MATH 100 – Introduction to the Profession

Proofs

Greg Fasshauer

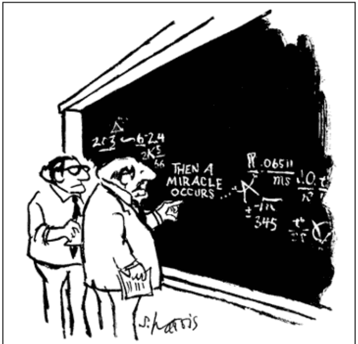
Department of Applied Mathematics
Illinois Institute of Technology

Fall 2012

Outline[1]

[1] Most of this discussion is linked to [Devlin, Section 2.5] and [Gowers, Chapter 3].

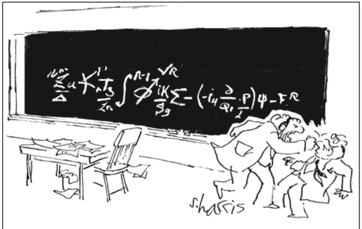
"A *proof* *of a statement in mathematics is a* *logically sound argument that establishes the truth* *of the statement." [Devlin]*



"I think you should be more explicit here in step two."

"A proof of a statement in mathematics is a logically sound argument that establishes the truth of the statement." [Devlin]

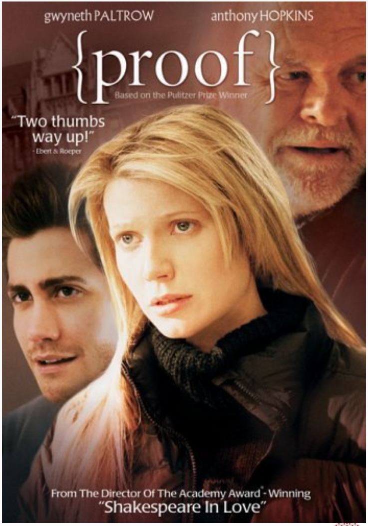
"Mathematicians . . . demand a proof, that is, an argument that puts a statement beyond all possible doubt." [Gowers]

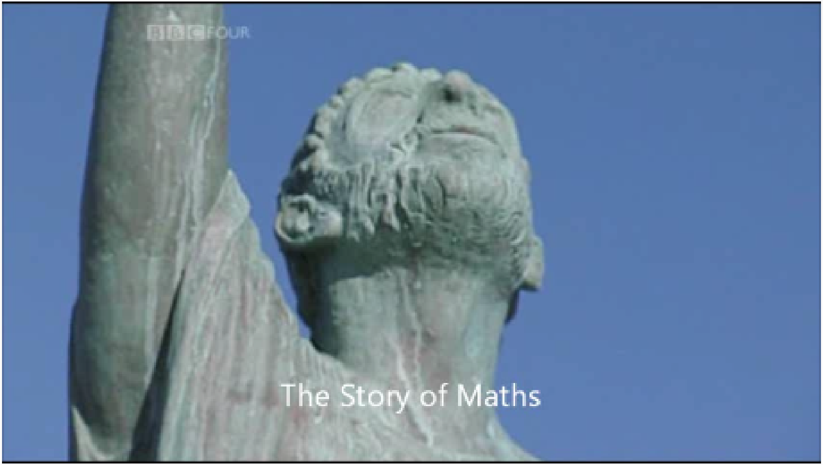


"You want proof? I'll give you proof!"

“A proof of a statement in mathematics is a logically sound argument that establishes the truth of the statement.” [Devlin]

“Mathematicians . . . demand a proof, that is, an argument that puts a statement beyond all possible doubt.” [Gowers]




BBC FOUR
The Story of Maths

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$n = 1$: $991 \cdot 1 + 1 = 992$,

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$n = 1: \; 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496$$

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$n = 1: \; 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \text{T}$$

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$n = 1: \; 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \text{T}$$

$$n = 2: \; 991 \cdot 4 + 1 = 3965, \quad \sqrt{3965} \approx 62.9682 \quad \text{T}$$

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$n = 1: \; 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \text{T}$$

$$n = 2: \; 991 \cdot 4 + 1 = 3965, \quad \sqrt{3965} \approx 62.9682 \quad \text{T}$$

$$n = 3: \; 991 \cdot 9 + 1 = 8920, \quad \sqrt{8920} = 2\sqrt{2230} \approx 94.4458 \quad \text{T}$$

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$n = 1:\ 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \text{T}$$

$$n = 2:\ 991 \cdot 4 + 1 = 3965, \quad \sqrt{3965} \approx 62.9682 \quad \text{T}$$

$$n = 3:\ 991 \cdot 9 + 1 = 8920, \quad \sqrt{8920} = 2\sqrt{2230} \approx 94.4458 \quad \text{T}$$

$$n = 10:\ 991 \cdot 100 + 1 = 99101, \quad \sqrt{99101} \approx 314.803 \quad \text{T}$$

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$n = 1: \; 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \text{T}$$
$$n = 2: \; 991 \cdot 4 + 1 = 3965, \quad \sqrt{3965} \approx 62.9682 \quad \text{T}$$
$$n = 3: \; 991 \cdot 9 + 1 = 8920, \quad \sqrt{8920} = 2\sqrt{2230} \approx 94.4458 \quad \text{T}$$
$$n = 10: \; 991 \cdot 100 + 1 = 99101, \quad \sqrt{99101} \approx 314.803 \quad \text{T}$$
$$n = 537: \; 991 \cdot 288369 + 1 = 285773680, \; \sqrt{285773680} \approx 16904.8 \; \text{T}$$

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$\begin{aligned}
n = 1:&\quad 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \text{T}\\
n = 2:&\quad 991 \cdot 4 + 1 = 3965, \quad \sqrt{3965} \approx 62.9682 \quad \text{T}\\
n = 3:&\quad 991 \cdot 9 + 1 = 8920, \quad \sqrt{8920} = 2\sqrt{2230} \approx 94.4458 \quad \text{T}\\
n = 10:&\quad 991 \cdot 100 + 1 = 99101, \quad \sqrt{99101} \approx 314.803 \quad \text{T}\\
n = 537:&\quad 991 \cdot 288369 + 1 = 285773680, \quad \sqrt{285773680} \approx 16904.8 \quad \text{T}
\end{aligned}$$

`http://www.wolframalpha.com/input/?i=Table[Sqrt[991*n^2%2B1]%2C+{n+%2C1%2C1000}]&cdf=1`

Example

Consider the following problem attributed to Sierpinski:

$$991n^2 + 1 \text{ is not a perfect square.}$$

Is this statement true for all positive integers n?

Try some values:

$$
\begin{aligned}
n = 1&: \ 991 \cdot 1 + 1 = 992, \quad \sqrt{992} = 4\sqrt{62} \approx 31.496 \quad \mathrm{T}\\
n = 2&: \ 991 \cdot 4 + 1 = 3965, \quad \sqrt{3965} \approx 62.9682 \quad \mathrm{T}\\
n = 3&: \ 991 \cdot 9 + 1 = 8920, \quad \sqrt{8920} = 2\sqrt{2230} \approx 94.4458 \quad \mathrm{T}\\
n = 10&: \ 991 \cdot 100 + 1 = 99101, \quad \sqrt{99101} \approx 314.803 \quad \mathrm{T}\\
n = 537&: \ 991 \cdot 288369 + 1 = 285773680, \ \sqrt{285773680} \approx 16904.8 \ \mathrm{T}
\end{aligned}
$$

`http://www.wolframalpha.com/input/?i=Table[Sqrt[991*n^2%2B1]%2C+{n+%2C1%2C1000}]&cdf=1`

Therefore, this statement is *obviously* true.

Not so!

It takes a *looong* time to find a counter-example, but for

$$n = 12055735790331359447442538767$$

we have

$$\begin{aligned} n^2 &= 145340765446276487999885076246978166471414204258297880289 \\ 991n^2 + 1 &= 144032698557259999607886110560755362973171476419973199366400 \end{aligned}$$

Not so!

It takes a *looong* time to find a counter-example, but for

$$n = 12055735790331359447442538767$$

we have

$$\begin{aligned} n^2 &= 145340765446276487999885076246978 16\ldots \\ &\quad 6471414204258297880289 \\ 991n^2+1 &= 144032698557259999607886110560755 36\ldots \\ &\quad 2973171476419973199366400 \\ \sqrt{991n^2+1} &= 379516400906811930638014896080 \end{aligned}$$

Not so!

It takes a *looong* time to find a counter-example, but for

$$n = 12055735790331359447442538767$$

we have

$$\begin{aligned} n^2 &= 145340765446276487999885076246978 16\ldots \\ &\quad 6471414204258297880289 \\ 991n^2+1 &= 1440326985572599996078861105607553 6\ldots \\ &\quad 2973171476419973199366400 \\ \sqrt{991n^2+1} &= 37951640090681193063801489608 0 \quad \textbf{F} \end{aligned}$$

Not so!

It takes a *looong* time to find a counter-example, but for

$$n = 12055735790331359447442538767$$

we have

$$\begin{aligned}
n^2 &= 1453407654462764879998850762469781 6\ldots \\
&\quad 6471414204258297880289 \\
991n^2+1 &= 14403269855725999960788611056075536\ldots \\
&\quad 2973171476419973199366400 \\
\sqrt{991n^2+1} &= 379516400906811930638014896080 \quad \textbf{F}
\end{aligned}$$

Conclusion

Simply checking (many) examples is not good enough to rigorously establish the truth of a statement. We need a mathematical proof.

Theorem (Exercise 2.5.5(e) in [Devlin])

The product of an even and an odd integer is even.

Theorem (Exercise 2.5.5(e) in [Devlin])

The product of an even and an odd integer is even.

Proof.

To formalize this we assume m is the even integer and n is the odd one. Then the statement we want to prove is

$$(\forall m, n \in \mathbb{Z})\,[((m \text{ even}) \wedge (n \text{ odd})) \Rightarrow (mn \text{ even})]\,.$$

Theorem (Exercise 2.5.5(e) in [Devlin])

The product of an even and an odd integer is even.

Proof.

To formalize this we assume m is the even integer and n is the odd one. Then the statement we want to prove is

$$(\forall m, n \in \mathbb{Z}) \left[((m \text{ even}) \wedge (n \text{ odd})) \Rightarrow (mn \text{ even}) \right].$$

We can represent

- any even integer as $m = 2k$, for some integer k and
- any odd integer $n = 2\ell + 1$ for some (other) integer ℓ.

Theorem (Exercise 2.5.5(e) in [Devlin])

The product of an even and an odd integer is even.

Proof.

To formalize this we assume m is the even integer and n is the odd one. Then the statement we want to prove is

$$(\forall m, n \in \mathbb{Z}) \left[((m \text{ even}) \wedge (n \text{ odd})) \Rightarrow (mn \text{ even}) \right].$$

We can represent

- any even integer as $m = 2k$, for some integer k and
- any odd integer $n = 2\ell + 1$ for some (other) integer ℓ.

Now

$$mn = (2k)(2\ell + 1)$$

Theorem (Exercise 2.5.5(e) in [Devlin])

The product of an even and an odd integer is even.

Proof.

To formalize this we assume m is the even integer and n is the odd one. Then the statement we want to prove is

$$(\forall m, n \in \mathbb{Z})\left[((m \text{ even}) \wedge (n \text{ odd})) \Rightarrow (mn \text{ even})\right].$$

We can represent

- any even integer as $m = 2k$, for some integer k and
- any odd integer $n = 2\ell + 1$ for some (other) integer ℓ.

Now

$$mn = (2k)(2\ell + 1) = 2(2k\ell + k)$$

Theorem (Exercise 2.5.5(e) in [Devlin])

The product of an even and an odd integer is even.

Proof.

To formalize this we assume m is the even integer and n is the odd one. Then the statement we want to prove is

$$(\forall m, n \in \mathbb{Z}) \left[((m \text{ even}) \wedge (n \text{ odd})) \Rightarrow (mn \text{ even}) \right].$$

We can represent

- any even integer as $m = 2k$, for some integer k and
- any odd integer $n = 2\ell + 1$ for some (other) integer ℓ.

Now

$$mn = (2k)(2\ell + 1) = 2(2k\ell + k)$$

and since $2k\ell + k$ is an integer[a] we see that $mn = (2 \times \text{integer})$ is even. □

[a] It doesn't matter if even or odd.

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

Proof.

Here ψ corresponds to "*n* is even". So we assume that

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

Proof.

Here ψ corresponds to "*n* is even". So we assume that "*n* is not even", i.e., *n* is odd.
The theorem is proved if we can show

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

Proof.

Here ψ corresponds to "n is even". So we assume that "n is not even", i.e., n is odd.
The theorem is proved if we can show $(\neg\phi)$, i.e., that n^2 is odd.
Any odd number can be represented as $n = 2k + 1$, for some integer k.
Therefore,

$$n^2 = (2k+1)^2$$

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

Proof.

Here ψ corresponds to "n is even". So we assume that "n is not even", i.e., n is odd.
The theorem is proved if we can show $(\neg\phi)$, i.e., that n^2 is odd.
Any odd number can be represented as $n = 2k + 1$, for some integer k.
Therefore,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

Proof.

Here ψ corresponds to "n is even". So we assume that "n is not even", i.e., n is odd.
The theorem is proved if we can show $(\neg\phi)$, i.e., that n^2 is odd.
Any odd number can be represented as $n = 2k + 1$, for some integer k.
Therefore,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

As mentioned earlier, proving a statement $\phi \Rightarrow \psi$ directly is difficult. Use of the contrapositive, $(\neg\psi) \Rightarrow (\neg\phi)$, often helps.

Theorem

For all integers n, if n^2 is even then n is even.

Proof.

Here ψ corresponds to "n is even". So we assume that "n is not even", i.e., n is odd.
The theorem is proved if we can show $(\neg\phi)$, i.e., that n^2 is odd.
Any odd number can be represented as $n = 2k + 1$, for some integer k.
Therefore,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $2k^2 + 2k$ is also an integer we have shown that n^2 is odd, and we are done. $\square$

We assume that the conclusion to be proved is false, and argue that this leads to a contradiction.

We assume that the conclusion to be proved is false, and argue that this leads to a contradiction.

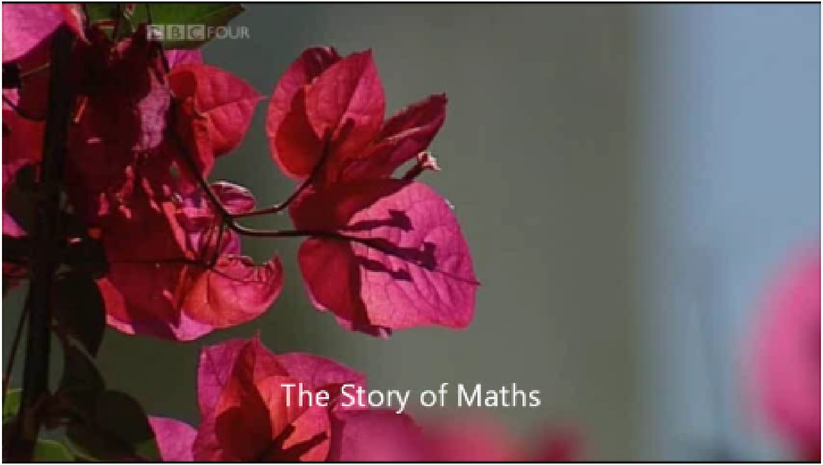
> *“Reductio ad absurdum, which Euclid loved so much, is one of a mathematician’s finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.” [Hardy]*

We assume that the conclusion to be proved is false, and argue that this leads to a contradiction.

> *"Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game." [Hardy]*

Some of the most famous examples of proofs by contradiction are:

- The proof that $\sqrt{2}$ is irrational (probably dating back to Aristotle ca. 350 B.C., see [Devlin, Section 2.5], [Gowers, Chapter 3]).
- The proof that there are infinitely many primes (dating back to Euclid ca. 300 B.C., see below).


BBC FOUR
The Story of Maths

To prove a statement of the form

$$(\forall n \in \mathbb{N})\, A(n)$$

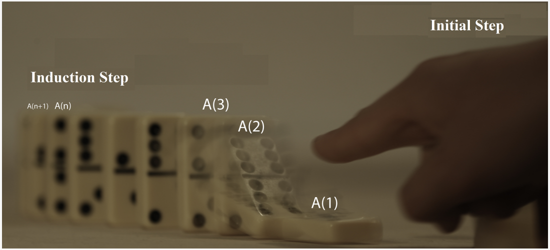
To prove a statement of the form

$$(\forall n \in \mathbb{N})\, A(n)$$

1. Initial step: Show that $A(1)$ holds
2. Induction step: Assume that $A(n)$ holds for an arbitrary n and show that $A(n+1)$ follows, i.e., show

$$(\forall n \in \mathbb{N})\, [A(n) \Rightarrow A(n+1)]$$

3. Combining (1) and (2) we conclude that the statement holds.



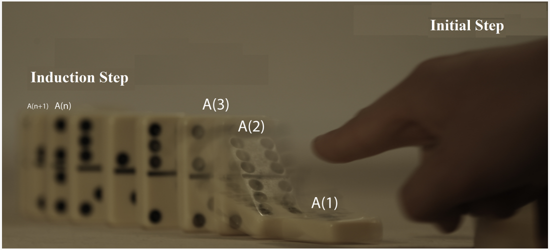
To prove a statement of the form

$$(\forall n \in \mathbb{N})\, A(n)$$

1. Initial step: Show that $A(1)$ holds
2. Induction step: Assume that $A(n)$ holds for an arbitrary n and show that $A(n+1)$ follows, i.e., show

$$(\forall n \in \mathbb{N})\, [A(n) \Rightarrow A(n+1)]$$

3. Combining (1) and (2) we conclude that the statement holds.



To prove a statement of the form

$$(\forall n \in \mathbb{N})\, A(n)$$

1. Initial step: Show that $A(1)$ holds
2. Induction step: Assume that $A(n)$ holds for an arbitrary n and show that $A(n+1)$ follows, i.e., show

$$(\forall n \in \mathbb{N})\, [A(n) \Rightarrow A(n+1)]$$

3. Combining (1) and (2) we conclude that the statement holds.

This works because of the axioms that define the natural numbers.

Theorem (Exercise 2.5.7(a) in [Devlin], Gauss (9 years old))

For any natural number n, $1+2+3+\ldots+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Theorem (Exercise 2.5.7(a) in [Devlin], Gauss (9 years old))

For any natural number n, $1+2+3+\ldots+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof

We use mathematical induction to prove $(\forall n \in \mathbb{N})\, A(n)$, where

$A(n)$ stands for

Theorem (Exercise 2.5.7(a) in [Devlin], Gauss (9 years old))

For any natural number n, $1+2+3+\ldots+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof

We use mathematical induction to prove $(\forall n \in \mathbb{N})\, A(n)$, where

$$A(n) \text{ stands for } \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Theorem (Exercise 2.5.7(a) in [Devlin], Gauss (9 years old))

For any natural number n, $1+2+3+\ldots+n=\sum_{k=1}^{n} k=\frac{n(n+1)}{2}$.

Proof

We use mathematical induction to prove $(\forall n \in \mathbb{N})\, A(n)$, where

$$A(n) \text{ stands for } \sum_{k=1}^{n} k=\frac{n(n+1)}{2}.$$

The initial step

$$A(1) \text{ corresponds to}$$

Theorem (Exercise 2.5.7(a) in [Devlin], Gauss (9 years old))

For any natural number n, $1+2+3+\ldots+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$

Proof

We use mathematical induction to prove $(\forall n \in \mathbb{N})\, A(n)$, where

$$A(n) \text{ stands for } \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

The initial step

$$A(1) \text{ corresponds to } \sum_{k=1}^{1} k = \frac{1(1+1)}{2}.$$

Theorem (Exercise 2.5.7(a) in [Devlin], Gauss (9 years old))

For any natural number n, $1+2+3+\ldots+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof

We use mathematical induction to prove $(\forall n \in \mathbb{N})\, A(n)$, where

$$A(n) \text{ stands for } \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

The initial step

$$A(1) \text{ corresponds to } \sum_{k=1}^{1} k = \frac{1(1+1)}{2}.$$

Since both sides of this equality evaluate to one we have ensured that the initial step holds.

Proof cont.

For the induction step

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.
The left-hand side of $A(n+1)$ is

$$\sum_{k=1}^{n+1} k \quad = \quad 1+2+3+\ldots+n+(n+1) =$$

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.
The left-hand side of $A(n+1)$ is

$$\sum_{k=1}^{n+1} k \quad = \quad 1+2+3+\ldots+n+(n+1) = \sum_{k=1}^{n} k + (n+1)$$

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.
The left-hand side of $A(n+1)$ is

$$\sum_{k=1}^{n+1} k = 1+2+3+\ldots+n+(n+1) = \sum_{k=1}^{n} k + (n+1)$$

$$\overset{A(n) \text{ holds}}{=} \frac{n(n+1)}{2} + (n+1)$$

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.
The left-hand side of $A(n+1)$ is

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= 1+2+3+\ldots+n+(n+1) = \sum_{k=1}^{n} k + (n+1) \\
&\overset{A(n)\text{ holds}}{=} \frac{n(n+1)}{2} + (n+1) \\
&= (n+1)\left(\frac{n}{2}+1\right)
\end{aligned}$$

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.
The left-hand side of $A(n+1)$ is

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= 1+2+3+\ldots+n+(n+1) = \sum_{k=1}^{n} k + (n+1) \\
&\stackrel{A(n) \text{ holds}}{=} \frac{n(n+1)}{2} + (n+1) \\
&= (n+1)\left(\frac{n}{2}+1\right) = (n+1)\left(\frac{n}{2}+\frac{2}{2}\right) = (n+1)\frac{n+2}{2},
\end{aligned}$$

Proof cont.

For the induction step we assume that $A(n)$ holds for an arbitrary (but fixed) value of n and try to show that $A(n+1)$ follows.
The left-hand side of $A(n+1)$ is

$$\begin{aligned}\sum_{k=1}^{n+1} k &= 1+2+3+\ldots+n+(n+1) = \sum_{k=1}^{n} k + (n+1) \\ &\overset{A(n)\text{ holds}}{=} \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2}+1\right) = (n+1)\left(\frac{n}{2}+\frac{2}{2}\right) = (n+1)\frac{n+2}{2},\end{aligned}$$

but this corresponds to the right-hand side of $A(n+1)$.
Since both the initial step and the induction step are true, the statement follows for all $n \in \mathbb{N}$.

Gauss actually proved the above theorem directly (see [Gauss's Day of Reckoning]).

Gauss actually proved the above theorem directly (see [Gauss's Day of Reckoning]).
How would such a direct proof go?

Gauss actually proved the above theorem directly (see [Gauss's Day of Reckoning]).

How would such a direct proof go?

Little Gauss had to solve only the problem for $n = 100$:

$$1 \quad + \quad 2 \quad + \quad 3 \quad + \quad \ldots \quad + \quad 98 \quad + \quad 99 \quad + \quad 100$$

Gauss actually proved the above theorem directly (see [Gauss's Day of Reckoning]).
How would such a direct proof go?
Little Gauss had to solve only the problem for $n = 100$:

$$
\begin{array}{ccccccccccccc}
1 & + & 2 & + & 3 & + & \ldots & + & 98 & + & 99 & + & 100 \\
100 & + & 99 & + & 98 & + & \ldots & + & 3 & + & 2 & + & 1 \\
\hline
\end{array}
$$

Gauss actually proved the above theorem directly (see [Gauss's Day of Reckoning]).
How would such a direct proof go?
Little Gauss had to solve only the problem for $n = 100$:

$$\begin{array}{ccccccccccccc} 1 & + & 2 & + & 3 & + & \ldots & + & 98 & + & 99 & + & 100 \\ 100 & + & 99 & + & 98 & + & \ldots & + & 3 & + & 2 & + & 1 \\ \hline 101 & + & 101 & + & 101 & + & \ldots & + & 101 & + & 101 & + & 101 \end{array}$$

Gauss actually proved the above theorem directly (see [Gauss's Day of Reckoning]).

How would such a direct proof go?

Little Gauss had to solve only the problem for $n = 100$:

$$\begin{array}{ccccccccccccc} 1 & + & 2 & + & 3 & + & \ldots & + & 98 & + & 99 & + & 100 \\ \\ 100 & + & 99 & + & 98 & + & \ldots & + & 3 & + & 2 & + & 1 \\ \hline 101 & + & 101 & + & 101 & + & \ldots & + & 101 & + & 101 & + & 101 \end{array}$$

The number 101 is added 100 times, but we used two copies of the sum we wanted to compute, so

$$1 + 2 + 3 + \ldots + 98 + 99 + 100 = \frac{1}{2} 100 \cdot 101.$$

For general n the argument is analogous:

1	+	2	+	3	+	...	+	(n-2)	+	(n-1)	+	n
n	+	(n-1)	+	(n-2)	+	...	+	3	+	2	+	1
(n+1)	+	(n+1)	+	(n+1)	+	...	+	(n+1)	+	(n+1)	+	(n+1)

and we have

$$1 + 2 + 3 + \ldots + (n-2) + (n-1) + n = \frac{1}{2}n(n+1).$$

For general n the argument is analogous:

1	+	2	+	3	+	...	+	(n-2)	+	(n-1)	+	n
n	+	(n-1)	+	(n-2)	+	...	+	3	+	2	+	1
(n+1)	+	(n+1)	+	(n+1)	+	...	+	(n+1)	+	(n+1)	+	(n+1)

and we have

$$1 + 2 + 3 + \ldots + (n-2) + (n-1) + n = \frac{1}{2}n(n+1).$$

This same problem can already be found (with a very similar solution) in [Problems to Sharpen the Young] by the English scholar Alcuin of York written in the 8$^{\text{th}}$ century.

Recall our problem from the beginning of the semester, where we conjectured the following:

Theorem

If the sequence $a_0, a_1, a_2, \ldots$ *satisfies*

$$a_{m+n} + a_{m-n} = \frac{1}{2}\left(a_{2m} + a_{2n}\right) \tag{*}$$

for all nonnegative integers m *and* n *with* $m \geq n$ *and* $a_1 = 1$*, then* $a_n = n^2$ *for all* $n \in \mathbb{N}_0$*.*

Recall our problem from the beginning of the semester, where we conjectured the following:

Theorem

If the sequence $a_0, a_1, a_2, \ldots$ satisfies

$$a_{m+n} + a_{m-n} = \frac{1}{2}\left(a_{2m} + a_{2n}\right) \qquad (*)$$

for all nonnegative integers m and n with $m \geq n$ and $a_1 = 1$, then $a_n = n^2$ for all $n \in \mathbb{N}_0$.

While we computed a number of special values that might serve as the initial step of a mathematical induction proof for this problem, such as

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = 4, \quad a_3 = 9, \quad \text{and even } a_{2m} = 4a_m,$$

ordinary induction does not suffice for this proof.

Instead we can use strong (or complete) induction. Here the induction step is:

- Assume that for an arbitrary n all of the following statements hold

$$A(1), A(2), \ldots, A(n)$$

and show that then $A(n+1)$ follows.

Instead we can use strong (or complete) induction. Here the induction step is:

- Assume that for an arbitrary n all of the following statements hold

$$A(1), A(2), \ldots, A(n)$$

  and show that then $A(n+1)$ follows.

So – in contrast to ordinary induction – we now take advantage of complete historical information.

Instead we can use strong (or complete) induction. Here the induction step is:

- Assume that for an arbitrary n all of the following statements hold

$$A(1), A(2), \ldots, A(n)$$

  and show that then $A(n+1)$ follows.

So – in contrast to ordinary induction – we now take advantage of complete historical information.

Using the domino analogy, we're using not only the immediate predecessor to knock over the n^{th} domino, but we're allowed to use the combined force of all of its predecessors.

Proof (of sequence problem).

Let $A(n)$ be the statement that $a_n = n^2$.
Certainly the initial step $A(0)$ is true.

Proof (of sequence problem).

Let $A(n)$ be the statement that $a_n = n^2$.
Certainly the initial step $A(0)$ is true.
Induction step: assume that $A(k)$ is true for all $k = 0, 1, \ldots, m$.
We have (using m and $n = 1$ in $(*)$, and $a_{2m} = 4a_m$ and $a_2 = 4$)

$$a_{m+1} + a_{m-1} = \frac{1}{2}\left(a_{2m} + a_2\right)$$

Proof (of sequence problem).

Let $A(n)$ be the statement that $a_n = n^2$.
Certainly the initial step $A(0)$ is true.
Induction step: assume that $A(k)$ is true for all $k = 0, 1, \ldots, m$.
We have (using m and $n = 1$ in $(*)$, and $a_{2m} = 4a_m$ and $a_2 = 4$)

$$a_{m+1} + a_{m-1} = \frac{1}{2}(a_{2m} + a_2) = \frac{1}{2}(4a_m + 4) = 2a_m + 2.$$

Proof (of sequence problem).

Let $A(n)$ be the statement that $a_n = n^2$.
Certainly the initial step $A(0)$ is true.
Induction step: assume that $A(k)$ is true for all $k = 0, 1, \ldots, m$.
We have (using m and $n = 1$ in $(*)$, and $a_{2m} = 4a_m$ and $a_2 = 4$)

$$a_{m+1} + a_{m-1} = \frac{1}{2}(a_{2m} + a_2) = \frac{1}{2}(4a_m + 4) = 2a_m + 2.$$

Using our assumption that both $A(m)$ and $A(m-1)$ hold, we get

$$(a_{m+1} + a_{m-1} = 2a_m + 2) \Longleftrightarrow \left(a_{m+1} + (m-1)^2 = 2m^2 + 2\right)$$

Proof (of sequence problem).

Let $A(n)$ be the statement that $a_n = n^2$.
Certainly the initial step $A(0)$ is true.
Induction step: assume that $A(k)$ is true for all $k = 0, 1, \ldots, m$.
We have (using m and $n = 1$ in $(*)$, and $a_{2m} = 4a_m$ and $a_2 = 4$)

$$a_{m+1} + a_{m-1} = \frac{1}{2}(a_{2m} + a_2) = \frac{1}{2}(4a_m + 4) = 2a_m + 2.$$

Using our assumption that both $A(m)$ and $A(m-1)$ hold, we get

$$(a_{m+1} + a_{m-1} = 2a_m + 2) \iff \left(a_{m+1} + (m-1)^2 = 2m^2 + 2\right)$$

or

$$a_{m+1} = 2m^2 + 2 - (m^2 - 2m + 1) = m^2 + 2m + 1 = (m+1)^2,$$

Proof (of sequence problem).

Let $A(n)$ be the statement that $a_n = n^2$.
Certainly the initial step $A(0)$ is true.
Induction step: assume that $A(k)$ is true for all $k = 0, 1, \ldots, m$.
We have (using m and $n = 1$ in $(*)$, and $a_{2m} = 4a_m$ and $a_2 = 4$)

$$a_{m+1} + a_{m-1} = \frac{1}{2}(a_{2m} + a_2) = \frac{1}{2}(4a_m + 4) = 2a_m + 2.$$

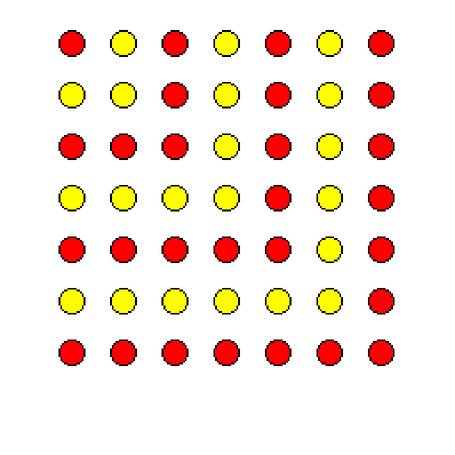
Using our assumption that both $A(m)$ and $A(m-1)$ hold, we get

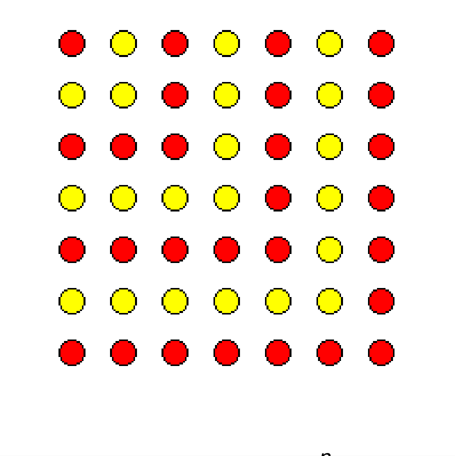
$$(a_{m+1} + a_{m-1} = 2a_m + 2) \iff \left(a_{m+1} + (m-1)^2 = 2m^2 + 2\right)$$

or

$$a_{m+1} = 2m^2 + 2 - (m^2 - 2m + 1) = m^2 + 2m + 1 = (m+1)^2,$$

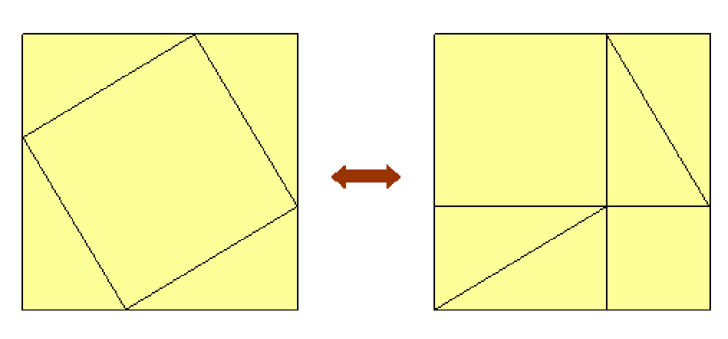
which corresponds to $A(m+1)$. $\square$

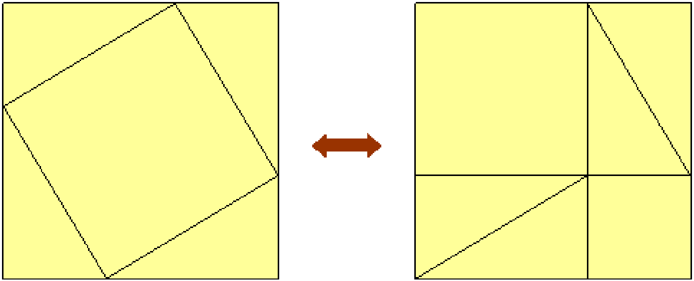




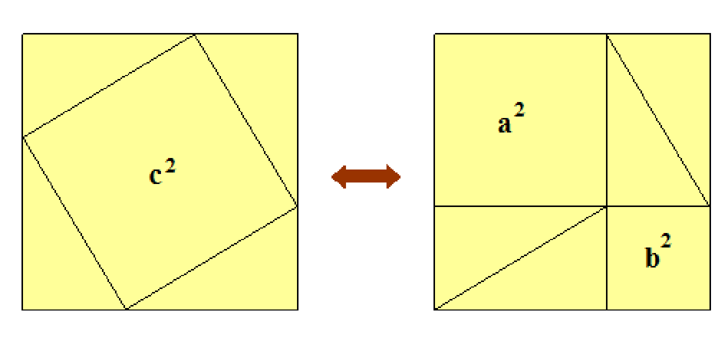
$$1 + 3 + 5 + \ldots + (2n - 1) = \sum_{k=1}^{n} (2k - 1) = n^2$$

See also HW problem 2.5.8(b) in [Devlin].





$$a^2 + b^2 = c^2$$

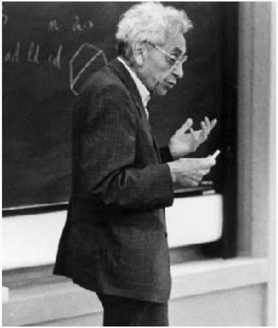


$$a^2 + b^2 = c^2$$

See also [Gowers, Chapter 3].


BBC FOUR
The Story of Maths

“This one’s from the book.” (Paul Erdős)



Refers to (famous) results with beautiful/elegant proofs.

Example

The Basel problem, first proved by Leonhard Euler in 1735:

Example

The Basel problem, first proved by Leonhard Euler in 1735:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Example

The Basel problem, first proved by Leonhard Euler in 1735:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

One way to prove this is via Fourier series (see MATH 461).

See [Proofs from THE BOOK] for three different proofs.

Theorem (Book IX, Prop. 20 of Euclid’s [Elements])

There are infinitely many primes.

Theorem (Book IX, Prop. 20 of Euclid's [Elements])

There are infinitely many primes.

Euclid's Proof (a proof by contradiction).

Assume there are *finitely many* primes: $\{p_1, \ldots, p_r\}$

Theorem (Book IX, Prop. 20 of Euclid's [Elements])

There are infinitely many primes.

Euclid's Proof (a proof by contradiction).

Assume there are *finitely many* primes: $\{p_1, \ldots, p_r\}$
Now consider the number $n = p_1 p_2 \cdots p_r + 1$.

Theorem (Book IX, Prop. 20 of Euclid's [Elements])

There are infinitely many primes.

Euclid's Proof (a proof by contradiction).

Assume there are *finitely many* primes: $\{p_1, \ldots, p_r\}$
Now consider the number $n = p_1 p_2 \cdots p_r + 1$.
According to our assumption, n is not a prime number (it's obviously not one of the p_i), so it has prime divisor, say p.

Theorem (Book IX, Prop. 20 of Euclid's [Elements])

There are infinitely many primes.

Euclid's Proof (a proof by contradiction).

Assume there are *finitely many* primes: $\{p_1, \ldots, p_r\}$
Now consider the number $n = p_1 p_2 \cdots p_r + 1$.
According to our assumption, n is not a prime number (it's obviously not one of the p_i), so it has prime divisor, say p.
But p is not one of the p_i either since otherwise p would not only be a divisor of n, but also of the product $p_1 p_2 \cdots p_r$.

Theorem (Book IX, Prop. 20 of Euclid’s [Elements])

There are infinitely many primes.

Euclid’s Proof (a proof by contradiction).

Assume there are *finitely many* primes: $\{p_1, \ldots, p_r\}$
Now consider the number $n = p_1 p_2 \cdots p_r + 1$.
According to our assumption, n is not a prime number (it’s obviously not one of the p_i), so it has prime divisor, say p.
But p is not one of the p_i either since otherwise p would not only be a divisor of n, but also of the product $p_1 p_2 \cdots p_r$.
Consequently, p would be a divisor of the difference $n - p_1 p_2 \cdots p_r = 1$.

Theorem (Book IX, Prop. 20 of Euclid's [Elements])

There are infinitely many primes.

Euclid's Proof (a proof by contradiction).

Assume there are *finitely many* primes: $\{p_1, \ldots, p_r\}$
Now consider the number $n = p_1 p_2 \cdots p_r + 1$.
According to our assumption, n is not a prime number (it's obviously not one of the p_i), so it has prime divisor, say p.
But p is not one of the p_i either since otherwise p would not only be a divisor of n, but also of the product $p_1 p_2 \cdots p_r$.
Consequently, p would be a divisor of the difference $n - p_1 p_2 \cdots p_r = 1$.
But that is impossible, and so we have a contradiction, which means that set $\{p_1, \ldots, p_r\}$ cannot contain all primes. $\square$

The concept of proof is also relevant outside of mathematics.

In [The Elements of a Proposition] the authors analyze some of Abraham Lincoln’s speeches as they relate to Euclid’s [Elements].

Try this in MATLAB:

```
load penny.mat
contour(P,15)
colormap(copper)
axis ij square
```

Summary

You may see some of these proofs again in classes such as

- MATH 230 – Introduction to Discrete Math
- MATH 410 – Number Theory

Other classes that depend on lots of proofs are

- MATH 332 – Elementary Linear Algebra
- MATH 400 – Real Analysis
- MATH 420 – Geometry
- MATH 430/431 – Applied Algebra I/II
- MATH 453 – Combinatorics
- MATH 454 – Graph Theory

References I

- Aigner, Martin, Günter M. Ziegler, and Karl H. Hofmann.
  Proofs from THE BOOK (4th Ed.).
  Springer, 2009.
- Devlin, Keith J.
  Set, Functions and Logic (3rd Ed.).
  Chapman & Hall/CRC, 2004.
- Euclid.
  Elements.
  ca. 300 B.C.
- Gowers, Timothy.
  Mathematics: A Very Short Introduction.
  Oxford University Press, 2002.
- Hardy, G. H.
  A Mathematician's Apology.
  Cambridge University Press, 1940.

References II

Hirsch, D. and D. Van Haften.
The Elements of a Proposition.
Savas Beatie, 2010. http://www.thestructureofreason.com/

Hayes, Brian.
Gauss's Day of Reckoning.
American Scientist 94 (2006), 200–205. http://bit-player.org/bph-publications/AmSci-2006-05-Hayes-Gauss.pdf

Alcuin of York.
Propositiones ad Acuendos Juvenes (Problems to Sharpen the Young). http://en.wikipedia.org/wiki/Propositiones_ad_acuendos_juvenes