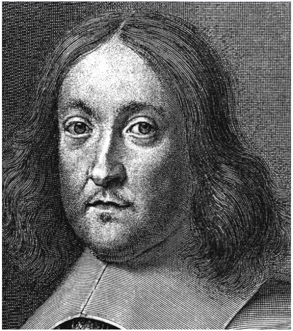
1. Proof Techniques

Terence Sim

The essential quality of a proof is to compel belief.



Pierre de Fermat,
1601 — 1665

Reading

Sections 2.1 — 2.7 of Campbell
Sections 4.1 — 4.3, 4.7 of Epp

1.1.1. Notation

We begin our study of proofs by recalling the following notations:

$\mathbb{R}$: the set of all real numbers
$\mathbb{Z}$: the set of all integers
$\mathbb{Q}$: the set of all rational numbers

Examples of real numbers: -1, π, 17, $\sqrt{2}$
Examples of integers: -3263, 0, $\sqrt{9}$, 2^{32}
Examples of rationals: $\frac{-21}{10}$, $\frac{1}{2}$, 5, $9.9\bar{9}$

And, as is well-known, all integers are rationals, and all rationals are reals.

Additional notations:

$\exists$: There exists ...
$\exists!$: There exists a unique ...
$\forall$: For all ...
$\in$: Member of (a set) ...
$\ni$: such that

Examples:

$$\exists x \in \mathbb{Z} \ni x^2 = 4$$

There exists an integer x such that $x^2 = 4$.

$$\forall y \in \mathbb{R},\ \exists! z \in \mathbb{R} \ni\ y + z = 0$$

For all real numbers y, there is a unique real z such that $y + z = 0$.

or

Every real number y has exactly one real z such that $y + z = 0$.

We will also assume, without proof, the usual properties of numbers. For example:

- *Closure:* integers are closed under addition and multiplication, i.e. $\forall x, y \in \mathbb{Z}, \quad x + y \in \mathbb{Z}$ and $xy \in \mathbb{Z}$.

  For all real numbers a, b and c,
- *Commutativity:* $a + b = b + a$ and $ab = ba$
- *Distributivity:* $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$
- *Trichotomy:* exactly one of the following is true: $a < b$, or $b < a$, or $a = b$

See Appendix A of Epp's textbook for all the properties.

1.1.2. Number Theory

Let's learn some Number Theory.

Definition 1.1.1 (Colorful)

An integer n is said to be colorful if there exists some integer k such that $n = 3k$.

This terminology colorful is non-standard; used only in this class.

Questions:

- Is 1353 colorful?
- What about $(208 - 201)$?
- 0?

Answer

- Yes, 1353 is colorful because $1353 = 3 \times 451$.
- No, because $208 - 201 = 7$, and there is no integer k such that $7 = 3k$. (See Example 7: Proposition 1.6.2)
- Yes, 0 is colorful because $0 = 3 \times 0$.

1.2. Proof by Construction

Existence Proof 1

Prove the following:

$$\exists x \in \mathbb{Z} \ni x > 2 \text{ and } x^2 - 5x + 6 > 0.$$

That is, there exists an integer x such that $x > 2$ and $x^2 - 5x + 6 > 0$.

Proof:

1. Note that $1000 \in \mathbb{Z}$ and $1000 > 2$.
2. Also, $1000^2 - 5(1000) + 6 = 995006 > 0$.

QED[1]

- A proof is a concise, polished argument explaining the validity of a statement to a skeptic (usually, you).
  - Concise means there are no irrelevant details. It also means to use few words.
  - Polished means it should be the final draft, i.e. you need to revise it to make it understandable, like writing an essay.
  - Argument means every step should follow logically from all previous steps.

[1] *quot erat demonstrandum* — that which was to be demonstrated.

- A proof is not an attempt to determine whether or not something is true. That is your scratch work. You should be convinced the statement is true *before* you write your proof.
- In the proof above, there is no need to explain how 1000 was obtained. You just need to show that 1000 has the said properties. Of course, many integers satisfy the same properties (as you can easily verify), and any one of these will suffice for the proof.
- This style of proof — where you explicitly find the value with the correct properties — is called a proof by construction. It is the most direct way to prove that something exists.
- Sometimes, finding the right thing takes some cleverness, as the next example shows.

Existence Proof 2

Prove that there exist irrational numbers p and q such p^q is rational.

Recall that a number x is rational if it can be written as a ratio of two integers: $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$.

A number that is not rational is irrational.

Proof:

1. We know from Theorem 4.7.1 (Epp) that $\sqrt{2}$ is irrational.
2. Consider ${\sqrt{2}}^{\sqrt{2}}$: it is either rational or irrational.
3. Case 1: It is rational.
   - 3.1 Let $p = q = \sqrt{2}$, and we are done.
4. Case 2: It is irrational.
   - 4.1 Then let $p = {\sqrt{2}}^{\sqrt{2}}$, and $q = \sqrt{2}$.
   - 4.2 p is irrational (by assumption), so is q (by Theorem 4.7.1 (Epp))
   - 4.3 Consider $p^q = ({\sqrt{2}}^{\sqrt{2}})^{\sqrt{2}}$
   - 4.4 $= (\sqrt{2})^{\sqrt{2}\times\sqrt{2}}$, by the power law
   - 4.5 $= (\sqrt{2})^2 = 2$, by algebra
   - 4.6 Clearly 2 is rational.
5. In either case, we have found the required p and q. ■

1.2.3. Disproof

- To disprove a statement, you are arguing why the statement is *not* true.
- You may use the same type of argument as in a proof. But sometimes, it is easier just to show a counterexample.

Example

Disprove this statement:

$$\forall x, y \in \mathbb{Z}^+, \sqrt{x+y} = \sqrt{x} + \sqrt{y}.$$

In other words, for all positive integers x and y, $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$.

$\mathbb{Z}^+$ denotes the set of nonnegative integers, i.e. $\{1, 2, 3, \ldots\}$.

Disproof

1. Let $x = y = 2$. Clearly, they are nonnegative integers.
2. Then $\sqrt{x+y} = \sqrt{2+2} = 2$,
3. But, $\sqrt{x} + \sqrt{y} = 2\sqrt{2} = 2.828427...$
4. Thus $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$, and the statement is false.

Disproof by counterexample is particularly useful for statements involving $\forall$.

Quiz: you try

If the following statement is true, prove it, otherwise give a counterexample:

The square of an irrational number is irrational.

1.2.4. Jigsaw Analogy

- Doing a proof is like solving a jigsaw puzzle[2]. No two jigsaws are alike; no two proofs are alike.
- Sometimes you solve large chunks quickly; other times you get stuck. You don't have to solve from top to bottom.
- Some strategies are useful eg. fixing the border of the puzzle first. Likewise, there are useful strategies for proofs.

[2] Adapted from D. Velleman, *How to Prove It, 2nd Edition*, 2006.

1.3. *if-then* statements

Many statements to be proven take the form:

if P then Q

One strategy is to use a direct proof: assume P is true, then combine this with other known facts F and theorems T to conclude that Q must be true.

Think of P as the starting point, and Q the destination. The other known facts F and theorems T make up the route that go from P to Q. Each step of the route must be logically connected.

In your draft, you can work forwards from P, or backwards from Q, but be careful never to assume Q to be true.

In your final, polished proof, you must argue only forwards, not backwards.

Example

Prove that:

if x, y are colorful integers, then so is $x + 2y$.

Identify P and Q to be:

P : x, y are colorful integers

Q : $x + 2y$ is colorful

We can immediately write down the start and end of the proof, as follows:

Draft proof:

1. Assume that x, y are colorful integers.
2. ...
3. And thus $x + 2y$ is colorful. QED.

The next logical thing is to use the definition of colorful.

Draft proof:

1. Assume that x, y are colorful integers.
2. Then by definition of colorful, $\exists a, b \in \mathbb{Z}$ such that $x = 3a$ and $y = 3b$.
3. $\dots$
4. So $\exists c \in \mathbb{Z}$ such that $x + 2y = 3c$.
5. And thus $x + 2y$ is colorful, by definition of colorful. QED.

This means we need to connect c to a and b. Obviously, we should try writing $(x + 2y)$ in terms of a, b:

$$\begin{aligned} x + 2y &= 3a + 2(3b), \text{ by substitution} \\ &= 3a + (2 \cdot 3)b, \text{ by associativity} \\ &= 3a + (3 \cdot 2)b, \text{ by commutativity} \\ &= 3a + 3(2b), \text{ by associativity} \\ &= 3(a + 2b), \text{ by distributivity} \end{aligned}$$

Aha! It is clear what c should be now. So here's our final proof:

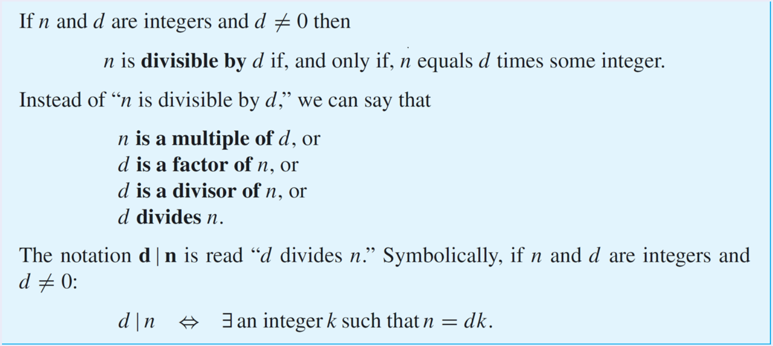
Proof.

1. Assume that x, y are colorful integers.
2. Then by definition of colorful, $\exists a, b \in \mathbb{Z}$ such that $x = 3a$ and $y = 3b$.
3. Now, $x + 2y = 3a + 2(3b)$, by substitution
4. $= 3a + 3(2b)$, by commutativity and associativity
5. $= 3(a + 2b)$, by distributivity
6. Let $c = a + 2b$. Note that $a + 2b \in \mathbb{Z}$ because integers are closed under addition and multiplication.
7. So $\exists c \in \mathbb{Z}$ such that $x + 2y = 3c$.
8. And thus $x + 2y$ is colorful, by definition of colorful.■

Note that *every* step is justified by appealing to definitions or to known properties of integers.

1.3.2. Divisibility

Definition 1.3.1 (Divisibility)



If n and d are integers and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of “n is divisible by d,” we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read “d divides n.” Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

e.g. Clearly $3 \mid 6$ (3 divides 6), but $4 \nmid 11$ (4 does not divide 11).

More examples

- For integers a, b, c, it is clear that if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$. Reason: if a is a factor of b and c, then it is a factor of the sum.
  Trivial example: $2 \mid 6$ and $2 \mid 8$. Also, $2 \mid (6 + 8)$.
- But the inverse is not true. That is, if $a \nmid b$ and $a \nmid c$, then it is still possible to have $a \mid (b + c)$.
  Trivial example: $3 \nmid 10$ and $3 \nmid 14$, but $3 \mid (10 + 14)$.
- Finally, it should be obvious that $a \mid ab$, for any b.

Warning!

Do NOT use division. There is no concept of division in Number Theory. The notation $a \mid b$ simply means a is a factor of b. No actual division is performed.

Theorem 4.3.1 (Epp)

$$\forall a, b \in \mathbb{Z}^+, \text{ if } a \mid b \text{ then } a \leq b.$$

That is, when dealing with positive integers, a divisor of a number cannot be larger than the number.

Note that the theorem is silent for the case $b = 0$, because 0 is not positive.

When doing proofs, it is often helpful to keep track of what we are given and what our goals are. Since the statement to be proven is an if-then statement, we can quickly write the P as our givens and the Q as our goal.

Givens	Goals
$a, b \in \mathbb{Z}^+$	$a \leq b$
$a \mid b$	

From the definition of $a \mid b$, we know that $b = ak$ for some integer k. We may add this to our givens.

Givens	Goals
$a, b \in \mathbb{Z}^+$	$a \leq b$
$a \mid b$	
$b = ak$, for some $k \in \mathbb{Z}$	

- So we now have one equality in our givens, but our goal involves an inequality. How do we achieve this?
- Intuitively, the equality says that if a needs to be multiplied by something to get b, then b must be larger than a. But this requires k to be positive. Fortunately, rule T25 of Appendix A (Epp) assures this.

- So what we want is to argue that since $ak = b$ and k is positive, we may "drop" k to get $a \leq b$. Although this is intuitively true, none of the rules in Appendix A (Epp) justifies this argument. We need another approach.
- Since k is a positive integer, we have the inequality $1 \leq k$ for "free", which we can add to our givens. We can now invoke rule T20 to multiply both sides of this inequality by a (which is positive), to get $a \leq ak$. The right hand side is now b, which is our goal. Hence our proof:

Proof.

1. Assume $a, b \in \mathbb{Z}^+$, and $a \mid b$.
2. So by definition of divisibility, $b = ak$ for some $k \in \mathbb{Z}$.
3. Since $a, b > 0$, and $b = ak$, we deduce k is positive by rule T25 of Appendix A (Epp).
4. Thus $1 \leq k$.
5. Using rule T20, multiply the inequality by a to get $a \leq ak = b$ ■.

Consider the statement:

$$\forall a, b, c \in \mathbb{Z}, \text{ if } a \mid b \text{ and } a \mid c, \text{ then } \forall x, y \in \mathbb{Z}, a \mid (bx + cy)$$

That is, if a divides both b and c, then it also divides $(bx + cy)$, for any integers x, y.

The following is an attempted disproof of the statement. Let's play detective and determine if it is right or wrong.

Proposed Disproof

1. Let $a = 12, b = 4, c = 3$.
2. We know that $12 \mid 4$ and $12 \mid 3$.
3. Let $x = 1, y = 5$. Then $bx + cy = 4 \cdot 1 + 3 \cdot 5 = 19$.
4. Clearly, $12 \nmid 19$.
5. Therefore, $\exists x, y \in \mathbb{Z}$ such that $a \nmid (bx + cy)$.
6. Therefore, the statement is not true.

Now consider this proposed proof. Is it right or wrong?

Proposed Proof

1. Assume $a \mid b$ and $a \mid c$ for integers a, b, c.
2. So $am = b$ and $an = c$, for some m, n.
3. Then $bx + cy = amx + any = a(mx + ny)$.
4. Therefore, $a \mid (bx + cy)$. QED

Consider yet another proposed proof. Is it right or wrong?

Proposed Proof

1. Suppose $a \mid b$ and $a \mid c$.
2. Then $ax = b$ and $ay = c$ for any integers x and y.
3. Then $bx + cy = (ax)x + (ay)y = a(xx + yy)$.
4. Since x and y are any integers and the integers are closed under addition and multiplication, we know that $(xx + yy) \in \mathbb{Z}$.
5. Thus $a \mid (bx + cy)$. QED.

1.4. *for-all* statements

$$\forall x \; P(x)$$

The strategy for proving such statements is to prove from the particular to the general. That is, take x to be a particular, but arbitrarily chosen, value. Prove that $P(x)$ is true. Conclude that since $P(x)$ is true for this particular x (which has no other special properties), it must be true for all x.

An analogy: suppose you are asked to prove the statement "All CS students take CS1231". You pick Tom, a typical CS student. Now you show that Tom is taking (or has taken) CS1231. You then argue that, since Tom is representative of CS students, what is true about him must be true of all other CS students. And thus the statement is true.

Theorem 4.3.3 (Epp) Transitivity of Divisibility

$$\forall a, b, c \in \mathbb{Z}\ , \text{ if } a \mid b \ \text{ and } \ b \mid c \ \text{ then } \ a \mid c.$$

Proof.

1. Take any three integers a, b, c.
2. Assume that $a \mid b$ and $b \mid c$.
3. Then by definition of divisibility, we know that $b = ar$ and $c = bs$, for some $r, s \in \mathbb{Z}$
4. Thus, $c = (ar)s = a(rs)$, by basic algebra
5. Now, rs is an integer, by closure of integers
6. $\therefore \quad a \mid c$, by definition of divisibility
7. Since a, b, c was chosen arbitrarily, the statement is true for all integers. ■

Remarks:

- We will usually omit Line 7, since it is understood.
- For Line 1, if instead we had said: Take positive integers a, b, c, then the proof would still be valid until Line 6. But in Line 7, we would not be able to generalize to *all* integers, because our proof thus far was valid only for positive integers.
- Likewise, we cannot assume $a \leq b$ or $b \leq c$ or $a \leq c$, since this is an unnecessary restriction.
- Another common mistake is to say, in Line 3: $b = ar$ and $c = br$. This forces b and c to be the same multiple, which again restricts our proof.

1.5. Proof by Contraposition

The contrapositive of the statement:

$$\text{if } P \text{ then } Q$$

is the statement:

$$\text{if } \sim Q \text{ then } \sim P$$

Note that $\sim P$ means not P, the negation of P. If P is True, then $\sim P$ is False, and vice versa.

Both statements are logically equivalent; that is, they are True and False for exactly the same truth values of P and Q.

Thus, instead of proving an if-then statement directly, we may prove it indirectly by proving its contrapositive.

Prove the following by Contraposition:

if x^2 is irrational then x is irrational

Proof.

Contrapositive form: if x is rational then x^2 is rational

1. Assume x is rational.
2. Then by definition of rationals, there exist integers a, b such that $b \neq 0$ and $x = a/b$.
3. So $x^2 = (a \cdot a)/(b \cdot b)$, by basic algebra
4. Both numerator and denominator are integers, by the closure property of integers.
5. Moreover, by rule T21 of Appendix A (Epp), $b^2 \neq 0$.
6. Thus, x^2 is a ratio of two integers.
7. Thus, by definition of rationals, x^2 is rational. ■

Remarks:

- To prove the statement directly, you would have to start by assuming x^2 is irrational. That is, $x^2 \neq a/b$ for *all* integer a and nonzero integer b.

  The unequality $\neq$ makes it difficult to continue. What form can you let x^2 take? Irrationality is defined by the *absence*, rather than the presence, of a form. If you cannot write down a form for x^2, then you cannot manipulate it to get a form for x. The proof cannot proceed.
- By using the contrapositive, you instead deal with rationals, rather than irrationals. You can thus exploit the form of rationals in your proof.
- Thus, whenever you encounter an if-then statement involving the absence of a form, you should consider proving by contraposition instead.

1.6. Proof by Contradiction

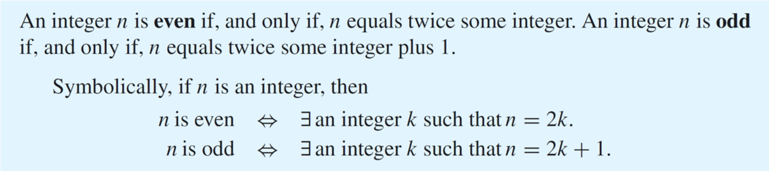
Reductio ad absurdum is one of a mathematician's finest weapons.

G.H. Hardy, 1877 — 1947

Remarks:

- To prove a statement S by contradiction, you first assume that $\sim S$ is true. Based on this, you use known facts and theorems to arrive at a contradiction. Since every step of your argument thus far is logically correct, the problem must lie in your assumption. Thus, you conclude that $\sim S$ is false, and hence S is true.
- A formal definition of contradiction will be given in the chapter on logic; for now, it suffices to say that a contradiction is something that is logically impossible. For example, at the start of your proof, you may assume (or deduce) that $x \geq 5$. Then later you deduce that $x < 5$. These two facts are clearly contradictory.
- In a proof by contradiction, the contradictory facts need not be directly related to S. As long as you contradict any known thing in mathematics, eg. $1 = 0$, your proof has succeeded.

Definition 1.6.1 (Even and Odd)



An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$\begin{aligned} n \text{ is even} \quad &\Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k. \\ n \text{ is odd} \quad &\Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k + 1. \end{aligned}$$

Examples:

$$328 \text{ is even because } 328 = 2 \times 164$$

$$91 \text{ is odd because } 91 = 2 \times 45 + 1$$

Theorem 4.7.1 (Epp) Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational

As with Example 5, it is difficult to use a direct proof because irrationality is the absence of a form.

On the other hand, proving by contradiction begins by assuming that $\sqrt{2}$ is rational, thereby allowing us to exploit the form of a rational number. The resulting proof is a mathematical classic.

Proof by contradiction

1. Assume that $\sqrt{2}$ is rational.
2. Then by definition of rationals, there exists integers m, n, with $n \neq 0$, such that $\sqrt{2} = m/n$.
3. Further, we may assume that m/n is reduced to lowest terms, ie. the only common factor of m, n is 1.
4. From Line 2, $m^2 = 2n^2$, by basic algebra.
5. So m^2 is even, by definition of even, and because n^2 is an integer by the closure property.
6. $\Rightarrow$ m is even, by Proposition 4.6.4 (Epp)
7. $\Rightarrow$ $\exists k \in \mathbb{Z} \ni m = 2k$, by definition of even.
8. Subtituting into Line 4: $(2k)^2 = 2n^2$.
9. $\Rightarrow$ $2k^2 = n^2$, by basic algebra.

…

proof cont'd

10. So n^2 is even, by definition of even, and because k^2 is an integer by the closure property.

11. $\Rightarrow$ n is even by Proposition 4.6.4 (Epp).

12. But this means 2 is a common factor of m, n, contradicting Line 3.

13. Hence $\sqrt{2}$ must be irrational. ■

Proposition 1.6.2

7 is not colorful.

Proof.

[Proof by contradiction]

1. Suppose 7 is colorful.
2. Then, by definition of colorful, $7 = 3k$ for some integer k.
3. $\Rightarrow \quad 6 = 3k - 1$, by basic algebra.
4. $\Rightarrow \quad 1 = 3(k - 2)$, by basic algebra.
5. Since $k - 2$ is an integer by the closure property, the above means that $3 \mid 1$, by definition of divisibility.
6. Then by Theorem 4.3.1 (Epp), this means $3 \leq 1$.
7. Clearly, this is absurd, so the Proposition is true. ■

Remarks:

- It is wrong to say: "7 is not colorful because $7/3 = 2.333...$, which is not an integer." There is no concept of division in Number Theory. Moreover, the definition of colorful does not use division, but instead uses the existence of an integer.
- It is also wrong to say: "I cannot find an integer k such $7 = 3k$, therefore 7 is not colorful." If you cannot find it, it doesn't mean no such integer exists.
- The irrefutable way to prove the non-existence of something is to show that if it exists, then it will lead to an absurd conclusion. This is the essence of a proof by contradiction.

Summary

- Proofs are at the heart of mathematics.
- Proving a statement is like solving a jigsaw puzzle. No two proofs are alike. Some strategies are useful.
- These lecture notes illustrate strategies for dealing with: existence proofs, if-then and for-all statements, disproof by counterexample, proof by contraposition and contradiction.
- For a given proof, which strategy to use will come with experience. For longer proofs, multiple strategies may be combined.
- Read Section 4.1 (pages 154 — 158) of the textbook for how to correctly write a proof, and the common mistakes to avoid. Use indentation to facilitate reading.
- Two more proof techniques — Induction and Diagonalization — will be covered in future lectures.