Tashfeen, Ahmad
CS 2813: Tashfeen's Discrete Structures
Spring 2023

Historical Proofs

The proofs given here may contain careless-errors and might not be to someone's high standards of mathematical rigour. These are not meant for anything more than a learning guide of different proof methods for undergraduates who are new to proof writing in mathematics. Please note that the form of arguments presented here is quite likely not the one used by the original authors of proof since I want the students to be able to use and understand the modern mathematical notation.

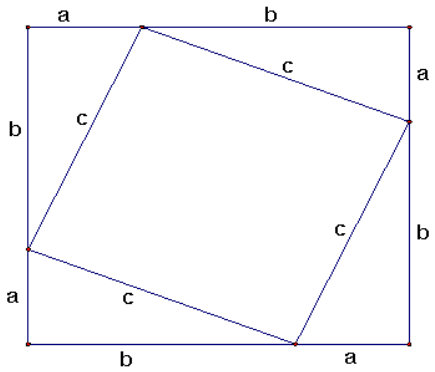

FIGURE 1. Taken from jwilson.coe.uga.edu

1. PYTHAGORAS (C. 570-495 BC)

Proof by Construction. If a right angle triangle has perpendicular side of lengths a, b then its hypotenuse is $c = \sqrt{a^2 + b^2}$ long.

1) Assume a right angle triangle has perpendicular side of lengths a, b.
2) Then four such triangles can be arranged as in figure 1 to form an inscribed square with side length of c. The area of the four such triangles and the inscribed square is,
$$4\left(\frac{1}{2}ab\right) + c^2$$
3) The area of the parameter formed by the triangles is $(a + b)^2$.
4) Note that the area of the four triangles and the inscribed square is the same as the area of the parameter formed by the triangles,
$$4\left(\frac{1}{2}ab\right) + c^2 = (a + b)^2$$
5) We rearrange,
$$\begin{aligned} c^2 &= (a + b)^2 - 4\left(\frac{1}{2}ab\right) && \text{Subtracting } 4\left(\frac{1}{2}ab\right) \text{ from both sides.} \\ c^2 &= a^2 + b^2 + 2ab - 4\left(\frac{1}{2}ab\right) && \text{Expanding } (a + b)^2 \\ c^2 &= a^2 + b^2 + 2ab - 2ab \\ c^2 &= a^2 + b^2 \\ c &= \sqrt{a^2 + b^2} \end{aligned}$$
6) Therefore, a right angle triangle with perpendicular side of lengths a, b has hypotenuse is $c = \sqrt{a^2 + b^2}$ long.

QUOD ERAT DEM■

2. Hippasus of Metapontum (c. 500 BC)

The famous legend that comes with this proof is that Pythagoreans preached all numbers as rational, i. e., expressible as a ratio of integers. Upon proof of $\sqrt{2}$'s irrationality, Hippasus was drowned for crimes against the sanctity of number.

Proof by contradiction. Square-root of two is irrational.

1) Assume for the sake of contradiction that $\sqrt{2} \in \mathbb{Q}$, then $\sqrt{2} = p/q$ for $(p, q) \in \mathbb{Z}^2$ and $\gcd(p, q) = 1$. This last condition requires that the p, q have no common factors or the fraction p/q is in its most reduced form. Then by algebra,

$$\begin{aligned} \left(\sqrt{2}\right)^2 &= \left(\frac{p}{q}\right)^2 && \text{Squaring both sides.} \\ 2 &= \frac{p^2}{q^2} \\ 2q^2 &= p^2 && \text{Multiplying } q^2 \text{ on both sides.} \end{aligned}$$

2) Since q^2 is an integer because the product of two integers is an integer, $2q^2 = p^2$ is an even number.
3) If p^2 is an even number then so is p. Therefore we can write $p = 2c$ for $c \in \mathbb{Z}$. Substituting for p,

$$\begin{aligned} 2q^2 &= (2c)^2 && \text{Since } p = 2c \\ 2q^2 &= 2 \cdot 2c^2 && \text{Dividing 2 on both sides.} \\ q^2 &= 2c^2 \end{aligned}$$

4) By the same closure of integers under multiplication, $c^2 \in \mathbb{Z}$ and q^2 along with q are even. If q is even and p is even then they have common factors $\gcd(p, q) \geq 2$ which is a contradiction! Therefore, $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ is irrational.

QUOD ERAT DEM■

3. Euclid (c. 323-285 BC)

Proof. There are infinitely many prime numbers.

1) Assume for the sake of contradiction that there are finitely many n prime numbers.

$$p_1 < p_2 < p_3 < \cdots < p_n$$

2) Since there are no primes past p_n, we know that

$$p_n < (p_1 \times p_2 \times p_3 \times \cdots \times p_n) + 1 = t \text{ is not a prime number.}$$

3) Since t is not prime, then by the fundamental theorem of arithmetic, t must have a non-trivial prime factor p_i. Therefore, p_i divides t.
4) Note that p_i also divides $p_1 \times p_2 \times p_3 \times \cdots \times p_n$.
5) If p_i divides t and it divides $p_1 \times p_2 \times p_3 \times \cdots \times p_n$ then it divides their difference,

$$t - (p_1 \times p_2 \times p_3 \times \cdots \times p_n) = (p_1 \times p_2 \times p_3 \times \cdots \times p_n) + 1 - (p_1 \times p_2 \times p_3 \times \cdots \times p_n) = 1$$

6) That is a contradiction since p_i does not divide 1. Therefore, there must be infinite prime numbers.

QUOD ERAT DEM■

4. Gauss (1777 - 1855)

Gauss has been said to have written this proof as a 10 year old boy to avoid busy work of adding up the first hundred numbers assigned to him by his school teacher. Read more here.

Proof by Induction. $1+2+3+\cdots+n=\frac{n(n+1)}{2}$

Basis: Take $n \in \{1,2,3,4\}$ then we have,

$$1=\frac{1(1+1)}{2}=1, \quad 1+2=\frac{2(2+1)}{2}=3, \quad 1+2+3=\frac{3(3+1)}{2}=6, \quad 1+2+3+4=\frac{4(4+1)}{2}=10$$

Weak Inductive Hypothesis: Assume for some positive integer n,

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

Strong Inductive Hypothesis: Assume *for all* positive integer *till* some positive integer n,

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

Inductive Step: We show the bellow by induction on n,

$$1+2+3+\cdots+n=\frac{n(n+1)}{2} \Rightarrow 1+2+3+\cdots+(n+1)=\frac{(n+1)((n+1)+1)}{2}$$

Add $n+1$ to $1+2+3+\cdots+n$.

$$1+2+3+\cdots+n+(n+1)=\frac{n(n+1)}{2}+n+1 \qquad \text{By the Inductive Hypothesis.}$$

$$\begin{aligned} 1+2+3+\cdots+(n+1) &= \frac{n(n+1)}{2}+\frac{2(n+1)}{2} \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

Then by induction on n we showed that $1+2+3+\cdots+n=\frac{n(n+1)}{2}$.

QUOD ERAT DEM■

5. Peter Gustav Lejeune Dirichlet (1834)

Proof by Contrapositive. We see m pigeons fly into n trees. If $m > n$ then some tree has at least two pigeons.

1) Assume all trees have zero or one pigeons, i. e., let x_i be the number pigeons in the i^{th} tree, then $x_i \in \{0,1\}$.
2) Then the total number of pigeons is,

$$m=\sum_{i}^{n} x_i \leq n \quad \text{The equality case occurs when all } x_i = 1.$$

3) Therefore, by the contrapositive we know that if $m > n$ then there exists a tree with at least two pigeons.

QUOD ERAT DEM■

6. Tashfeen (2023)

A demonstration in Tashfeen trying to come up with a proof which is easier when proven via contrapositive and failing with flying colours.

We will prove, "For numbers where one is not zero such that if one is rational and the other irrational then the product is irrational."

Proof by Contrapositive. Let $b \neq 0$, $a \notin \mathbb{Q} \wedge b \in \mathbb{Q} \Rightarrow ab \notin \mathbb{Q}$.

1) By contrapositive we establish,

$$\begin{aligned}
&\sim (ab \notin \mathbb{Q}) \Rightarrow \sim (a \notin \mathbb{Q} \wedge b \in \mathbb{Q}) && \\
&\quad ab \in \mathbb{Q} \Rightarrow a \in \mathbb{Q} \vee b \notin \mathbb{Q} && \text{DeMorgan's Law} \\
&\sim (ab \in \mathbb{Q}) \vee a \in \mathbb{Q} \vee b \notin \mathbb{Q} && \text{By } P \Rightarrow Q \iff \sim P \vee Q \\
&\quad ab \notin \mathbb{Q} \vee b \notin \mathbb{Q} \vee a \in \mathbb{Q} && \text{Commutativity of Disjunction} \\
&\sim (ab \in \mathbb{Q} \wedge b \in \mathbb{Q}) \vee a \in \mathbb{Q} && \text{DeMorgan's Law} \\
&\quad (ab \in \mathbb{Q} \wedge b \in \mathbb{Q}) \Rightarrow a \in \mathbb{Q} && \text{By } \sim P \vee Q \iff P \Rightarrow Q
\end{aligned}$$

2) Now we assume, $ab \in \mathbb{Q}$ and $b \in \mathbb{Q}$, then there exists $(m, n) \in \mathbb{Z}^2 \ni (t, w)$ such that,

$$ab = \frac{m}{n}, \quad b = \frac{t}{w}, \quad n \neq w \neq 0$$

3) We not write a as a fraction of integers,

$$\begin{aligned}
a &= a \\
a &= a \times 1 && \text{Times Identity} \\
a &= a \times \frac{b}{b} \\
a &= \frac{ab}{b} \\
a &= \frac{m}{n} \times \frac{w}{t} \\
a &= \frac{mw}{nt}
\end{aligned}$$

4) Since mw and nt are integers, we have shown that $a \in \mathbb{Q}$. QUOD ERAT DEM■

Proof by Contradiction. Let $b \neq 0$, $a \notin \mathbb{Q} \wedge b \in \mathbb{Q} \Rightarrow ab \notin \mathbb{Q}$.

1) Assume for the sake of contraction, $\sim (a \notin \mathbb{Q} \wedge b \in \mathbb{Q} \Rightarrow ab \notin \mathbb{Q})$,

$$\begin{aligned}
&\sim (\sim (a \notin \mathbb{Q} \wedge b \in \mathbb{Q}) \vee (ab \notin \mathbb{Q})) && \text{By } P \Rightarrow Q \iff \sim P \vee Q \\
&\quad a \notin \mathbb{Q} \wedge b \in \mathbb{Q} \wedge ab \in \mathbb{Q} && \text{DeMorgan's}
\end{aligned}$$

2) Since $b \in \mathbb{Q} \wedge ab \in \mathbb{Q}$ then $(ab/b) \in \mathbb{Q}$ because dividing two rationals gives another rational.

3) Then, $(ab/b) = a \in \mathbb{Q}$ and $a \notin \mathbb{Q}$ which is a contradiction. Therefore, $a \notin \mathbb{Q} \wedge b \in \mathbb{Q} \Rightarrow ab \notin \mathbb{Q}$. QUOD ERAT DEM■

University of Oklahoma, Computer Science