BU CAS CS 131. Writing Proofs.

Leonid Reyzin

Contents

1 Simple Examples of Different Proof Techniques

1.1 Direct Proofs Based on Algebra

We will take basic rules about manipulating equations and inequalities in algebra for granted (it is possible to prove those from even more basic axioms, but we will not be doing so in this class).

We have already seen direct proofs for logical equivalences, written as a series of equations with reasons for each transformation (such as DeMorgan's law or commutativity). For example, the proof that an implication is equivalent to its contrapositive goes like this.

Theorem 1. $P \to Q \equiv \neg Q \to \neg P$.

Proof.

$$\begin{aligned} P \to Q &\equiv \neg P \vee Q && \text{conditional identity} \\ &\equiv Q \vee \neg P && \text{commutativity} \\ &\equiv \neg(\neg Q) \vee \neg P && \text{double negation} \\ &\equiv \neg Q \to \neg P && \text{conditional identity} \end{aligned}$$

□

Note that we used the □ symbol to end the proof. We could also have written "which is what we needed to prove," or its Latin equivalent *quod erat demonstrandum*, commonly written as just QED, or some other similar text. Letting your reader know that the proof is over helps the reader.

Similar direct proofs are, of course, possible in algebra, with a slightly different set of laws. For example:

Theorem 2. $(a-b)(a+b) = a^2 - b^2$.

Proof.

$$\begin{aligned} (a-b)(a+b) &= a(a+b) - b(a+b) && \text{distributivity} \\ &= a^2 + ab - ba - b^2 && \text{distributivity} \\ &= a^2 + ab - ab - b^2 && \text{commutativity} \\ &= a^2 + 0 - b^2 && \text{opposites} \\ &= a^2 - b^2 && \text{add 0} \end{aligned}$$

□

We will now show a theorem whose proof is also by application of a series of algebraic laws, but doesn't fit neatly into a sequence of algebraic manipulations of a single equation; instead, we manipulate a few inequalities.

Theorem 3. *If* $a, b \in \mathbb{R}^+$, *and* $a < b$, *then* $a^2 < b^2$.

To make the proof readable, we will use full sentences to explain what we are doing.

Proof. Multiplying both sides of $a < b$ by a (which preserves the inequality because $a > 0$) gives us $a^2 < ab$. Similarly, multiplying both sides of $a < b$ by b gives us $ab < b^2$. By transitivity, $a^2 < b^2$. □

1.2 Proofs of Existence

It is often easy to prove an $\exists$ statement by simply showing the object that the statement claims exists. Here's an example that says Pythagorean triples exist.

Theorem 4. $\exists a, b, c \in \mathbb{Z}^+ : a^2 + b^2 = c^2$.

Proof. Let $a = 3$, $b = 4$, $c = 5$. Then

$$\begin{aligned} a^2 + b^2 &= 3^2 + 4^2 \\ &= 9 + 16 \\ &= 25 \\ &= 5^2 \\ &= c^2. \end{aligned}$$

□

The above proof format may be too much for such a simple statement; we could have also written simply "observe that $a^2 + b^2 = c^2$ because $3^2 + 4^2 = 5^2$."

In fact, proving that something exists by simply finding it and verifying that it works can also be used for more complicated statements, like $\forall\exists$. Here's an example from geometry of lines (or, if you prefer, from linear algebra).

Theorem 5. $\forall y \in \mathbb{R}\exists x \in R : 2x + 3 = y$.

Proof. Let $x = \frac{y-3}{2}$. Then $2x + 3 = 2\frac{y-3}{2} + 3 = y - 3 + 3 = y$. Note also that $x \in \mathbb{R}$ because $\mathbb{R}$ is closed under subtraction and division by nonzero values. □

On the other hand, proofs that something does not exist tend to be harder, because $\neg\exists$ is $\forall$. For example, if we change exponent 2 to any higher exponent in Theorem 4, then such a, b, c do not exist; since there are infinitely many possibilities for a, b, and c, we can't simply demonstrate that none of them work. The theorem stating that they do not exist is rather famous; it is known as Fermat's Last Theorem. It was proposed by Pierre de Fermat around year 1637, but not proven until 1994, with the final proof due to Andrew Wiles.

Theorem 6. *The domain of discourse is positive integers.* $\forall n > 2\ \neg\exists a, b, c : a^n + b^n = c^n$.

The proof of this theorem is too long to fit into these notes.

Not all existence proofs are easy, of course. Here's an example known as Goldbach's conjecture (proposed by Christian Goldbach in a letter to Leonhard Euler in 1742):

Conjecture 1. *Let* $\mathbb{P}$ *denote the set of prime numbers.* $\forall n \in \mathbb{N} : n$ *is even* $\rightarrow \exists p, q \in \mathbb{P} : p + q = n$.

In other words, the conjecture states that for every even integer, there exist primes that add up to it. This conjecture remains unproven to this day.

1.3 Counterexamples

Notice that $\neg\forall$ is the same is $\exists$, and so $\neg\forall$ proofs can be quite simple. For example, in 1769, Leonhard Euler stated the following conjecture about positive integers: sum of three fourth powers is never a fourth power (as a sort of generalization of Fermat's Last Theorem). That is $\forall a, b, c, d \in \mathbb{Z}^+ : a^4 + b^4 + c^4 \neq d^4$. Over 200 years later, in 1987, Noam Elkies disproved Euler's conjecture.

Theorem 7. *Euler's conjecture is false. That is,* $\neg\forall a, b, c, d \in \mathbb{Z}^+ : a^4 + b^4 + c^4 \neq d^4$.

Proof. By DeMorgan's law, this statement is equivalent to $\exists a, b, c, d \in \mathbb{Z}^+ : a^4 + b^4 + c^4 = d^4$. Thus, it suffices to simply show such a, b, c, and d. Indeed, setting $a = 2682440$, $b = 15365639$, $c = 18796760$, and $d = 20615673$, we can verify that the equation is satisfied. □

This proof illustrates two important points. First, to disprove a $\forall$, it suffices to give an example. Such an example is often called a "counterexample." Second, it is much easier to verify a proof than to come up with it. This proof tells you nothing about how these numbers were found, and, in fact, it took over 200 years and some very sophisticated math to find them.

1.4 Proofs that Go from Existence to Existence

Definition 1. $n \in \mathbb{Z}$ is even if and only if $\exists k \in \mathbb{Z}$ s.t. $2k = n$.

(Definitions are typically "if and only if" but people are sloppy with language and often write just "if" in a definition because it is understood to mean "if and only if." We will also do so when it's clear from the context.)

Theorem 8. *If n is even then n^2 is even.*

To do this proof, we will need to unwrap the definition of even. We need to prove that something exists (namely, an integer that, when doubled, gives n^2). But we are also given that something exists (namely, an integer that, when doubled, gives n). So we can use what we are given to prove the existence of the thing we need.

Proof. Since n is even, $\exists k \in \mathbb{Z}$ such that $2k = n$. Therefore, $(2k)^2 = n^2$, i.e., $2 \cdot (2k^2) = n^2$. Set $\ell = 2k^2$. Note that $\ell \in \mathbb{Z}$ (because $k \in \mathbb{Z}$, so $k^2 \in \mathbb{Z}$, so $2k^2 \in \mathbb{Z}$, because $\mathbb{Z}$ is closed under multiplication). And $2\ell = n^2$. Thus, $\exists \ell \in \mathbb{Z}$ s.t. $2\ell = n^2$, so n^2 is even by definition. □

Note the change in the variable name inside the definition: we used ℓ instead of k, because k ended up already taken. In fact, we didn't have to give $2k^2$ a name at all; we could have just written "note that $2k^2$ is an integer because integers are closed under multiplication, and $2 \cdot (2k^2) = n^2$, so n^2 is even by definition." But giving something a name often helps us reason about it.

Let us do another existence proof.

Definition 2. $x \in \mathbb{R}$ is rational (also written as $x \in \mathbb{Q}$) if $\exists n, d \in \mathbb{Z} : d \neq 0 \wedge x = \frac{n}{d}$.

Theorem 9. *If x_1 and x_2 are rational, then $x_1 + x_2$ is rational.*

This theorem can be equivalently stated as $\forall x_1, x_2 \in \mathbb{Q} : x_1 + x_2 \in \mathbb{Q}$. It can also be equivalently stated as "$\mathbb{Q}$ is closed under addition."

This proof is similar to the previous one: we will unwrap the definition of "rational" and go from there.

Proof. Let n_1, n_2, d_1, d_2 be such that $x_1 = \frac{n_1}{d_1}$, $x_2 = \frac{n_2}{d_2}$, $d_1 \neq 0$, and $d_2 \neq 0$ (we know they exist because x_1 and x_2 are rational). Then

$$x_1 + x_2 = \frac{n_1}{d_1} + \frac{n_2}{d_2} = \frac{n_1 d_2}{d_1 d_2} + \frac{n_2 d_1}{d_1 d_2} = \frac{n_1 d_2 + n_2 d_1}{d_1 d_2}.$$

Let $n_3 = n_1 d_2 + n_2 d_1$ and $d_3 = d_1 d_2$. Because $\mathbb{Z}$ is closed under multiplication and addition, $n_3 \in \mathbb{Z}$ and $d_3 \in \mathbb{Z}$. Moreover, $d_3 \neq 0$ because it is a product of two nonzero numbers. Since $x_1 + x_2 = \frac{n_3}{d_3}$, it is rational by definition. □

1.5 Proofs by Contrapositive

As we mentioned above, nonexistence is often more difficult to prove that existence. A proof by contrapositive is a useful technique for proving nonexistence by turning it into an existence proof. Here is an example.

Definition 3. $n \in \mathbb{Z}$ is odd if it is not even.

Note that this definition differs from definitions you may have seen elsewhere; we will reconcile this difference later, in Theorem 21

Theorem 10. *If $3n$ is odd then n is odd.*

To prove this theorem, we need to prove that $\neg\exists k : 2k = n$. That seems difficult to do directly. Instead, we will remember the contrapositive rule, which says $P \leftarrow Q \equiv \neg Q \leftarrow \neg P$ (Theorem 1). Here $P =$"$3n$ is odd" and $Q =$"n is odd".

Proof. Suppose not. Then n is even, so $\exists k : 2k = n$. Multiplying both sides by 3, we get $2 \cdot 3k = 3n$. Since $3k \in \mathbb{Z}$ (because integers are closed under multiplication), $3n$ is even by definition. Thus, the statement is true by contrapositive. □

Here is another example.

Definition 4. $x \in \mathbb{R}$ is irrational if it is not rational.

Theorem 11. *If x is irrational then $x/3$ is irrational.*

Proof. We will prove this statement by contrapositive. Suppose $x/3$ is rational. Then $\exists n, d \in \mathbb{Z} : d \neq 0 \wedge \frac{n}{d} = \frac{x}{3}$. Therefore, $\frac{3n}{d} = x$. Note that $3n \in \mathbb{Z}$ because integers are closed under multiplication, and thus x is rational by definition. □

1.6 Proofs by Cases

Theorem 12. *If x or y is even, then $x(y + 2)$ is even.*

Proof. Consider two cases (which together cover all possibilities of our hypothesis).

Case 1: x is even. Then $\exists k \in \mathbb{Z} : 2k = x$, and thus $2 \cdot k(y + 2) = x(y + 2)$. Note that $k(y + 2)$ is an integer because $\mathbb{Z}$ is closed under multiplication and addition, so $x(y + 2)$ is even by definition.

Case 2: y is even. Then $\exists k \in \mathbb{Z} : 2k = y$. Then $2(k + 1) = 2k + 2 = y + 2$, and therefore $2 \cdot x(k + 1) = x(y + 2)$. Note that $x(k + 1)$ is an integer because $\mathbb{Z}$ is closed under multiplication and addition, so $x(y + 2)$ is even by definition. □

Theorem 13. *If $|x| > 10$ then $x^2 > 100$.*

Proof. Case 1: $x \geq 0$. Then $|x| = x$, so $x > 10$. Note that $x \in \mathbb{R}^+$ because $x > 10$ and $10 > 0$, so $x > 0$ by transitivity. And $10 \in \mathbb{R}^+$. Thus, by Theorem 3, $x^2 > 100$.

Case 2: $x < 0$. Then $|x| = -x$, so $-x > 10$. By the same argument as above, replacing x with $-x$, we get $(-x)^2 > 100$. Since $(-x)^2 = (-1 \cdot x)^2 = (-1)^2x^2 = x^2$, we have $x^2 > 100$. □

Note that the cases are carefully arranged to cover all real numbers. If our proof used $x > 0$ rather than $x \geq 0$ in Case 1, it would not be complete, because it wouldn't address $x = 0$ case (which could be added as Case 3, but in this proof it's easier to just include it into Case 1). Sometimes it is not obvious how to cover all possibilities with the cases; sometimes it requires a separate portion of the proof to demonstrate that the cases actually cover everything.

Here's an example of combining two proof techniques: by contrapositive and by cases.

Theorem 14. *If xy is odd then x and y are odd.*

Note that we did not bother to specify the domain of discourse here: "even" and "odd" are terms that apply to integers, so it's clear to from the context that we are talking about integers (just like when you are talking "scientists" it's clear that you are talking about humans).

Proof. We will prove this theorem by contrapositive. Suppose not. Then either x or y is even.

Case 1: x is even. Then $\exists k \in \mathbb{Z} : 2k = x$, and thus $2 \cdot ky = xy$. Note that ky is an integer because $\mathbb{Z}$ is closed under multiplication, so xy is even.

Case 2: y is even. Then xy is even by the same proof as Case 1, swapping x and y. □

1.7 Proof by Contradiction

We have seen how proofs on nonexistence can sometimes be done by contrapositive. We will now turn to a more powerful and more general proof technique.

Theorem 15. $\neg\exists x : x < 0 \wedge x > 3$.

Proof. Suppose not. That is, suppose some x satisfies $x < 0$ and $x > 3$. Then $3 < x$ and $x < 0$, so, by transitivity, $3 < 0$. This is false, and thus x cannot exist. □

Let's analyze what happened here. We want to prove a statement Q. Instead, we proved $\neg Q \to F$ (where F stands for "False"). But that's equivalent to Q by the following derivation:

$$\begin{aligned} \neg Q \to F &\equiv \neg\neg Q \vee F && \text{conditional identity} \\ &\equiv Q \vee F && \text{double negation} \\ &\equiv Q && \text{identity} \end{aligned}$$

So by showing that the negation of our statement implies something False, we showed that our statement must be True.

Let's do one more simple example.

Theorem 16. *If x is rational and y is irrational, then $y - x$ is irrational.*

Proof. Suppose not; that is, suppose $y - x$ is rational. Let $z = y - x$. Then $y = z + x$ and, by Theorem 9, y is rational, because x and z are rational. But we are given that y is irrational. $\to\leftarrow$. □

The last symbol in this proof (two colliding arrows) is a shorthand for "we have reached a contradiction" — in other words, we have derived a false statement. How did we derive a false

statement? By simultaneously showing some statement S (in this case $S =$"y is rational") and $\neg S$ (in this case $\neg S =$"y is irrational"); we know by laws of propositional logic that $S \wedge \neg S = F$.

Like in the previous theorem, let's analyze what just happened. We wanted to prove that some statement R (in this case, $R =$"x is rational and y is irrational") implies some statement Q (in this case, $Q =$"$y - x$ is irrational"). Instead of doing this proof directly, we assumed $\neg Q$, and showed that $R \wedge \neg Q \to F$ (here F stands for "False").

What does that mean? It means we have proven $R \to Q$, which was exactly our goal, by the following derivation:

$$\begin{aligned}
(R \wedge \neg Q) \to F &\equiv \neg(R \wedge \neg Q) \vee F && \text{conditional identity} \\
&\equiv \neg R \vee \neg\neg Q \vee F && \text{DeMorgan's} \\
&\equiv \neg R \vee Q \vee F && \text{double negation} \\
&\equiv \neg R \vee Q && \text{identity} \\
&\equiv R \to Q && \text{conditional identity}
\end{aligned}$$

1.8 Stating and Proving Uniqueness

We will prove the following example statement, which is fundamental to linear algebra: the equation $ax + b = 0$, for any real values $a \neq 0$ and b, has a unique solution x in the real numbers. (Recall that real numbers are denoted by $\mathbb{R}$.)

Theorem 17. $\forall a, b \in R : a \neq 0 \to \exists! x \in \mathbb{R} : ax + b = 0$.

Recall that $\exists!$ means "there exists exactly one." Note that moving $a \neq 0$ to the right would be incorrect: $\forall a, b \in R : \exists! x \in \mathbb{R} : a \neq 0 \to ax + b = 0$ is false, because when $a = 0$, the statement $a \neq 0 \to ax + b = 0$ is trivially true (because false implies anything), so there is more than one value of x that works when $a = 0$, but $\exists!$ means that there is only one x. Note also that using $\wedge$ instead of $\to$ would be incorrect: anything that starts with $\forall a, b \in \mathbb{R} : a \neq 0 \wedge \ldots$ is false, because $\forall$ is simply a giant "and" that combines all possible values of a, and one of those values of a is 0, so $a \neq 0$ would be false for it, making the entire $\forall$ false.

Proof. First we will prove existence. Set $x = -b/a$ (this is allowed because division exists in the real numbers as long as the denominator is not 0, and $a \neq 0$). Plugging in, we have $a \cdot (-b/a) + b = 0b + b = 0$, as required.

Now we will prove uniqueness. Typically, uniqueness is easiest to prove by assuming there are two objects and either directly proving that they are equal or assuming they are not equal and deriving a contradiction. Here we will use the first method. So, suppose the are two values x_1 and x_2 satisfying $ax_1 + b = 0$ and $ax_2 + b = 0$. Then $ax_1 + b = ax_2 + b$ so, subtracting b, we have $ax_1 = ax_2$, and dividing by a (which is nonzero by assumption, so division is allowed), we get $x_1 = x_2$. □

2 Proofs about Division

2.1 The Well-Ordering Principle

Consider the set $S = \{x \in \mathbb{R} : 1 < x < 2\}$. This is the set of all real numbers between 1 and 2, exclusive.

Theorem 18. *The set S has neither a maximum nor a minimum.*

Proof. Indeed, if m is the minimum of S, then $m \in S$, so $1 < m < 2$. Let $m' = (1+m)/2$. $m' < m$, because $1 < m$, so $1 + m < 2m$, so $(1 + m)/2 < m$. But also $m' \in S$, because $1 < m'$ (since $1 < m$, so $2 < 1 + m$, so $1 < (1 + m)/2$) and $m' < 2$ because $m' < m$ and $m < 2$. So $m' \in S$ is smaller than m, which contradicts the assumption that m is the minimum of S. Similarly for the maximum. □

Fortunately, the situation is not the same for integers. A nonempty subset of integers that is bounded from above always has a maximum, and a nonempty subset of integers that is bounded from below always has a minimum. This is often expressed as the *well-ordering principle*, which is written as follows.

Axiom 1. Every nonempty subset of natural numbers contains a smallest element. That is, if $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then $\exists m \in S \, \forall n \in S : m \leq n$.

Note that this is an axiom — we take it for granted as the defining feature of natural numbers. (The first natural number—namely, 0—is $\min \mathbb{N}$; each next natural number can be obtained by removing the minimum from the set so far, and finding the minimum of what's left.)

2.2 Odds and Evens

Definition 5. An integer n is *even* if $\exists k \in \mathbb{Z} : n = 2k$ (equivalently $2 \mid n$).

Definition 6. An integer $n \in \mathbb{Z}$ is *odd* if it is not even.

This last definition is inconvenient to work with. It tells us what an odd integer is not, but not what it is. We'd like to know that odd integers are ones of the form $2\ell + 1$ for some $\ell \in \mathbb{Z}$. To get us there, the following theorem will help. It says that every integer is either of the form $2k$ or of the form $2\ell + 1$.

Theorem 19. $\forall n \in \mathbb{Z} : (\exists k \in \mathbb{Z} : n = 2k) \vee (\exists \ell \in \mathbb{Z} : n = 2\ell + 1)$.

Note: this theorem is not claiming that it cannot be both. That is, for now, we are not trying to prove an exclusive-or, even though it is actually exclusive-or. Eventually we will prove exclusive-or, and once we prove it, then we'll know that every odd integer is of the form $2\ell + 1$ for some ℓ.

The challenge of this proof is that we have very little to work with. All we have is the starting integer (let's call it n). We know nothing about it. We need to find either k such that $n = 2k$ or ℓ such that $n = 2\ell + 1$. But, unlike many previous proofs, where we could construct our k from k_1 and k_2 or something similar, we have nothing to work with here.

Here's the main idea. Assume, for a moment, that n is nonnegative. Subtract 2 repeatedly from n until you no longer can subtract without going negative. The number of times you subtract 2 will be your k or ℓ. (If n is negative, add 2 instead of subtracting, as many times as is needed to make it nonnegative.)

Proof of Theorem 19. Let n be an integer. Consider the set S of all nonnegative integers that can be obtained by computing $n-2t$ for some integer t. (In set notation, $S = \{s \in \mathbb{N} : \exists t \in \mathbb{Z} \text{ s.t. } x = n-2t\}$).

Claim 1. *S is nonempty.*

Proof. We will do a proof by cases. In the case n is nonnegative, we know $n \in S$ by setting $t = 0$. In the case n is negative, set $t = n$; then $n - 2t = n - 2n = -n$, which is positive, so $-n \in S$. □

Let r (for "remainder") be the smallest element in S (we know it exists by the well-ordering principle, i.e., Axiom 1).

Claim 2. *$r < 2$.*

The proof of this claim is very similar to the proof of Theorem 18.

Proof. Suppose, for purposes of contradiction, that $r \geq 2$. We know $r = n - 2t$ for some t, by definition of S. Then let $t' = t + 1$. Consider $n - 2t'$. On the one hand, $n - 2t' = n - 2(t+1) = n - 2t - 2 \geq 2 - 2 = 0$, so $n - 2t' \in S$. But on the other hand, $n - 2t' = n - 2t - 2 = r - 2 < r$, so r is not the minimum of S. This is a contradiction. □

Thus, $r \geq 0$ and $r < 2$. This leaves two cases. In the first case, $r = 0$; in this case let $k = t$. Then $n - 2k = 0$, so $n = 2k$. In the second case, $r = 1$. Let $\ell = t$. Then $n - 2\ell = 1$, so $n = 2\ell + 1$. □

2.3 The Division Theorem

Imagine replacing 2 with 3 in Theorem 19. We would then have three clauses instead of two: $\forall n \in \mathbb{Z} : (\exists k \in Z : n = 3k) \vee (\exists \ell \in \mathbb{Z} : n = 3\ell + 1) \vee (\exists m \in Z : n = 3m + 2)$. More generally, if we replaced 2 with d, we'd have d clauses instead. Naturally, writing d clauses is cumbersome. Since these clauses are all connected by an "or", we can simply write a theorem stating that there exists a remainder r that makes one of clauses true. This theorem is known as the *division theorem* or *division algorithm* (the latter is a misnomer, because no algorithm is specified).

Theorem 20. *Let n be an integer and d a positive integer. There are unique integers q and r such that $n = qd + r$ and $0 \leq r < d$.*

The proof of existence is similar to the proof of Theorem 19. Like the the proof of Theorem 19, it is constructive: it constructs the remainder as the minimum of the set $S = \{s \in \mathbb{N} : \exists t \in \mathbb{Z} \text{ s.t. } s = n - td\}$ (for example, if $n = 131$ and $d = 20$, then S contains $131, 111, 91, 71, 51, 31, 11$, as well as $151, 171, 191, 211, \ldots$).

The proof of uniqueness is not very difficult. We will not present either of the proofs here (we may have them in the textbook and/or the homework).

By taking $d = 2$, we can improve on Theorem 19.

Theorem 21. $\forall n \in \mathbb{Z} : (\exists k \in Z : n = 2k) \oplus (\exists \ell \in \mathbb{Z} : n = 2\ell + 1)$.

Proof. We know at least one of the two clauses is true by Theorem 19. It remains to prove that both cannot be true at the same time. Suppose, for contradiction, that both were true. Then $n = 2k + 0$ and $n = 2\ell + 1$. We thus have two different results for division with remainder of n by 2, which contradicts the uniqueness statement of Theorem 20. □

Definition 7. We will say $d \mid n$ (pronounced "d divides n", which is equivalent to "n is divisible by d") if $\exists q \in \mathbb{Z} : n = dq$).

Note that the above defines a two-input predicate: d and n are inputs to $d \mid n$, and the output is either true or false.

Definition 8. Let $\texttt{divisors}(n)$ be the set of all d such that $d \mid n$ (in set notation, $\texttt{divisors}(n) = \{d : d \mid n\}$).

2.4 A Simple Fact about Divisibility

Theorem 22. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proving theorems often starts with unwrapping the definitions. This proof is a simple example of that.

Proof. Because $a \mid b$, we know $\exists k_1 \in \mathbb{Z}$ such that $ak_1 = b$.

Because $b \mid c$, we know $\exists k_2 \in \mathbb{Z}$ such that $bk_2 = c$.

Set $k_3 = k_1 k_2$. Note that $k_3 \in \mathbb{Z}$ and $ak_3 = a(k_1 k_2) = (ak_1)k_2 = bk_2 = c$, and thus $a \mid c$ by definition of $\mid$. □

3 The Pythagoreans, Euclid, and the Greatest Common Divisor

The Pythagoreans were a religious sect in ancient Greece who lived about 2500 years ago. One of the problems they studied was the problem of measuring line segments: if you have two line segments a and b, how can you compare them? Since fractions weren't well developed yet, integer measurements were much easier. So if you found some other line segment c that goes an integer number of times into a (say, n times — that is, $a = cn$) and some other integer number of times into b (say, d times — that is, $b = cd$), then you could compare a to b: $a/b = n/d$. In other words, you could just measure a and b using c, by putting the length c back to back to until you got a or b. In fact, you could do all this purely geometrically by looking at lines and never measuring them numerically or even fixing a unit of measurement.

But how do you find c? They came up with a brilliant algorithm, known today as "Euclid's" algorithm (Euclid, who lived a couple of hundred years later, wrote down a lot of the geometry invented by the Pythagoreans and their successors in his book The Elements).

3.1 Euclid's Algorithm

Suppose a is longer than b. Then take out b from a as many times as you can, until you have some remainder. This remainder will be shorter than b. Replace a with the remainder. Now b is the longer segment, and the remainder is shorter segment. Swap their roles and repeat. Keep doing this until you have no remainder left. The last value you had before the remainder is that common length c.

We can write this idea down using our modern day algebraic notation. In fact, we'll do it in Python.

```
def Euclid(x, y):
    while y>0:
        r = x % y    # Note that x%y in Python means "remainder of x when divided by y"
        x = y
        y = r
    return x
```

3.2 Analyzing Euclid's Algorithm

We can shorten Euclid's algorithm in Python as follows:

```
def Euclid(x, y):
    while y>0:
        x, y = y, x%y
    return x
```

This version does exactly the same as the one before, simply skipping the temporary variable r and computing two assignments at once.

As we said last time, if the starting values a and b are lengths, then `Euclid(a,b)` computes another length g that goes into both x and y an integral number of times (i.e., $g \mid a$ and $g \mid b$). In fact, it computes the largest such g. In other words, a/g and b/g are as small as possible, and thus you are working with small numbers when talking about how a relates to b (for example, $a = 5g$ and $b = 7g$ instead of $a = 10g$ and $b = 14g$).

This statement requires a proof. In fact, before we even show that this algorithm computes something, let's ask why it computes anything at all — in other words, why does it even stop?

Claim 3. *`Euclid(a,b)` stops for any inputs a, b that are positive integers, and when it stops, $y = 0$.*

To prove this fact, we need to recall the well-ordering principle from above (Axiom 1).

Proof. Let S be the set of all values that the variable y takes during the run of `Euclid(a,b)`. $S \neq \emptyset$ because $b \in S$. Every value in S is nonnegative, because every value in S (besides b, which is positive) is a remainder, and remainders, by definition, are nonnegative.

Since S is a nonempty subset of nonnegative integers, S contains its own minimum, by the well-ordering principle (Axiom 1). Let this minimum be m. Suppose, for purposes of contradiction, $m > 0$. Then, when $y = m$, the loop is entered (because $y > 0$) and y becomes a remainder after division by m, so y becomes less than m by definition of remainder, and thus m is not the minimum of S. Therefore, $m = 0$. So at some point y becomes 0 and the program stops. □

Now that we know it stops, let's prove that it outputs the correct value. Recall that `divisors`(a) contains all the numbers that divide a, `divisors`(b) contains all the numbers that divide b, and their intersection `divisors`$(a) \cap$ `divisors`(b) contains all the numbers that divide both a and b.

Definition 9. Let a and b be integers. Define "the greatest common divisor (GCD)" (also known as "the greatest common factor") of a and b (written $\gcd(a, b)$) as the maximum value in the set `divisors`$(a) \cap$ `divisors`(b).

Theorem 23. *For positive integers a and b, `Euclid(a, b)` outputs* $\gcd(a, b)$.

Proof. To prove this theorem, we start with the following claim.

Claim 4. *For any positive* (x, y), $\gcd(x, y) = \gcd(y, x \bmod y)$.

We will leave this claim as an exercise to the reader. It requires proving that

$$\texttt{divisors}(x) \cap \texttt{divisors}(y) = \texttt{divisors}(y) \cap \texttt{divisors}(x \bmod y)\,.$$

Since the sets are the same, their maximum values are also the same.

This claim says that even though the numbers x and y change at every iteration of the loop, their GCD doesn't. Let g be the very last value of x — that is, the value that is returned by the algorithm. We know from Claim 3 that the very last value of y is 0. Since the GCD doesn't change, $\gcd(a, b) = \gcd(g, 0)$. But $\gcd(g, 0) = g$ for any $g > 0$, because 0 is divisible by everything, and g is divisible by nothing greater than g. So $\gcd(a, b) = g$, which is the value returned by the algorithm. □

The amazing feature of Euclid's algorithm is that to compute the greatest common divisor of a and b, we do not need to factor a and b into their constituent primes. That is, in fact, a necessary condition for a successful algorithm, because finding prime factorization for large numbers remains an unsolved problem to this day. (Our inability to factor large numbers into primes underlies some common techniques in modern cryptography; if someone were able to factor large numbers into primes, the security of many websites and even some cryptocurrency protocols would be broken.)

Euclid's algorithm (actually, its more complex version called "extended Euclid's algorithm," which, in addition to $g = \gcd(a, b)$, computes c and d such that $ac + bd = g$) is used in a variety of applications, including cryptography and error-correcting codes, and is likely invoked by your computer hundreds of times a day.

4 Rationals, Irrationals, Euclid's Algorithm, and (Maybe) a Tragic Death

We will now study one of the first known interesting proofs by contradiction.

Euclid's algorithm can be applied to numbers that aren't integers, because division with remainder makes sense not only for integers: for any numbers x and y, we can write $x = qy + r$ for some integer q and remainder r such that $0 \le r < y$. Only q here must be an integer. For example, $5.7 = 2 \cdot 2.6 + 0.5$ — here, 0.5 is a remainder. If $r = 0$, we say $x \,|\, y$. For example, $1.5 \,|\, 4.5$. We can also define the greatest common divisor: for example, 6.5 and 2.6 have the greatest common divisor of 1.3. This means that if you have a line segment a of 6.5cm in length and another line segment b of 2.6cm in length, you can measure them both using the line segment g of 1.3cm in length: there are 5 gs in a and 2 gs in b.

(If you run this algorithm on a computer, you have to be careful because decimals are usually approximated, rather than precisely represented, inside a computer, and rounding errors may mess things up. There are techniques for dealing with this: basically, rescale things so that everything is an integer, by multiplying everything by the common denominator. In the example above, use millimeters instead of centimeters.)

What Pythagoreans really wanted to know is whether every pair of line segments will have a common length that divides them both. They called such line segments "commensurable." In other words, can we, for every picture with lines segments in it, find a length that can be used to measure

all the line segments only integer measurements. In the example two paragraphs above, 1.3 was that length, and the measurements were 5 and 2. Why integer measurements only? Because those are much easier to carry out by placing equal-length rods back-to-back. They seem much more intuitive, especially in a culture that doesn't do fractions much and hasn't invented decimals yet.

Another way to put this question is whether, no matter what two inputs a and b you pick, Euclid's algorithm stops. We proved that's the case for integers, but what about for real numbers?

Unfortunately, the answer is no. Some real numbers cannot be measured with a common length, i.e., are "incommensurable." In fact, it doesn't take much to build such awful numbers (today they are called "irrationals"). Take a square with side length 1. It's diagonal has length $\sqrt{2}$ (by the Pythagorean theorem, which was, of course, known to the Pythagoreans). There is no length that divides both 1 and $\sqrt{2}$. We now prove this fact.

Theorem 24. *There is no real number c such that $c \mid 1$ and $c \mid \sqrt{2}$.*

Proof. Suppose there is such a number. By definition of division, there are integers n and d such that $cd = 1$ and $cn = \sqrt{2}$. The first equation implies $c = 1/d$; plugging this in to the second equation we get $n/d = \sqrt{2}$. (In other words, the two equations imply that $\sqrt{2}$ is rational, by definition of rational.)

The informal idea of the proof is the following: since $n/d = \sqrt{2}$, we have $n^2/d^2 = 2$. Let's look at the power of 2 in the prime factorization of the values in this equation. The factorization of n^2 contains an even power of 2 because it is a square; the factorization of d^2 contains an even power of 2 because it is a square; even minus even is even, so n^2/d^2 contains an even power of 2. But on the right-hand side we have just 2, which is 2^1, which is an odd power of 2. That's a contradiction.

The above approach is totally fine if we first prove that every integer has a unique factorization into primes, which is a big complicated proof we don't want to do now. Instead, we'll do something similar, but without the unique factorization theorem.

First, we will reduce the fraction n/d to its lowest terms to get $m/e = n/d$, where m and e have no common factors — they satisfy $\gcd(m, e) = 1$. This can always be done by simply setting $m = n/g$ and $e = d/g$; you will prove that this works on the homework.

We thus have

$$m/e = \sqrt{2}\,. \tag{1}$$

Multiplying both sides of Equation (1) by e, we get $m = e\sqrt{2}$. Squaring both sides we get $m^2 = 2e^2$, so m^2 is even.

Claim 5. *If x is an integer and x^2 is even, then x is even.*

Proof. Suppose x is not even. Then x is of the form $2\ell + 1$ by Theorem 21. Thus $x = 2\ell + 1$ for some ℓ, and $x^2 = 4\ell^2 + 4\ell + 1 = 2(2\ell^2 + 2\ell) + 1 = 2j + 1$ for $j = 2\ell^2 + 2\ell$. Then x^2 is not even by Theorem 21. We have thus proven the result by contrapositive. □

Since m^2 is even, by Claim 5, m is even. So $m = 2k$ for some integer k, so $4k^2 = 2e^2$, so $2k^2 = e^2$, so e^2 is even, so e is even (by Claim 5). Thus, $\gcd(m, e) \geq 2$, which contradicts the fact that $\gcd(m, e) = 1$. The concludes the proof of Theorem 24. □

This result is one of the earliest known examples of an interesting proof by contradiction, dating back about 2500 years. According to legend, this proof was discovered by Hippasus. It greatly upset the Pythagoreans, because it showed that there is no length that could be used to measure both

the side of a square and its diagonal. In fact, the legend says that they were so upset with him for revealing such an ugly truth about the world (which they wanted to be numerically perfect) that they threw him off the boat into the Mediterranean sea to drown. The legend is likely not true, but makes a good story about martyrdom for mathematical truth.

So if you run Euclid's algorithm in its pure form, with exact representation of real numbers (which computers can't do) on inputs $\sqrt{2}$ and 1, it will go on forever, getting smaller and smaller values, but never reaching 0.

Corollary 1. *$\sqrt{2}$ is irrational.*

Proof. Suppose, for purposes of contradiction, $\sqrt{2} = n/d$ for integers n and d with $d \neq 0$. Then letting $c = 1/d$, we get $c \mid 1$ (because $dc = 1$ and $d \in \mathbb{Z}$) and $c \mid \sqrt{2}$ (because $cn = \sqrt{2}$ and $n \in \mathbb{Z}$). That contradicts Theorem 24. □

We have thus shown that irrational numbers exist. This fact of great importance to computer science. Integers are easy to represent as finite sequences of bits (simply write them in binary notation). Rational numbers are easy to represent as pairs of integers (numerator and denominator). But irrational numbers do not have such a convenient representation. Since computers have finite memory, representing irrational numbers precisely becomes a challenge.

5 Infinitely Many Primes

We will now cover a second example of an early nontrivial contradiction proof. It also appears in Euclid's Elements 2300 years ago.

Recall that a prime number is an integer greater than 1 that has exactly two positive integer divisors (1 and itself).

Theorem 25. *There are infinitely many primes.*

Proof. We will use the following fact:

Claim 6. *Every integer greater than 1 is divisible by a prime.*

Proving this claim is an exercise to the reader.

Now, suppose for purposes of contradiction, that there are only finitely many primes. Multiply them all together to get some integer N. Take any prime p. Let q be the product of all primes other than p. Then $N = pq$ and so $N + 1 = pq + 1$. Since $0 < 1 < p$ (because p is a prime), 1 is the remainder after $N + 1$ is divided by p, by definition of remainder. We thus know that $N + 1$ is not divisible by p (because if it were divisible by p, the remainder would be 0, by the remainder cannot be both 0 and 1, because division gives a unique remainder by the division theorem).

Thus, $N + 1$ is not divisible by any prime p, which contradicts Claim 6 □

This proof has a step that is not obvious at all: multiplying all the primes together. Discovering proofs is not an always an easy task; verifying them is much easier.