
- limits. "$(u_n \to \infty)$"

} review.

Existence (7.3 in the book)

Classical proof:

Theorem Let $a, b \in \mathbb{Z}$ Let $d = \gcd(a, b)$.
Then $\exists\ x, y \in \mathbb{Z}$ such that $d = ax + by$.

Understanding what the theorem says:

$\gcd(a,b)$ = greatest common divisor of a, b
= the largest ~~int~~ positive integer that divides both a and b

Example: $\gcd(60, 24) = 12$

check: $12 \mid 60$
$12 \mid 24$, so it is a common divisor.

Does there exist a number greater than 12 that divides both 60 and 24?

No: how to check? - go through 13, 14, 15, ..., 24 and check they do not work.

better: the positive divisors of 24 are:

$\{d \in \mathbb{N} \mid d \mid 24\} = \{1, 2, 3, 4, 6, 8, 12, 24\}$

not a divisor of 60.

What does the theorem say for this example:

$a = 60 \qquad b = 24 \quad , \; d = \gcd(60, 24) = 12$

Theorem says: $\exists\, x, y \in \mathbb{Z}$:

$$60 \cdot x + 24 \cdot y = 12$$

/ the gcd(a,b) can be represented as a combination of a, b with integer coefficients /

Here $x = 1$, $y = -2$: $\boxed{60 - 24 \cdot 2 = 12}$

Proof of the Theorem

Let $A = \{ n \in \mathbb{Z} : n = ax + by \text{ with } x, y \in \mathbb{Z} \}$

– the set of all linear combinations of a and b with integer coefficients.

Want to prove: $\gcd(a,b) \in A$.

We are going to look for gcd(a,b) among the elements of A:

Let d_0 be the smallest positive element of A.

/ looks obvious that ~~a~~ such a smallest positive element should exist. In fact it is an axiom of natural numbers – see next class /

We will prove that $d_0 = \gcd(a,b)$.

We need to show that d_0 satisfies the definition of gcd(a,b).

This means, prove two things: 1) that $d_0 | a$ and $d_0 | b$

2) It is the largest ~~positive~~ common divisor

Proving (1): We know: $d_0 \in A$
so exist $x_0, y_0 \in \mathbb{Z}$ s.t.
$d_0 = ax_0 + by_0$, and d_0 is the smallest positive integer of this kind.

~~..~~ Let us divide a by d_0 with remainder:

$a = d_0 q + r$ for some $q \in \mathbb{Z}$ and $0 \le r < d_0$.

Want to prove: $r = 0$

We have: $r = a - d_0 q = a - (\underbrace{ax_0 + by_0}_{d_0}) q$

$= a(\underbrace{1 - x_0 q}_{\in \mathbb{Z}}) + b(\underbrace{-y_0 q}_{\in \mathbb{Z}})$ – again an element of A.

Now we got: $r \in A$, and if $r \neq 0$, then $r > 0$.
but we also know: $r < d_0$. (because it's a remainder!)

Since we know d_0 is the smallest positive element of A, we must have $r = 0$.

WLOG, d_0 also divides b.

[without loss of generality.

Proving (2): d_0 is the greatest ~~common~~ common divisor.

We will prove:

$(d|a \wedge d|b) \Rightarrow d | d_0$.

(every common divisor of a and b divides d_0)
(this would mean that d_0 is the greatest of them).

Proving $d|a$ and $d|b \Rightarrow d|d_0$:

let $d|a$ and $d|b$.

Then: exists $k \in \mathbb{Z}$ s.t. $a = dk$ and $\exists n \in \mathbb{Z}: b = dn$

We also have: $d_0 = ax_0 + by_0$.

Then we have: $d_0 = dkx_0 + dny_0 = d(\underbrace{kx_0 + ny_0}_{\in \mathbb{Z}})$

So $d|d_0$.

This completes the proof. ∎

Why is this proof so complicated when many other existence proofs just require an example?

Consider two statements:

1) $\exists\, x, y \in \mathbb{Z}$ s.t. $60x + 24y = 12$

2) Let $a, b \in \mathbb{Z}$, $d = \gcd(a,b)$. Then $\exists\, x, y \in \mathbb{Z}$ s.t. $ax + by = d$ ← our theorem.

In (1), example proves it: take $x = 1$, $y = -2$ and we are done!

The theorem is about all a, b:

$\forall\, a, b \in \mathbb{Z}$ if $d = \gcd(a,b)$, then $\exists\, x, y \in \mathbb{Z}: d = ax + by$.

Now we need to prove it for all a, b.

Aside: The logic of the argument:

Suppose I want to prove that there exists a person named John who knows how to prove theorems.

Strategy: Let $A = \{$ people who know how to prove theorems $\}$

$= \{$ famous mathematicians, students who took math 220, ... $\}$

In this set, look for someone named John.

We did: make a set A of numbers that have the property we want to prove about $\gcd(a,b)$.

Look for gcd in this set.

imagine in my set of people who know proofs there's one wearing a name tag: "John".

Then I am lucky!

Here: we know from mathematical experience that the smallest positive element of A is a likely candidate.

Proving equivalent statements.

"The following are equivalent": (TFAE)

Example 1 Prove that TFAE:

1) $3^n \equiv 2 \mod 5$
2) $n \equiv 3 \mod 4$
3) $n = 4k+3$ for some $k \in \{0,1,2,3,\dots\}$.

Example 2 TFAE:

1) $a \geq 2$
2) $\exists\, x > 0 : x^2 - ax + 1 = 0$
3) $((1+a)(a-2) \geq 0) \wedge (a > 0)$ ← note the correction!

About TFAE: it says: $(1) \Leftrightarrow (2) \Leftrightarrow (3)$
(also $(1) \Leftrightarrow 3$).

Strategy: choose some order and only prove $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$
$1 \Rightarrow 2 \Rightarrow 3$ - cycle.

We will prove some of these for both examples:

Example 1: will prove: $(1) \Rightarrow (2)$ and $(3) \Rightarrow (1)$.
Homework: $(2) \Rightarrow (3)$.

Pf: to start with, look at the first few powers of 3:

back to this line.

$3^1 = 3 \equiv 3 \mod 5$

$3^2 = 9 \equiv 4 \equiv -1 \mod 5$ (recall congruences!)

do not have to compute! → $3^3 \equiv 3 \cdot (-1) \equiv -3 \mod 5$
$\equiv 2 \mod 5$

$\boxed{3^4 \equiv 3 \cdot 2 = 1 \mod 5}$

$3^5 \equiv 3 \cdot 1 \mod 5$

From this, we see that:

$$3^5 \equiv 3^1 \mod 5.$$

And then $3^6 \equiv 3^2 \mod 5$, ...

~~Then~~ Want to prove: (1) $\Rightarrow$ (2)

if $3^n \equiv 2 \mod 5$, then $n \equiv 3 \mod 4$

We proved: $3^4 = 81 \equiv 1 \mod 5$.

Then $3^{4k} \equiv 1^k = 1 \mod 5$

Then if $n = 4k+3$, then

$$3^n = 3^{4k+3} \equiv 1 \cdot 3^3 \equiv 2 \mod 5.$$

We proved: (3) $\Rightarrow$ (1)

So: we were trying to prove (1) $\Rightarrow$ (2) but instead so far proved (3) $\Rightarrow$ (1).

back to (1) $\Rightarrow$ (2): know: $3^n \equiv 2 \mod 5$

Want to prove: $n \equiv 3 \mod 4$.

Proof by cases: cases are:

$n \equiv 1 \mod 4$

$n \equiv 0 \mod 4$

$n \equiv 2 \mod 4$

$n \equiv 3 \mod 4$

want to eliminate these.

if $n \equiv 0 \mod 4$, then $n = 4k$

Then $3^n = 3^{4k} = (3^4)^k \equiv 1^k \equiv 1$ ← NOT 2.

$n \equiv 1 \mod 4$, then $n = 4k+1$

... ← finish it at home!

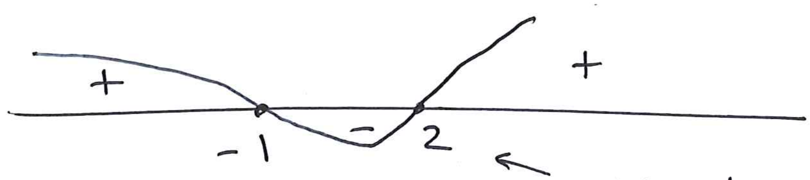
Example 2 Analysis: understanding (2) and (3):

(2) says: $x^2 - ax + 1$ has a positive root.

which means: $a^2 - 4 \geq 0$

and $\dfrac{a \pm \sqrt{a^2-4}}{2}$ has to be positive for at least one choice of + or −

(3) says: $(1+a)(a-2) \geq 0$



points where factors = 0.

$(1+a)(a-2) \geq 0 \iff \left[\begin{array}{l} a \leq -1 \\ a \geq 2 \end{array}\right. \iff (a \leq -1) \vee (a \geq 2).$

or

So (3) says:

$((1+a)(a-2) \geq 0) \wedge (a > 0)$

$\iff$ ~~means~~: $(a \leq -1) \vee (a \geq 2) \wedge (a > 0)$

$\iff \boxed{a \geq 2}$