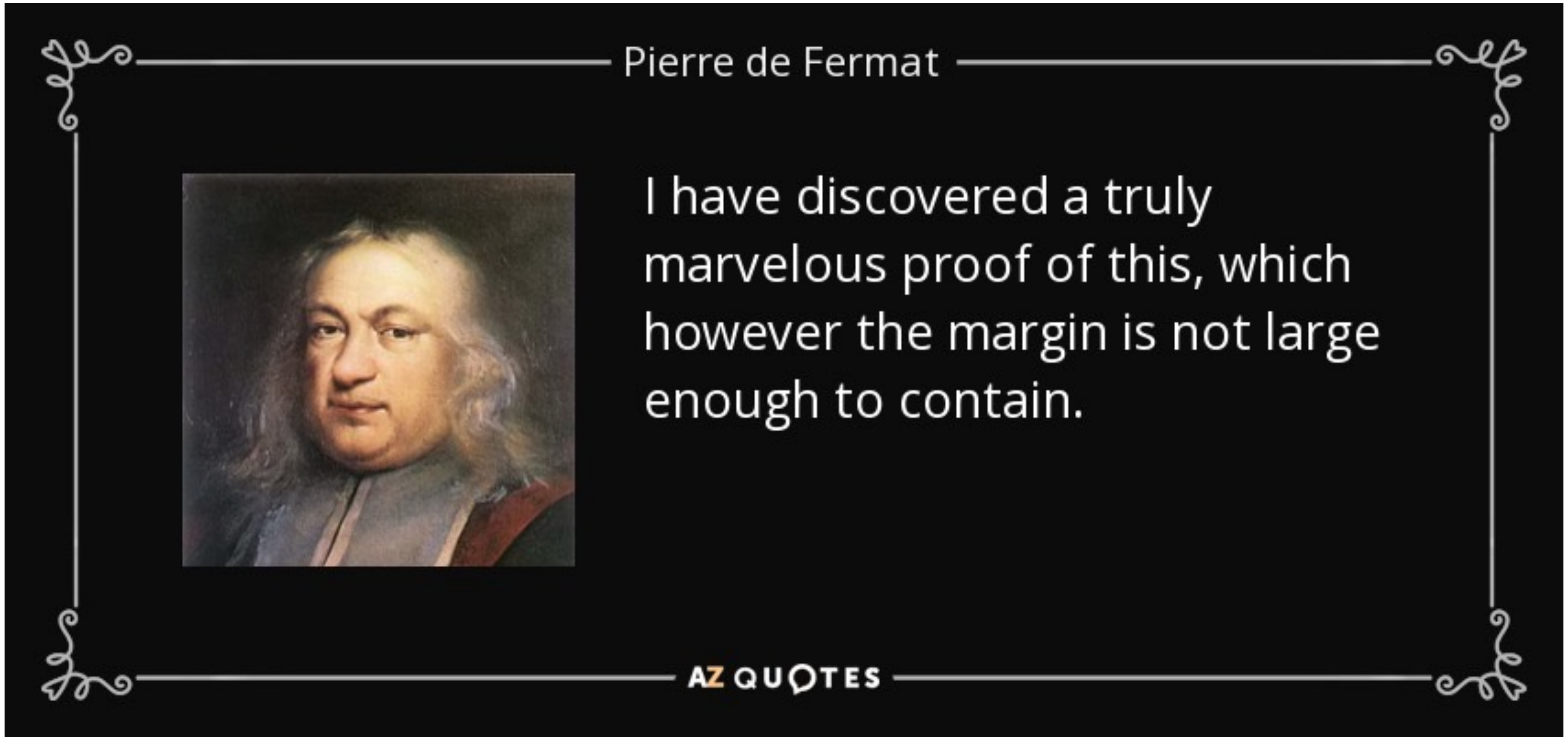
Lecture 2: Mathematical Proofs



Recap of Lecture 1

- Propositions. (mathematical ”sentences”)
    - “$\sqrt{3}$ is irrational”
    - “1+1 = 5”

- NOT Propositions
    - “$2 + 2$”
    - “3x = 6” without specifying what x is

Recap of Lecture 1

- Variables (“Let x be …. ”)
  - In math, we like to name things with variables.
  - We can represent propositions with variables as well!

  - Let P be “$\sqrt{3}$ is irrational”.
  - Let Q be “1+1 = 5”.

Recap of Lecture 1

- Connectives (connect "sentences" to form longer sentences!)
  - Conjunction. $P \land Q$ ("AND")
  - Disjunction. $P \lor Q$ ("OR", logical OR, NOT exclusive OR)
  - Negation. $\neg P$ ("NOT")
  - Implication. $P \Rightarrow Q$ (Short hand for $(\neg P) \lor Q$)

- Proposition Forms (Connectives + Variables)
  - E.g. $(P \land Q) \lor ((\neg P) \land R)$
  - You can plug anything into these variables!

Recap of Lecture 1

- Quantifiers ("Range" of the statement)
  - "For all". $\forall$ + scope of x + proposition about x
  - "Exists". $\exists$ + scope of x + proposition about x

- Logical Equivalence
  - Most importantly $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$ "contrapositive"

Today's Outline

- What is a mathematical proof?
  - Examples
  - Structure

- The art of writing mathematical proofs.
  - Direct Proof.
  - Proof by contraposition.
  - Proof by contradiction.
  - Proof by cases.

What is a mathematical proof?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

We know integer x is odd.
So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b.

We know $x^2 - 1 = (x + 1)(x - 1)$.
So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$.

In conclusion, $x^2 - 1$ is divisible by 4.

What is a mathematical proof?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

What we know is true

We know integer x is odd.

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b.

We know $x^2 - 1 = (x + 1)(x - 1)$.

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$.

What we derived from previous lines

(avoid circular proof)

In conclusion, $x^2 - 1$ is divisible by 4.

What makes the conclusion correct?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

What we know is true

We know integer x is odd. ✅

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b.

We know $x^2 - 1 = (x + 1)(x - 1)$. ✅

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$.

In conclusion, $x^2 - 1$ is divisible by 4.

What makes the conclusion correct?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

What we know is true

We know integer x is odd. ✅

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b. ✅

We know $x^2 - 1 = (x + 1)(x - 1)$. ✅

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$.

In conclusion, $x^2 - 1$ is divisible by 4.

What makes the conclusion correct?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

What we know is true

We know integer x is odd. ✅

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b. ✅

We know $x^2 - 1 = (x+1)(x-1)$. ✅

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$. ✅

In conclusion, $x^2 - 1$ is divisible by 4.

What makes the conclusion correct?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

What we know is true

We know integer x is odd. ✅

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b. ✅

We know $x^2 - 1 = (x + 1)(x - 1)$. ✅

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$. ✅

In conclusion, $x^2 - 1$ is divisible by 4. ✅

What makes the conclusion correct?

Example

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

What we know is true

We know integer x is odd. ✅

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b. ✅

We know $x^2 - 1 = (x + 1)(x - 1)$. ✅

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$. ✅

In conclusion, $x^2 - 1$ is divisible by 4. ✅

What we derived from previous lines

(avoid circular proof)

What is a mathematical proof?

Structure

A mathematical proof is many lines of propositions

proposition-1
proposition-2
proposition-3
.
.
.
proposition-n (the conclusion we want to prove)

Each line is either known to be correct / derived from previous lines.

What is a mathematical proof?

A proof vs. a poem

Written in many lines.

When is elegantly written,
one line more is too much,
one line less is incomplete.

For a poem you use repetition, metaphor……
For a proof you use contraposition, contradiction, cases….

What is a mathematical proof?

What make the proof valid.

First, lines that are known to be correct are correct. ✅

Second, lines that derived from known-to-be correct lines are correct. ✅

Third, lines that derived from known-to-be correct lines and lines that became correct in the second step are correct. ✅

.

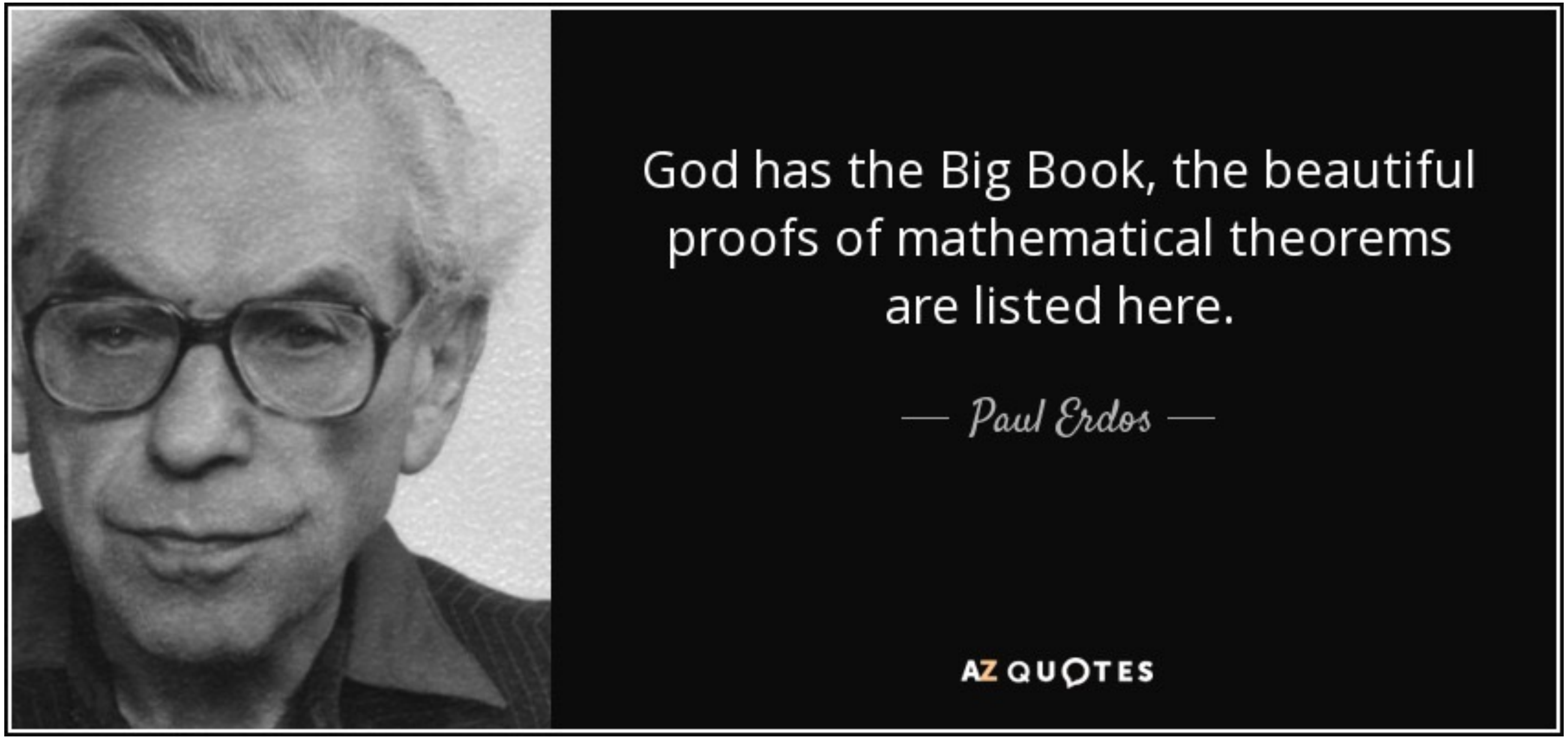
.

.

.

At last, the conclusion becomes correct. ✅

The art of writing mathematical proofs.



Proof Techniques

Direct Proof.

Proof by contraposition.

Proof by contradiction.

Proof by cases.

Direct Proof.

Structure

Goal: To prove $P \Rightarrow Q$.

Approach:

Assume P is true.

proposition

proposition

.

.

.

proposition

Therefore Q

We can add this assumption because of the statement we are proving

Each line is either known to be correct / derived from previous lines.

Direct Proof.

Example : The proof we just saw

Prove that if integer x is odd, then $x^2 - 1$ is divisible by 4.

Proof.

Assuming P

We know integer x is odd.

So $x - 1$ and $x + 1$ are even. Let $x - 1 = 2a$ and $x + 1 = 2b$ for integers a,b.

What we know is true

What we derived from previous lines

We know $x^2 - 1 = (x + 1)(x - 1)$.

So for integers a, b, $x^2 - 1 = 2a * 2b = 4ab$.

In conclusion, $x^2 - 1$ is divisible by 4.

We get Q

Notation setup.

A few notations

Integer	$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.
Natural number	$\mathbb{N} = \{0, 1, 2, \dots\}$ (Culture Debate: Does it start from 0? In 70, it always does!)
Positive Integers	$\mathbb{N}_+ = \{1, 2, 3, \dots\}$
a divides b	$a \mid b$
Prime number	Only divisible by 1 and itself.

Proof by contraposition.

- Logical Equivalence
  - Most importantly $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$ "contrapositive"

Structure

Goal: To prove $P \Rightarrow Q$.

Approach:

Assume $\neg Q$ is true.

proposition

proposition

.

.

.

proposition

Therefore $\neg P$

We proved $\neg Q \Rightarrow \neg P$ which is *equivalent to* $P \Rightarrow Q$

Each line is either known to be correct / derived from previous lines.

Proof by contraposition.

Example 1 :

Suppose $n, d \in \mathbb{N}_+$ and $d \mid n$.

Prove that if n is odd, then d is odd.

We proved $\neg Q \Rightarrow \neg P$

which is *equivalent to*

$P \Rightarrow Q$

Proof.

Assume that d is even.

Then there exists $\mathrm{k} \in \mathbb{N}_+$ such that $d = 2k$.

Because $d \mid n$, we know there exists $\ell \in \mathbb{N}_+$ such that $n = \ell d$.

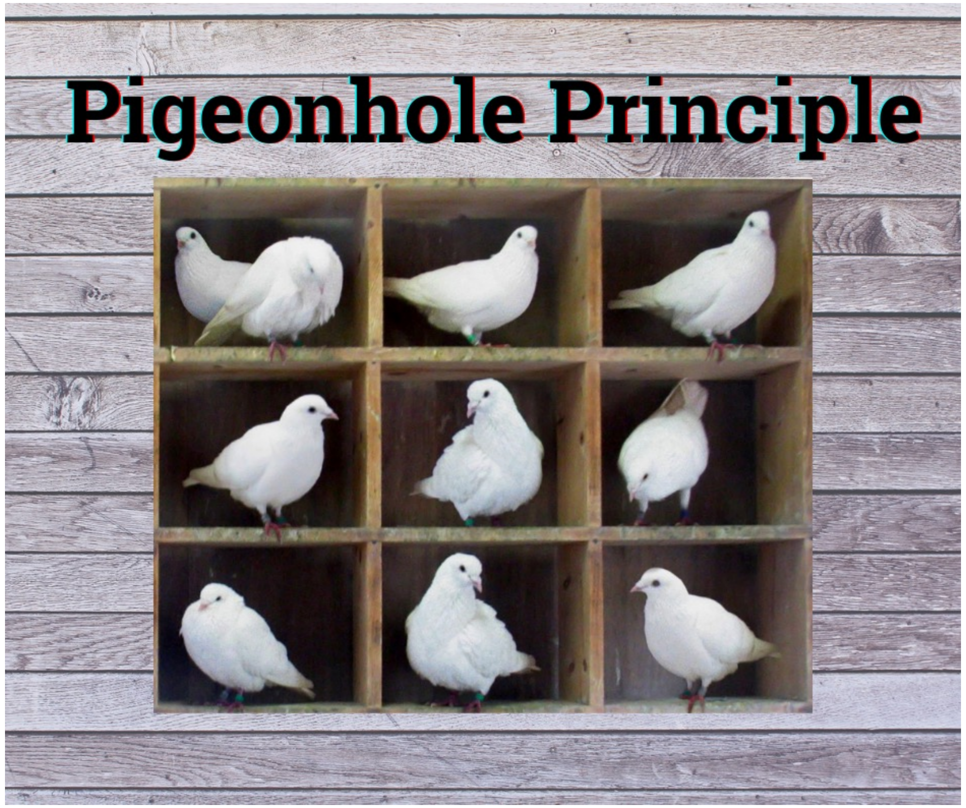
Then $n = \ell d = 2k\ell$.

n is even.

Proof by contraposition.

Example 2 (Pigeonhole principle) :

There are n pigeonholes. Suppose there are $n+1$ pigeons in them. There must exists (at least) two pigeons in the same hole.



Proof by contraposition.

Example 2 (Pigeonhole principle) :

There are n pigeonholes. Suppose there are $n+1$ pigeons in them. There must exists (at least) two pigeons in the same hole.

Proof.

Assume that every hole has only at most one pigeon.
There are n pigeonholes.
Therefore at most n piegons in them.

Proof by contraposition.

Example 3 :

Prove that if n^2 is even, then n is even.

Proof.

Assume that n is odd and $n = 2k + 1$.
Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$.
Hence n^2 is odd.

Proof by contradiction.

Structure

Goal: To prove P.

Approach:

Assume $\neg P$ is true.

.

.

R

.

.

$\neg R$

Contradiction!

Therefore P

The only possibility for a contradiction is that our assumption is wrong.

Each line is either known to be correct / derived from previous lines.

Proof by contradiction.

Example 1.

Prove there exists infinitely many primes.

Proof.

Assume that there are only finitely many primes.

Let these primes be $p_1 < p_2 < \cdots < p_n$.

Then consider $m = p_1 p_2 \cdots p_n + 1$.

Every natural number is either a prime or has a prime divisor.

(We know this Is true. Might prove later in class.)

Because m is not divisible by $p_1, p_2, \ldots, p_n$, m must be a prime.

This contradicts that $p_1, p_2, \ldots, p_n$ are the only primes. ($m > p_n$)

Thus there exits infinitely many primes.

Proof by contradiction.

Example 2.

Prove that $\sqrt{2}$ is irrational.

Proof.

Assume that rational.

There exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{\mathrm{p}}{\mathrm{q}}$. Thus, $p^2 = 2q^2$.

Let x be the odd number such that $q = 2^y \cdot x$.

$p^2 = 2q^2 = 2^{2y+1} \cdot x^2$

Because p^2 is a square, it must have an even number of prime factor 2. (We know this Is true.)

x^2 must be even. Then x is even.

Contradiction. Thus $\sqrt{2}$ is irrational.

Proof by cases.

Structure

Goal: To prove P.

Approach:

Assume R is true.

.

.

P is true.

Now instead assume $\neg R$ is true.

.

.

P is true.

Therefore P is always true.

Proof by cases.

Example (Again, Pigeonhole principle) :

There are n holes. Suppose there are $n+1$ pigeons in them. There must exists (at least) two pigeons in the same hole.

Proof.

Among the first n pigeons, if there are two pigeons in the same hole.
Then there must exists (at least) two pigeons in the same hole among all $n+1$ pigeons.

Among the first n pigeons, if there are NOT two pigeons in the same hole.
Then because there are n holes, each hole must have one pigeon in it.
The (n+1)-th pigeon must be in the same hole with another pigeon.

A hidden proof technique: Reduction

The interview

A mathematician is interviewing for a prestigious job. To make sure he has the right morals, the interviewer gives him the following situation:

"You're late for a meeting, when you come across a burning house, a fire hydrant, and a fire hose lying across the street. What do you do?"

The mathematician responds: "People's lives are more important than the meeting. I screw the fire hose into the hydrant and put out the fire before coming to the office."

A hidden proof technique: Reduction

The interview

The interviewer is impressed, but asks him a followup question just to make sure:

"You're late for a meeting when you pass a fire hose connected to a hydrant, next to a perfectly safe house. What do you do?"

The mathematician thinks for a moment, then replies:

"I unscrew the fire hose, carry it across the street, and set the house on fire. Then I've reduced it to a problem I've already solved."

A proof is correct / wrong

The world of mathematics is cruel.

“Rope breaks at its thinnest point.”

There is no such thing as a 99% correct proof. That is just a wrong proof.

Any step on the logic chain is wrong, the proof is wrong.

When actually writing a proof

DO NOT have to separate it in lines.

Make it concise and elegant.