Week 2: Introduction to Proofs

Michael Zhou

2023-01-01

- How can we figure out whether a statement is True or False?
- If we do know that a statement is True, how can we convince others?
- How can we read someone else's proof?

1 Examples of proofs

Definition 2.1. A **mathematical proof** is how we communicate ideas about the truths of a statement to others.

The following examples will be divided into three or four parts:

1. The statement we are proving or disproving.
2. A translation of the statement into predicate logic, describes the logical structure we will be using.
3. A discussion to try to gain some intuition about why the statement is True. These are written informally, and often the hardest part about developing a proof.
4. The formal proof, the standalone final product of the earlier work.

Example 2.1. Prove that $15 \cdot 3^2 - 7 = 7 + (19 + 3)^2/4$.

Translation. Since this statement has no logical operators, the translation is simply itself.

Discussion. You can check if this is True by entering both sides into a calculator.

Proof. This statement is True because both sides equal 128.

Example 2.2. Prove that there exists a power of two bigger than 1000.

Translation. "There exists" translates to an existential quantifier, and "powers of 2" have the form 2^n, where n is a natural number.

$$\exists n \in \mathbb{N}, 2^n > 1000$$

Discussion. This must be True since you know that powers of 2 can grow to infinity, so you just need to do some calculations for a large value of n.

Proof. Let $n = 10$.
Then $2^{10} = 1024$, which is greater than 1000.[1]

Drawing from this example, in general, we only have to prove for one element in existentence proofs.

[1] This is easily checkable with a calculator, so no need for further verification.

Example 2.3. Prove that every real number n greater than 20 satisfies the inequality $1.5n - 4 \geq 3$.

Translation. “Every real number n” translates to a universal quantifier, and we can restrict n to be greater than 20 as a condition on the hypothesis.

$$\forall n \in \mathbb{R}, n > 20 \Rightarrow 1.5n - 4 \geq 3$$

Discussion. You could gain intuition by substituting numbers for n that are greater than 20, but that does not serve to prove *all* real numbers. Instead, you could perform some algebraic manipulation on the formula to preserve the inequality $n > 20$: multiplying by 1.5, and subtracting 4.

Proof. Let $n \in \mathbb{R}$ be an *arbitrary* real number. Assume that $n > 20$. We want to prove that $1.5n - 4 \geq 3$.[2]

$$\begin{aligned} n &> 20 \\ 1.5n &> 30 \\ 1.5n - 4 &> 26 \\ 1.5n - 4 &\geq 3 \end{aligned}$$

We can observe some standard patterns that these proofs always follow:

Existential	$\exists x \in S, P(x)$.	Let $x = a$, proof that $P(x)$ is True.
Universal	$\forall x \in S, P(x)$.	Let $x \in S$, proof that $P(x)$ is True.
Implication	Assume p	Proof that q is True.

2 What goes into a proof?

2.1 Proof header: setting up the proof

Definition 2.2. Every proof should start with a **proof header**. The main purpose of a proof header is to introduce all variables and assumptions used in the proof. Pay attention to ordering, as we have learned about alternating quantifiers.

Existential	“Let $x = 5$.”
Universal	“Let $x \in S$.” or “Let x be an arbitrary element of S.”
Local	“Let $\epsilon = x - x^2$.”

Example 2.4. $\forall x \in \mathbb{N}, P(x) \Rightarrow Q(x)$.

$$\boxed{\text{Let } x \in \mathbb{N}\text{. Assume } P(x)\text{.}}$$

Example 2.5. $\forall x \in \mathbb{N}, P_1(x) \wedge P_2(x) \wedge P_3(x)$.

$$\boxed{\text{Let } x \in \mathbb{N}\text{. Assume that } P_1(x), P_2(x)\text{, and } P_3(x) \text{ are all True.}}$$

Example 2.6. $P(x)$: ”$x^3 < 10x + 300$”, where $x \in \mathbb{N}$. Suppose we are proving a statement in the form of $\forall x \in \mathbb{N}, P(x) \Rightarrow Q(x)$.

$$\boxed{\text{Let } x \in \mathbb{N}\text{. Assume that } P(x) \text{ is True.}}$$

Example 2.7. $\forall x \in \mathbb{R}, \forall y \in \mathbb{N}, x > 10 \wedge y < z \Rightarrow \exists z \in \mathbb{R}, P(x, y, z)$. Let us write the proof header for this statement.

Proof. Let $x \in \mathbb{R}$ and let $y \in \mathbb{N}$. Assume that $x > 10$ and that $y < x$. Let $z =$ _____. We will prove that $P(x, y, z)$ is True. [3]

[*Proof body goes here.*]

[2] We could also just write “Let $n \in \mathbb{R}$” instead.

[3] Note that we picked apart the complex statement and focused on the core — the predicate $P(x, y, z)$.

2.2 Proof body: the chain of reasoning

Definition 2.3. The **proof body** contains the actual reasoning showing that a statement must be True.

Definition 2.4. Proof bodies consist of a seqeunce of True statements called **deductions**, where each statement logically followings from a combination of the following sources of truth:

- Definitions
- Assumptions (made in proof header)
- Previous deductions (made early in proof body)
- External true statements

The proof body is a *chain* in the sense that it uses statements already known to be True, then makes deductions until finally proving the statement — A proof is over when a deduction that is the statement being proven is written.

Example 2.8. A proof body is usually consisted of two parts, the deduction, and the reason for the deduction.

- "Since (reason), (deduction)."
- "Because we know (reason), we can conclude (deduction)."
- "It follows from (reason) that (deduction) is also True/holds."

2.3 Logical deductions

Definition 2.5. The most common form of logical deduction in proofs is **modus ponens**.[4] This rule says that if we know p and $p \Rightarrow q$ are both True, then we can conclude that q is also True. This matches the intuition of implication.

Example 2.9. Because we know $x > 10$ and that $x > 10$ implies $x^2 - x > 90$, we can conclude that $x^2 - x > 90$.

Definition 2.6. Another common form of logical deduction is **universal instantiation**. This rule says that if we already know a universal like $\forall x \in S, P(x)$, and a variable y whose value is an element in the domain S, then we can conclude that $P(y)$ must be True. This matches the intuition for universally-quantified statements.

Example 2.10. Because we know that $y \in \mathbb{N}$ and that $\forall x \in \mathbb{N}, x^2+5x+4$ is not prime, we can conclude that $y^2 + 5y + 4$ is not prime.

2.4 Writing reasons and deductions

You must provide explicit reasons for all statements in a proof.

However, there are two exceptions:

- Any deduction verifiable by a calculator, like $100 < 3 \cdot 4$.
- Any basic manipulation of an equality or inequality, like $x > 4$ to $2x > 8$.

For other types of reasonings — definitions, assumptions, prior deductions, and external facts — make references explicitly.

[4] Also known as implication elimination.

2.5 The direction of a proof

For a normal arithmetic calculation, we would want to simplify a complex statement into its simplest form. But for a proof, we want to start from the simple, known statement, and derive our target deduction from them.

We must always write our proofs in a **top-down** order to disambiguate statements. Think of it as reading an essay, but in the context of numbers.

3 A new domain: number theory

Mathematical domains can specify common definitions and properties that we can use freely in proofs. The first domain we will be exploring is number theory, and formalizing what we know about numbers. We will start off with the divisibility operator from the previous chapter.

Definition 2.7. Let $n, d \in \mathbb{Z}$. We say that d divides n, or n is divisible by d, if and only if there exists a $k \in \mathbb{Z}$ such that $n = dk$. We can use the notation $d \mid n$ to represent "d divides n," and call d a divisor of n, and n a multiple of d.

Example 2.11. Prove that $23 \mid 115$.

Translation. We can expand on the definition of divisibility to rewrite this statement:

$$\exists x \in \mathbb{Z}, 115 = 23x$$

Discussion. We can just divide 115 by 23.

Proof. Let $x = 5$. Then $115 = 23 \cdot x = 23 \cdot 5$.

Example 2.12. Prove that there exists and integer that divides 104.

Translation. "There exists" translates into an existential quantifier, and "an integer" translates into the set of integers. We can use the divisibility operator to represent "divides 104", and expand on that using the definition of the divisibility operator.[5]

$$\exists n \in \mathbb{Z}, n \mid 104$$

$$\exists a, n \in \mathbb{Z}, 104 = an$$

Discussion. We only need to find one example that satisfies this statement. Since 104 happens to be an even number, we know that it will be divisible by 2 at the very least.

Proof. Let $n = 2$ and let $a = 52$. Then $104 = an$.

4 Alternating quantifiers revisited

Recall from the previous chapter that we said changing the order of an existential and universal quantifier changed the meaning of a statement. Now, we will investigate this affects variable introductions in a proof.

[5] Since the variables share the same set, we can group them together.

Example 2.13. Prove that all integers are divisible by 1.

Translation. "All integers" translates into a universal quantifier, and proving that it is divisible by 1 uses an existential quantifier through the definition of divisibility.

$$\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = 1 \cdot k$$

Discussion. We can prove for $n = k$, but how do we introduce the variables? We must follow the same order they are quantified in the statement.

Proof. Let $n \in \mathbb{Z}$, and let $k = n$. Then $n = 1 \cdot n = 1 \cdot k$.

5 False statements and disproofs

Definition 2.8. A **disproof** is a proof that the negation of the statement is True. In other words, if $\neg X$ is True, then X must be False.

Example 2.14. Disprove "every natural number divides 360."

Translation. "Every natural number" translates to the set of natural numbers and a universal quantifier. We have to disprove this statement though, so we will use the converse.[6]

$$\neg(\forall n \in \mathbb{N}, n \mid 360)$$

$$\exists n \in \mathbb{N}, n \nmid 360$$

Discussion. We can find a natural number that does not divide 360.

Proof. Let $n = 7$. Then $n \nmid 360$, since $\frac{360}{7}$ is not an integer.

Example 2.15. Disprove "for all natural numbers a and b, there exists a natural number c which is less than $a+b$, and greater than both a and b, such that c is divisible by a or by b."

Translation. This is a fairly complex statement but we can break it down: "for all natural numbers" translates to a universally quantified variable in the set of natural numbers; "less than" and "greater than" translate to inequalities in the form of $a \geq b \geq c$; "is divisible by" translates to the divisibily operator.

$$\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N}, c < a + b \wedge c > a \wedge c > b \wedge (b \mid c \vee a \mid c)$$

We can derive the negation now:

$$\begin{aligned}&\neg(\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N}, c < a + b \wedge c > a \wedge c > b \wedge (b \mid c \vee a \mid c))\\&\exists a, b \in \mathbb{N}, \neg(\exists c \in \mathbb{N}, c < a + b \wedge c > a \wedge c > b \wedge (b \mid c \vee a \mid c))\\&\exists a, b \in \mathbb{N}, \forall c \in \mathbb{N}, \neg(c < a + b \wedge c > a \wedge c > b \wedge (b \mid c \vee a \mid c))\\&\exists a, b \in \mathbb{N}, \forall c \in \mathbb{N}, c \geq a + b \vee c \leq a \vee c \leq b \vee (\neg(a \mid c \vee b \mid c))\end{aligned}$$

$$\exists a, b \in \mathbb{N}, \forall c \in \mathbb{N}, c \geq a + b \vee c \leq a \vee c \leq b \vee a \nmid c \wedge b \nmid c))$$

Discussion. "There exists natural numbers a, b such that for every natural number c, $c \geq a + b$ or $c \leq a$ or $c \leq b$ or neither a or b divide c." We will pick values for a and b since there is an existential quantifier. It is helpful to pick small values so that we do not have to worry about the numbers in between.

[6] We will use the simplication rules for negation from the previous chapter to find the converse.

Proof. Let $a = 2$ and $b = 2$, and let $c \in \mathbb{N}$. We now need to prove that

$$c \geq a + b \lor c \leq a \lor c \leq b \lor (a \nmid c \land b \nmid c).$$

Substitute the values for a and b, and we have

$$c \geq 4 \lor c \leq 2 \lor 2 \nmid c.$$

To prove an OR, we only need one of the three parts to be True. But, which part is True depends on the value of c. For example, not all numbers c are greater or equal to 4. So we can split up the proof into three cases for different c values: numbers ≥ 4, numbers ≤ 2, and the single value 3.

Case 1. Assume $c \geq 4$, then the first part is True.

Case 2. Assume $c \leq 2$, then the second part is True.

Case 3. Assume $c = 3$, then the third part is True since $2 \nmid 3$.

Since all possible cases result in True, we can conclude that the statement is always True.

6 Proof by cases

The above proof illustrated a new technique.

Definition 2.9. A **proof by cases** divides a domain into different parts, and writes a separate argument for each part. Formally, we pick a set of unary predicates such that for every element x in the domain, x satisfies at least one of the predicates — thus, these predicates are *exhaustive*.[7]

In other words, a proof by cases combines simpler proofs to form a whole proof. We introduce the following theorem as a natural use of proof by cases in number theory.

Theorem 2.1. The **Quotient-Remainder Theorem** states that for all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exists $q, r \in \mathbb{Z}$ such that $n = qd + r$ and $0 \leq r < d$. Moreover, these q and r are *unique*.

Definition 2.10. Let n, d, q, r be the variables from the above theorem. We say that q and r are the **quotient** and **remainder**, respectively, when n is divided by d.

This theorem tells us that for any divisor $d \in \mathbb{Z}^+$, we can separate all possible integers into d different groups, corresponding to their possible remainders — between 0 and $d - 1$ — when divided by d.

Example 2.16. Prove that for all integers x, $2 \mid x^2 + 3x$.

Translation. Using the divisibility predicate or expanding it:

$$\forall x \in \mathbb{Z}, 2 \mid x^2 + 3x$$

$$\forall x \in \mathbb{Z}, \exists k \in \mathbb{Z}, x^2 + 3x = 2k$$

Discussion. We want to factor out a 2 from $x^2 + 3x$, but this only works if x is even. If x is odd, then both x^2 and $3x$ will be odd, therefore producing an even number. We can use the Quotient-Remainder Theorem to formalize this thought.

[7] Since a set and a predicate have an equivalence, we can also portray this as dividing the domain into subsets, and proving the statement for each subset.

Proof. Let $x \in \mathbb{Z}$. By the QRT, we know that when x is divided by 2, there will either be a remainder of 1 or 0. So, we can divide the proof into two cases.

Case 1. Assume the remainder of $x/2$ is 0. In other words, $\exists q \in \mathbb{Z}, x = 2q + 0$. Let $k = 2q^2 + 3q$, we will show that $x^2 + 3x = 2k$.

$$\begin{aligned} x^2 + 3x &= (2q)^2 + 3(2q) \\ &= 4q^2 + 6q \\ &= 2(2q^2 + 3q) \\ &= 2k \end{aligned}$$

Case 2. Assume the remainder of $x/2$ is 1. In other words, $\exists q \in \mathbb{Z}, x = 2q + 1$. Let $k = 4q^2 + 10q + 4$, we will show that $x^2 + 3x = 2k$.[8]

$$\begin{aligned} x^2 + 3x &= (2q+1)^2 + 3(2q+1) \\ &= 4q^2 + 4q + 1 + 6q + 3 \\ &= 4q^2 + 10q + 4 \\ &= 2(2q^2 + 5q + 2) \\ &= 2k \end{aligned}$$

7 Generalizing statements

We will investigat how to generalize existing knowledge into more generic and powerful forms. Let's give an example *without* generalization.

Example 2.17. Prove that for all integers x, if x divides $(x + 5)$, then x also divides 5.

Translation. There is a universal quantifier and an implication in this statement.

$$\forall x \in \mathbb{Z}, x \mid (x + 5) \Rightarrow x \mid 5$$

Discussion. You can assume x divides $x+5$, and prove that x also divides 5. Need to turn $x + 5 = k_1x$ into $5 = k_2x$. We can use the definition of divisibility. We will probably substitute k_1 into k_2x to prove $k_2x = 5$.

Proof. Let $x \in \mathbb{Z}$. Assume that $x \mid (x+5)$, such that $\exists k_1 \in \mathbb{Z}, x+5 = k_1x$. We want to prove that $\exists k_2 \in \mathbb{Z}, 5 = k_2x$. Let $k_2 = k_1 - 1$.[9]

$$\begin{aligned} k_2x &= (k_1 - 1)x \\ &= k_1x - x \\ &= (x + 5) - x \\ &= 5 \end{aligned}$$

What did we do in this proof?

1. To prove an implication, we assume the hypothesis to be True in order to prove the conclusion. We are *not* proving the hypothesis.
2. We used the definition of divisibility to include a variable $k_1 \in \mathbb{Z}$, and the same for k_2.
3. Finally, we proved that if a factor k_1 exists for x when it divides $(x + 5)$, another factor k_1 *also* exists for $x \mid 5$.

[8] As a reminder, we are using binomial expansion.

[9] Our intuition for choosing $k_2 = k_1 - 1$ is that we want to get rid of the x when we substitute $(x+5)$ for k_1x, leaving the singular 5 to prove our statement.

7.1 Generalizing our example

Example 2.18. The meta-technique **generalization** takes in a True statement with its proof, and replaces a concrete value in the statement with a universally quantified variable.

Consider the statement from the previous example, $\forall x \in \mathbb{Z}, x \mid (x+5) \Rightarrow x \mid 5$. It seems like the "5" does not serve any special purpose — we can probably replace it with another variable.

Rather than replacing 5 with another number, we can replace it with a universally quantified variable, and proving the corresponding statement. We will know that we can replace the "5" with *any* natural number and the statement will still hold.

Example 2.19. Prove that for all $d \in \mathbb{Z}$, and for all $x \in \mathbb{Z}$, if x divides $(x + d)$, then x also divides d.

Translation. The translation follows our previous example:

$$\forall d, x \in \mathbb{Z}, \Big((\exists k_1 \in \mathbb{Z}), x + d = k_1 x \Rightarrow (\exists k_2 \in \mathbb{Z}, d = k_2 x)\Big)$$

Discussion. We should be able to use the same sets of calculations.

Proof. Let $d, x \in \mathbb{N}$. Assume that $x \mid (x + d)$, there exists $k_1 \in \mathbb{Z}$, such that $x + d = k_1 x$. We want to prove that there exists $k_2 \in \mathbb{Z}$ such that $d = k_2 x$. Let $k_2 = k_1 - 1$.

$$\begin{aligned} k_2 x &= (k_1 - 1)x \\ &= k_1 - x \\ &= (x + d) - x \\ &= d \end{aligned}$$

Unlike the the previous proof, we **generalized** the proof so that it does not depend on the value of 5. By doing this, we have gone from one statement being True, to an infinite number of statements being True.

8 Characterizations

We will now present two related examples that both show how to prove a biconditional. We will also find alternative useful characterizations of definitions. In particular, we will show that prime numbers are exactly the numbers greater than 1 that satisfy the following predicate:

$$\mathit{Atomic}(n) : \forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab, \quad \text{where } n \in \mathbb{N}$$

Example 2.20. We will prove the following statement.[10]

$$\forall n \in \mathbb{N}, \Big(n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)\Big) \Rightarrow \mathit{Prime}(n)$$

It's not immediately clear how we should use the hypothesis to prove the conclusion. So, we can try writing the *contrapositive* of the statement.

$$\forall n \in \mathbb{N}, \neg \mathit{Prime}(n) \Rightarrow \Big(n \leq 1 \vee (\exists a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \wedge n \mid ab)$$

Now, we can assume that n is *not* prime, and we only need an existential proof or $n \leq 1$. We can prove the contrapositive as it will also be a proof for the original.

[10] Or said in English, "every number that is greater than one and atomic must also be prime."

Discussion. We are going to assume that n is not prime, and it's greater than 1. First, let's look at the definition of *Prime* and negate it.

$$Prime(n) : n > 1 \wedge (\forall d \in \mathbb{N}, d \mid n \Rightarrow d = 1 \vee d = n)$$

$$\neg Prime(n) : n \leq 1 \vee (\exists d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n)$$

So if we assume that $n > 1$, then we can also assume that there exists a number d that divides n that is not 1 or n.

Proof. Let $n \in \mathbb{N}$. Assume that n is not prime. Then by negating the definition of prime, either $n \leq 1$ or there exists $d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n$. We divide our proof into two cases based on the two parts.

Case 1. Assume $n \leq 1$. Then the first part is True.

Case 2. Assume $\exists d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n$.

Expanding on the divisibility predicate, this means that there exists $k \in \mathbb{N}$ such that $n = dk$. We will prove the second part of the OR, listed below. Let $a = d$ and $b = k$. We want to prove that $n \nmid a$, $n \nmid b$ and $n \nmid ab$.

$$\exists a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \wedge n \mid ab$$

We will substitute d and k into the statement:

$$\begin{aligned} n \nmid a \wedge n \nmid b \wedge n \nmid ab &= n \nmid d \wedge n \nmid k \wedge n \mid dk && (1) \\ &= dk \nmid d \wedge dk \nmid k \wedge dk \mid dk && (2) \end{aligned}$$

All cases of (2) are True:

1. $dk \nmid d$ is always True since $d \neq n$ and $n = dk$, meaning k cannot equal to 1.
2. $dk \nmid k$ is always True since $d \neq 1$.
3. $dk \mid dk$ is always True since a number dk is always a factor of itself.

What we just did was prove that if n is greater than 1, and satisfies the *Atomic* predicate, then it must be prime. But what about $n = 5$? It does not tell us whether 5 satisfies the property since a prime number would have a False hypothesis, leaving an unknown conclusion.[11] Next, we will prove the *converse* of the implication.

Example 2.21. Prove the following converse of example 2.20.[12]

$$\forall n \in \mathbb{N}, Prime(n) \Rightarrow \Big(n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)\Big)$$

Discussion. We can try an example to gain some intuition. Consider the prime $n = 7$ and arbitrary numbers a and b. When both a and b do not have 7 as a divisor, like $a = 12$ and $b = 10$, $a \cdot b = 120$ also does not have 7 as a divisor (satisfying $Atomic(n)$).

But how do we prove this? We could write out a prime factorization of a and b: $a \cdot b = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 5$. This clearly shows that 7 is not a divisor of $a \cdot b$.

The problem with this proof is that we would have to prove that every number has a unique prime factorization, which is quite unnecessary. Instead, we will use the following two facts that are easier to prove.[13]

[11] Recall the **vacuous truth** cases from the previous chapter for implication operators.

[12] Or said in English, " Every number that is prime must also be greater than one and atomic."

[13] These rely on properties of the *greatest common factor*, which will be discussed in the next section.

$$\forall n, m \in \mathbb{N}, Prime(n) \wedge n \nmid m \Rightarrow (\exists r, s \in \mathbb{Z}, rn + sm = 1) \qquad \text{(Claim 1)}$$
$$\forall n, m \in \mathbb{N}, Prime(n) \wedge (\exists r, s \in \mathbb{Z}, rn + sm = 1) \Rightarrow n \nmid m \qquad \text{(Claim 2)}$$

How might we setup a proof using these claims? Since we are assuming n to be prime, we can have two numbers a, b that are not divisible by n. Using Claim 1 twice, there exists r_1, s_1 (for a) and r_2, s_2 (for b) such that:

$$r_1 n + s_1 a = 1$$
$$r_2 n + s_2 b = 1$$

We want to conclude that ab is also not divisible by n, so we will use Claim 2, which says "to conclude that ab is not divisible by n, it suffices to find r, s such that $rn + s(ab) = 1$." We can then find r, s by multiplying the two equations together:

$$r_1 r_2 n^2 + r_2 s_1 an + r_2 s_2 bn + s_1 s_2 ab = 1$$

This can be rewritten as

$$(r_1 r_2 n + r_2 s_1 a + r_1 s_2 b)n + (s_1 s_2)(ab) = 1$$

Proof. Let $n \in \mathbb{N}$. Assume that n is prime. We need to prove that $n > 1$ and $Atomic(n)$ are True.

Case 1. $n > 1$. The definition of prime tells us that this is True.

Case 2. $Atomic(n)$ is True.

We want to prove that $(\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab$, where $n \in \mathbb{N})$. Let $a, b \in \mathbb{N}$, and assume that $n \nmid a$ and $n \nmid b$. We want to prove that $n \nmid ab$.[14]

We will first prove that there exists $r_3, s_3 \in \mathbb{N}, r_3 n + s_3 ab = 1$. By Claim 1 and the assumption that n is prime, there exists $r_1, s_1, r_2, s_2 \in \mathbb{Z}$ such that $r_1 n + s_1 a = 1$ and $r_2 n + s_2 b = 1$. Let $r_1 r_2 n + r_2 s_1 a + r_1 s_2 b = r_3$, and $s_1 s_2 = s_3$.

$$\begin{aligned} (r_1 n + s_1 a)(r_2 n + s_2 a) &= 1 \\ (r_1 r_2 n + r_2 s_1 a + r_1 s_2 b)n + (s_1 s_2)(ab) &= 1 \\ r_3 n + s_3 ab &= 1 \end{aligned}$$

By Claim 2, we have now proved the statement that $n \nmid ab$. In other words, we have proved both cases, thus concluding our proof.

8.1 A summary

We have proven both the following statements:[15]

$$\forall n \in \mathbb{N}, n > 1 \wedge Atomic(n) \Rightarrow Prime(n)$$
$$\forall n \in \mathbb{N}, Prime(n) \Rightarrow n > 1 \wedge Atomic(n)$$
$$\forall n \in \mathbb{N}, n > 1 \wedge Atomic(n) \Leftrightarrow Prime(n)$$

Thus, we have given a *characterization* or *alternate definition* of prime numbers. Equivalent characterizations are useful as they give a different way to look at the same concept.

[14] Just like all the other implication proofs, you should be used to this pattern by now.

[15] Recall how a biconditional operator, ⇔, is defined by implications from both directions being True.

9 Greatest common divisor

Definition 2.11. Let m, n be natural numbers which are not both 0. The **greatest common divisor (gcd)** of m and n, denoted $\gcd(m, n)$, is the highest natural number d such that d divides both m and n.

We define $\gcd(0, 0)$ to be 0 to make the domain of the gcd operator all pairs of natural numbers.

Let $m, n, k \in \mathbb{N}$, not all of which are 0, and suppose $k = \gcd(m, n)$.

$$k \mid m \wedge k \mid n \wedge (\forall e \in \mathbb{N}, e \mid m \wedge e \mid n \Rightarrow e \leq k)$$

Example 2.22. Prove that for all natural numbers p, q, if p and q are distinct primes, then $\gcd(p, q) = 1$.

Translation. We can translate the statement without unpacking definitions.[16]

$$\forall p, q \in \mathbb{N}, (Prime(p) \wedge Prime(q) \wedge p \neq q) \Rightarrow \gcd(p, q) = 1$$

Discussion. We know that primes only have two divisors, 1 and itself. We just need to make sure that neither p or q divides the other, since that would make the gcd larger than 1.

Proof. Let $p, q \in \mathbb{N}$. Assume that both p and q are prime, and that they are unique. We want to prove that $\gcd(p, q) = 1$.

By the definition of primality, p and q cannot be 1, and the only positive divisors of p and q are 1 and themselves. Since $p \neq q$ and $p \neq 1$, we know that $p \nmid q$.

Thus, $\gcd(p, q) = 1$ since the only positive divisors of p and q is 1.

Theorem 2.2. Let $a, b \in \mathbb{N}$, assume at least one of them is non-zero. Then $\gcd(a, b)$ is the smallest positive integer such that $\exists p, q \in \mathbb{Z}$ with $\gcd(a, b) = ap + bq$. In other words, the gcd is the smallest natural number that can be written as the sum of (positive or negative) multiple of the two numbers.

We will now use this theorem to introduce a new proof technique — **using an external statement** as a step in a proof. We do not need to know how the external theorem is implemented, only to know what it means.

Example 2.23. For all $a, b \in \mathbb{N}$, every integer that divides both a, b also divides $\gcd(a, b)$.

Translation. $\forall a, b \in \mathbb{N}, \forall d \in \mathbb{Z}, (d \mid a \wedge d \mid b) \Rightarrow d \mid \gcd(a, b)$

Discussion. All we know from gcd is that $d \leq \gcd(a, b)$, and that does not imply $d \mid \gcd(a, b)$. We can use the **GCD Characterization Theorem** to write $\gcd(a, b)$ as $ap + bq$.

Proof. Let $a, b \in \mathbb{N}$ and $d \in \mathbb{Z}$. Assume that $d \mid a$ and $d \mid b$. We want to prove that $d \mid \gcd(a, b)$.

By the GCD Characterization Theorem, $\exists p, q \in \mathbb{Z}$ such that $\gcd(a, b) = ap + bq$.[17] By divisibility of linear combinations, since $d \mid a$ and $d \mid b$, we know $d \mid ap + bq$. Since $\gcd(a, b) = ap + bq$, we can conclude that $d \mid \gcd(a, b)$.

[16] Unpacking definitions here would obscure the meaning of the statement and overcomplicating it — we will use the definitions in the proof, so it is meaningless to include it here.

[17] Using the external theorem

10 Modular arithmetic

When dealing with relationships between numbers, the divisibility predicate is often too constrained by the binary nature of its output. Instead, we often care more about the *remainder* when we divide a number by another.

Definition 2.12. Let $a, b, n \in \mathbb{Z}$, with $n \neq 0$. We say that a is **congruent to** b **modulo** n iff $n \mid a - b$. We can write $a \equiv b \pmod{n}$.[18]

In other words, a and b have the same remainder when divided by n.

$a = b$	Numeric values are literally equal.
$a \equiv b \pmod{n}$	Remainders when divided by n are equal.

We will now look at how addition, subtraction, and multiplication behave under modular arithmetic.

Example 2.24. Prove that for all $a, b, c, d, n \in \mathbb{Z}$, with $n \neq 0$, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$:

1. $a + b \equiv c + d \pmod{n}$
2. $a - b \equiv c - d \pmod{n}$
3. $ab \equiv cd \pmod{n}$

Translation. We will only show how to unpack (2), the rest are similar:

$$\forall a, b, c, d, n \in \mathbb{Z}, (n \neq 0 \land n \mid (a - c) \land n \mid (b - d)) \Rightarrow n \mid ((a - b) - (c - d))$$

Proof. Let $a, b, c, d, n \in \mathbb{Z}$. Assume $n \neq 0$ and $n \mid (a - c)$ and $n \mid (c - d)$. We want to prove that $n \mid ((a - c) - (b - d))$. By the divisibility of linear combinations, since $n \mid (a - c)$ and $n \mid (b - d)$, it will also divide their difference.

Example 2.25. Let $a, b, p \in \mathbb{Z}$. If p is a prime number and a is not divisible by p, then there exists $k \in \mathbb{Z}$ such that $ak \equiv b \pmod{p}$.

Translation. $\forall a, b, p, \in \mathbb{Z}, (Prime(p) \land p \nmid a) \Rightarrow (\exists k \in \mathbb{Z}, ak \equiv b \pmod{p})$

Discussion. We know we will have to use the definition of congruence like "there exists $k \in \mathbb{Z}$ such that ..." We will also use the GCD Characterization Theorem to write gcd as a sum of multiples. We can assume p is prime, $p \nmid a$, and gcd of two numbers can be written as the sum of multiples of the numbers.

We want to prove that:

- $\exists k \in \mathbb{Z}, ak \equiv 1 \pmod{p}$, which is equivalent to
- $\exists k \in \mathbb{Z}, p \mid (ak - 1)$ using the definition of mod. that is equal to
- $\exists k, d \in \mathbb{Z}, dp = ak - 1$
- $\exists k, d \in \mathbb{Z}, 1 = ak - dp$ which is a sum of multiples

Proof. Let $a, b, p \in \mathbb{N}$. Assume p is prime and p does not divide a. We want to prove that $ak \equiv b \pmod{p}$. We need to prove two subclaims in order to complete this proof.[19]

Claim 1. $\gcd(a, p) = 1$.

[18] The notation $a \equiv b$ is not entirely the same as the % operator used in programming: both a and b could be much larger than n, or even negative.

[19] We can think of these as **helper functions** in terms of progrmaming, to break up the proof in smaller steps.

Proof. By the defintion of prime, we know that the greatest divisor that is not itself is 1. Since we assumed that $p \nmid a$, we know that 1 is the only positve common divisor.

Claim 2. $\exists k \in \mathbb{Z}, ak \equiv 1 \pmod{p}$.

Proof. By the previous claim, we know $\gcd(a, p) = 1$. By Theorem 2.1 (QRT), we know that there exists $r, s \in \mathbb{Z}$ such that $ar + ps = 1$.

Let $k = r$, then we can rearrange

$$\begin{aligned} ak + ps &= 1 \\ ak - 1 &= p(-s) \\ p &\mid (ak - 1) \\ ak &\equiv 1 \pmod{p} \end{aligned}$$

Finally, we can combine these claims to prove there exists a $k' \in \mathbb{Z}$ such that $ak' = b \pmod{p}$.

Let $k' = kb$. Then we have

$$\begin{aligned} ak &\equiv 1 \pmod{p} \\ akb &\equiv b \pmod{p} \\ ak' &\equiv b \pmod{p} \end{aligned}$$

11 Proof by contradiction

Definition 2.13. A **proof of contradiction** states that given a statement P to prove, rather than proving it directly we assume that its **negation** $\neg P$ is True. We use this assumption to prove a statement Q and its negation $\neg Q$. We call Q and $\neg Q$ the **contradiction** that arises from the assumption that P is False.[20]

Theorem 2.3. There are infinitely many primes.

Proof. Assume that this statement is False. Let $k \in \mathbb{N}$ be the number of primes, and let $p_1, p_2, \ldots, p_k$ be the prime numbers.

Let $Q : \forall n \in \mathbb{N}, Prime(n) \Leftrightarrow (n \in p_1, p_2, \ldots p_k)$. Q is True because our asumption that there is a finite number of primes.

Now we will show that Q is False. Define the number

$$P = 1 + \prod_{i=1}^{k} p_i = 1 + p_1 \times p_2 \times \ldots \times p_k$$

There must be some prime p that divides P because $P > 1$. But $p \notin p_1, \ldots, p_k$ since otherwise p would divide $P - p_1 \times \ldots \times p_k = 1$, and no prime can divide 1. So p is a prime that is not one of $p_1 \times \ldots \times p_k$, so Q is False, thus there is a contradiction.

[20] In other words, “if P is False, then Q and its negation $\neg Q$ must be True.”