Lesson 1: Proofs

BATU YALÇIN

History of Proofs

- Ancient Greek
  - Thales (640 – 546 B.C.E)
  - Eudoxus (408 – 350 B.C.E.)
  - Theaetetus (417 – 369 B.C.E.)
- Euclid of Alexandria:
  - Axioms

Euclid's Axioms

P1 Through any pair of distinct points passes a line

P2 For each segment AB and CD, there is a unique point E s.t. B is between A and E, and BE is congruent to CD

P3 For each point C and each point A distinct from C there exists a circle with center C and radius CA

P4 All right angles are congruent

P5 For each line l and point P, there exists a line l' through P that is parallel to l.

(Krantz)

Statement Directly Provable from Euclid's Axioms

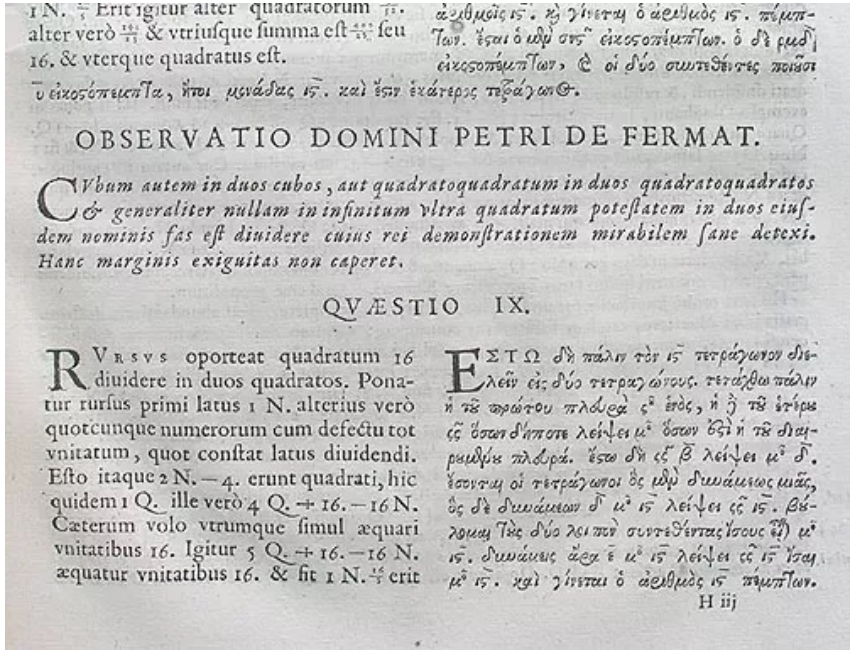
From two points A and B in the plane, there exists a unique circle with AB as its diameter.

Why Do We Need Proofs?

Fermat's Last Theorem:

There doesn't exist $a, b, c \in \mathbb{Z}, n > 2$ s.t.

$$a^n + b^n = c^n$$



alter verò $\frac{16}{1}$ & vtriuſque ſumma eſt $\frac{32}{1}$ ſeu
16. & vterque quadratus eſt.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rurſus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot conſtat latus diuidendi. Eſto itaque 2 N. — 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. — 16 N. Cæterum volo vtrumque ſimul æquari vnitatibus 16. Igitur 5 Q. + 16. — 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{4}{5}$ erit

H iij

Borwein Integrals:

$$\int_0^\infty \frac{\sin x}{x} dx = \frac{\pi}{2}$$

$$\int_0^\infty \frac{\sin x}{x} \frac{\sin x/3}{x/3} dx = \frac{\pi}{2}$$

$$\int_0^\infty \frac{\sin x}{x} \frac{\sin x/3}{x/3} \cdots \frac{\sin x/13}{x/13} dx = \frac{\pi}{2}$$

$$\int_0^\infty \frac{\sin x}{x} \frac{\sin x/3}{x/3} \cdots \frac{\sin x/15}{x/15} dx$$

$$= \frac{467807924713440738696537864469}{935615849440640907310521750000}\pi$$

Types of Proofs

Direct Proof

Logical Structure: p implies q: $p \implies q$

Example:

Prove that the product of two odd integers is odd.

Start: Take two odd integers u, v.

Proof by Contrapositive

Logical Structure: If not q implies p, $\neg q \implies \neg$p, then p implies q: $p \implies q$

Example:

Prove that the product of two odd integers is odd.

Start: Assume that the product of two integers is even.

Proof by Contradiction

Logical Structure: Prove that A leads to B. Assume that B doesn't hold and A holds. Find a contradictory statement

Example:

Prove that the point on circle ω_1 that is closest to the center of a different circle ω_2 lies on the line joining the centers of ω_1 and ω_2

Start: Assume that the length of $\overline{A'O_2}$ for a point A not on the line O_1O_2 is less than $\overline{AO_2}$ for $A \in O_1O_2$

Proof by Bijection (Bijective Proof)

Logical Structure: There exists a bijection between sets A and B. Thus, if property P holds for elements in set B, it will hold for the elements of A mapped by the respective elements in B.

Example:

A composition of an integer n is a set of positive integers $a = (a_1, ..., a_k)$ s.t.

$$\sum_{i=1}^{k} a_i = n$$

Prove that the number of compositions of n is 2^{n-1}

Proof by Exhaustion

Logical Structure: Check every logical case.

Example:

Find $n \in \mathbb{Z}^+$ s.t. $m = n^2 + n + 3$ is a perfect square.

Start: Find a way to reduce the number of cases.

Recognize this Proof

Recognize this Proof

Proposition: Product of two perfect squares is a perfect square.

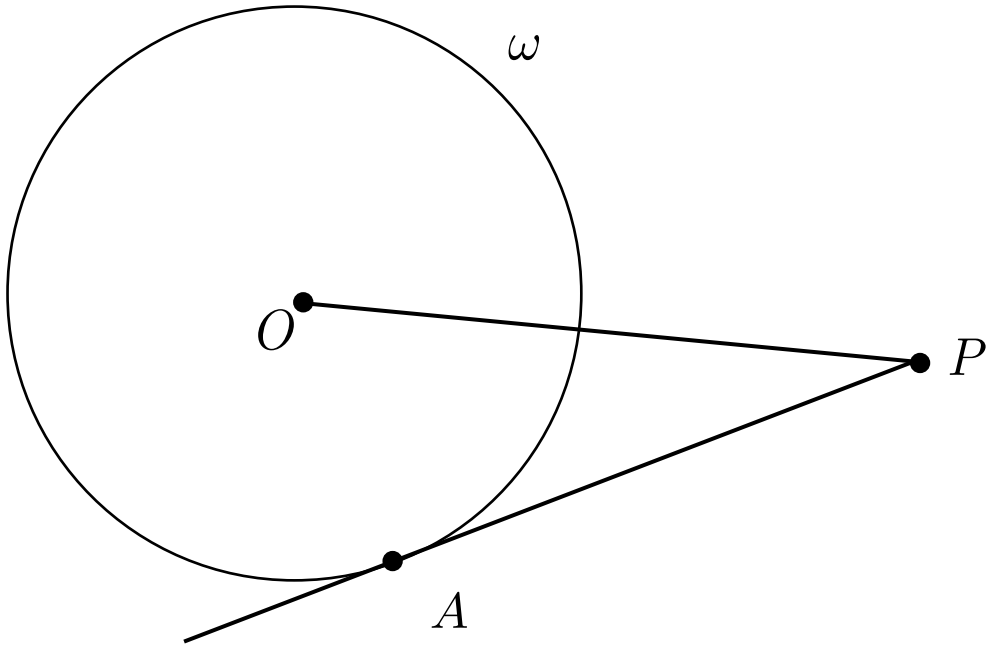
Proof: Let m be an integer that is not a perfect square. Assume that $m = a^2b^2$.
Then, $m = (ab)^2$ which is a perfect square. This is a contradiction.

Thus, m can't be written as a product of two perfect squares.
Then, if m can be written as a product of two perfect squares, m is a perfect square.

Important Mistakes

Circularity

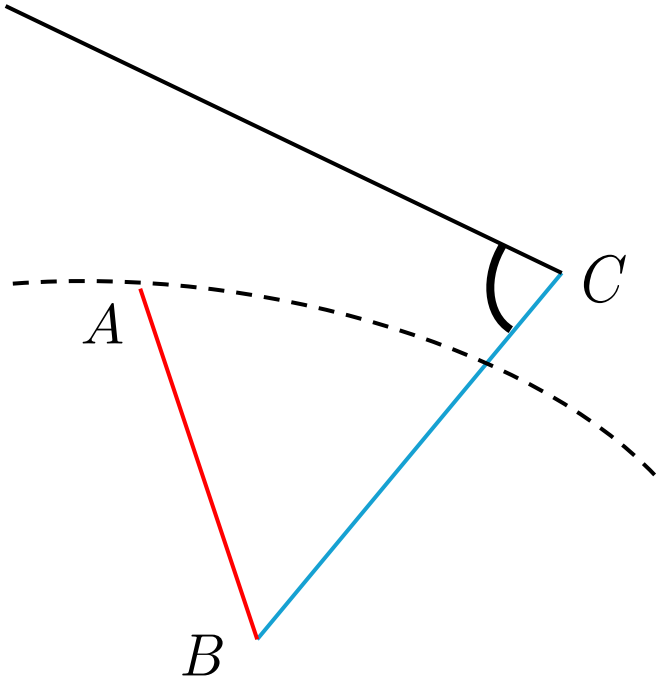
Define by the power of a point P w.r.t. a circle ω by $\text{Pow}_\omega(P) = |OP|^2 - r^2$, O being the center of ω and r being the radius. Prove that if a line *ell* from point P is tangent to ω at A, $\text{Pow}_\omega(P) = PA^2$



Using the theorem on the power of a point, prove the Pythagorean theorem.

Assumptions

Let's say you were asked: Prove that triangle with conditions ... can be determined uniquely.
After some work, you found $|AB|, |BC|, \hat{C}$ uniquely. Here, it may be convenient to end the proof and say that as two sides and one angle is determined uniquely. However, you must be careful, as these information may not allow a triangle to be constructed.



Choosing Your Battles

Existence Proofs:

Prove that for all primes p and $a \in \mathbb{Z}^+$ where a and p are relatively prime, there exists an integer k s.t. $a^k = pm + 1, m \in \mathbb{Z}^+$. In modular arithmetic language, $a^k \equiv 1 \pmod{p}$

Here, DO NOT try to find a specific k for which this is true. Finding that k easily follows through Fermat's Little Theorem; however, if you aren't familiar with this and want to prove this from the beginning, it would be unnecessary work.

Instead, see that there only exists only a finite amount of residues when a number is divided by p: $\emptyset, 1, ..., p-1$ (0 isn't possible as a and p are relatively prime). See that this would lead to two powers of a, a^k, a^n should have the same residue. If you do some algebra, you'll find that a^{k-n} should have a residue of 1 when divided by p.

Construction Proofs (Know When To Try):

Prove that there exists 11 consecutive integers whose squares sum up to a perfect square.

Do not attempt trying random consecutive integers. Write the sum:

$$\sum_{k=-5}^{5} (n+k)^2 = 11n^2 + 2 \cdot (1+4+9+16+25) = 11n^2 + 110 = 11(n^2+10)$$

See that n should have residue 1 when divided by 11. Try 10,12,21,23. You'll see that 23 works.

Providing Counterexamples:

Prove or disprove the statement $m = n^2 + n + 2$ can always be written as 2^k for some k.
Even though $n = -3, -2, -1, 0, 1, 2$ works, if you plug in some larger n, you'll see that this is false: $n = 4 \Rightarrow m = 22$.

Counterexamples or examples can save you from a lot of work when finishing a proof. For example, if you want to prove that a statement works if and only if $k \geq 3$, you may want to prove that it works for $k \geq 3$ and provide counter examples for $k = 1, 2$. Computers are also used to search for counterexamples of famous problems, such as Fermat's Last Theorem and Riemann Hypothesis.

Lesson 2: Advanced Proofs

BATU YALÇIN

Warming Up

Prove that there exists an infinite number of primes.
(Due to Euclid)

Induction

The induction principle consists of this basic idea: If a statement is true for some value, and the truth of a statement for the value before implies its truth for the current value, then the statement is true for all values larger than the initial value.

In more formal terms, if statement A is true for a $k \in \mathbb{Z}$, and A being true for a value $n \geq k$ implies that A is true for $n+1$, A is true for all $n \geq k$

Let's give a basic example. Prove that:

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$$

Let's continue with a more advanced problem. Prove that:

$$F_n = \frac{(a^n - b^n)}{\sqrt{5}}, \quad a = (1+\sqrt{5})/2, b = (1-\sqrt{5})/2$$

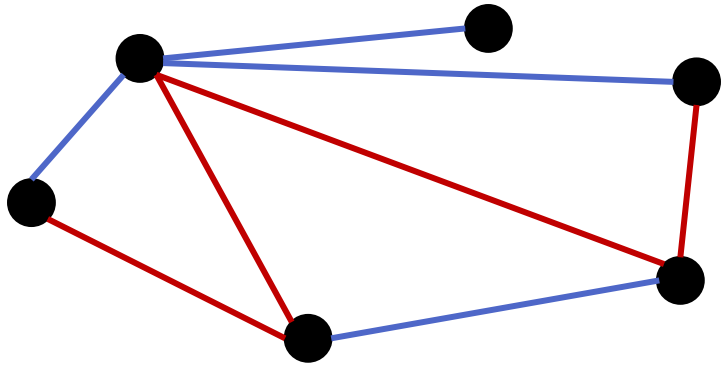
where F_n is the nth Fibonacci number. Do you think that using only k to prove $k+1$ would work here? why not?

Pigeonhole Principle

The statement for the pigeonhole principle is as follows: If there are n holes for pigeons to go in, and $n+1$ pigeons, then at least one hole should have two pigeons in it.

This seemingly trivial principle allows for a lot of statements to be proven with ease. Let's see an example:

In a party, there are 6 people who either know or don't know each other. Prove that there is a group of three in which either no one knows another, or all know each other.



Extremal Principle

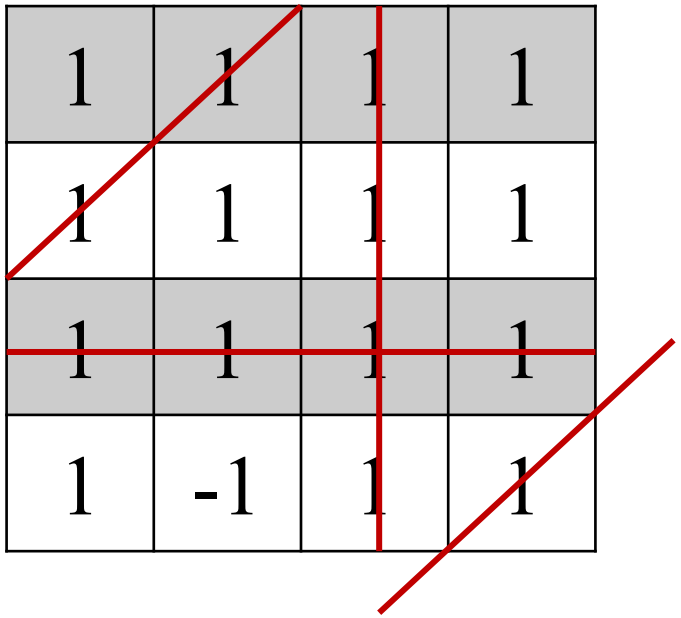
The extremal principle is the technique we've used to prove the infinitude of primes. As an outline, we assume that an element $s \in S$ is an extreme element: the largest, smallest, etc. Let's see an example:

a) Prove that $\sqrt{2}$ is irrational

b) Prove that $\sqrt{p}$ is irrational for a prime p

Invariance Principle

This principle is based on finding an invariant within algorithms. For example, if we are acting on a board with several numbers on it, erasing and writing new ones, we may find that the total sum's parity never changes. As an example, consider the board:



You're only allowed to act on rows, columns, and major/minor diagonals. In each step, you can multiply each number by -1 in the row/column/diagonal you've chosen. Can you make the board have all 1s?