Notes on How to Prove It: A Structured Approach

Alejandro Cadarso Nieto

November 17, 2023

Contents

Chapter 1

Introduction

1.1 Prime Numbers

This is a book about deductive reasoning in mathematics and mathematical proofs. Fundamental theorems regarding prime numbers are introduced in this chapter to provide an idea of what to expect later in the book.

Definition 1.1.1: Prime Numbers

A natural number $n > 1$ is considered prime if and only if its only positive divisors are 1 and p.

As a first proof, let's test the conjecture that there are infinitely many prime numbers.

Theorem 1.1.1 Euclid's Second Second Theorem

There are infinitely many prime numbers.

Proof: If we assume that there is a finite list of prime numbers denoted as $p_1, p_2, \ldots, p_n$, we can create a number m as follows:

$$m = p_1 p_2 \ldots p_n + 1$$

Note that m is not divisible by any of the primes p_n. [1] We acknowledge the fact that every integer larger than 1 is either a prime or can be written as a product of two or more primes. If m is a prime, it can't be on the list because that would contradict the first assumption that all primes are on the list. Now, assume m is a product of primes. Take q as one of the primes in that product and an element on the list, so m is divisible by q. Then again, we reach a contradiction because m is not divisible by any p_n.

Since the assumption that there is a finite amount of prime numbers reached a contradiction, there must be an infinite amount of prime numbers. 😄

Theorem 1.1.2 Mersenne Composites

For every composite integer $n > 1$, $2^n - 1$ will also be composite. [a]

[a] The analogy is sometimes true for primes, these are called Mersenne primes.

Proof: If n is composite then it can be expressed as $n = ab$. Let $x = 2^b - 1$ and $y = 1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}$.

[1] This is because the remainder when dividing m by any of the primes p_n is 1, which means m is not divisible by them.

Then:

$$\begin{aligned} xy &= (2^b - 1) * (1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}) \\ &= 2^b * (1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \ldots + 2^{ab}) - (1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

😄

1.1.1 Exercises

Question 1

*1.
(a) Factor $2^n - 1 = 32,767$ into a product of two smaller positive integers.
(b) Find an integer x such that $1 < x < 2^{32,767} - 1$ and $2^{32,767} - 1$ is divisible by x.

Solution: **(a)** $n = log_2(32,767 + 1) = 15$, we know that if n is not prime then $2^n - 1$ is not prime, so 32,767 is a composite number. One possible solution is $4,681 * 7 = 32,767$.
Solution: **(b)** $2^{32,767} - 1$ is composite so there exist at least two x that can solve the problem. From 1.1, if n is not prime then $n = a * b$. Also $2^n - 1 = (2^b - 1) * (1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b})$. So one possibility is $x = 2^7 - 1$.

Question 2

2. Make some conjectures about the values of n for which $3^n - 1$ is prime or the values of n for which $3^n - 2^n$ is prime. (You might start by making a table similar to *Figure I.1*)

Solution:

n	$3^n - 1$
1	2
2	8
3	26
4	80
5	242
6	728
7	2,186
8	6,560
9	19,682
10	59,408

Table 1.1: Values of $3^n - 1$ from 1 to 10

Conjecture 1.1.1
For every positive integer n, $3^n - 1$ is even.

Conjecture 1.1.2
For every positive integer $n > 1$, $3^n - 2^n$ is odd.

There are no aparent relationships involving primes.

n	$3^n - 2^n$
1	0
2	1
3	5
4	19
5	65
6	211
7	665
8	2,059
9	6,305
10	19,171

Table 1.2: Values of $3^n - 2^n$ from 1 to 10

Question 3

*3. The proof of Theorem 3 gives a method for finding a prime number different from any in a given list of prime numbers.
(a) Use this method to find a prime different from 2, 3, 5, and 7.
(b) Use this method to find a prime different from 2, 5, and 11.

Solution: **(a)** Given said proof, we have a list of primes $p_1, p_2 \ldots p_n$. We can create a number $m = p_1 * p_2 * \ldots * p_n + 1$, for the given list this results in $m = 211$.
Solution: **(b)** With the same process we reach $m = 111$.

Question 4

4. Find five consecutive integers that are not prime.

Solution: We can solve this with a simple python script:

```python
L = []
for n in range (2, 100):
    prime = True

    for i in range (2, int(n/2+1)):
        if n%i == 0:
            prime = False
            break

    if prime:
        L = []
    else:
        L.append(n)

    if len(L) == 5:
        print(L)
        break
```

Which outputs: $24, 25, 26, 27, 28$.

Question 5

5. Use the table in Figure I.1 and the discussion on p. 5 to find two more perfect numbers.

Solution: We know that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect. For $n = 7$, $2^n - 1$ is prime so $2^{n-1}(2^n - 1) = 8,128$ is perfect. For $n = 5$, $2^n - 1$ is prime so $2^{n-1}(2^n - 1) = 496$ is perfect.

Question 6

6. The sequence 3, 5, 7 is a list of three prime numbers such that each pair of adjacent numbers in the list differ by two. Are there any more such "triplet primes"?

Solution: Again, this can be solved using python:

```
L = []
for n in range (2, 10000):
    prime = True

    for i in range (2, int(n/2+1)):
        if n%i == 0:
            prime = False
            break

    if prime:
        if len(L) == 0:
            L.append(n)
        else:
            if n == L[-1]+2:
                L.append(n)
            else:
                L = [n]

    if len(L) == 3:
        print(L)
        L.pop(0)
```

The script only prints the sequence $3, 5, 7$, so it seems like there aren't any more such "triplet primes". [2]

Question 7

7. A pair of distinct positive integers (m, n) is called amicable if the sum of all positive integers smaller than n that divide n is m, and the sum of all positive integers smaller than m that divide m is n. Show that (220, 284) is amicable.

Solution: With python:

```
def find_divisors(number):
    divisors = []
    for i in range(1, number):
        if number % i == 0:
            divisors.append(i)
    return divisors

def check_amicable(m,n):
    divm = find_divisors(m)
    divn = find_divisors(n)

    if sum(divm) == n and sum(divn) == m:
        return True
    else:
        return False

print(check_amicable(220,284))
```

The output of the script shows that this pair is indeed amicable.

[2] According to number theory, prime triplets are of the form $(p, p+2, p+6)$ or $(p, p+4, p+6)$. Wich differ from the definition given by the exercise.

Chapter 2

Sequential Logic

2.1 Deductive Logic and Logical Connectives

Deductive reasoning is the foundation on which proofs are based.

Example 2.1.1 (Deductive Reasoning)

1. It will either rain or snow tomorrow.
   It's too warm to snow.
   Therefore, it will rain.
2. If today is Sunday, then I don't have to work today.
   Today is Sunday.
   Therefore, I don't have to work today.
3. I will work either tomorrow or today.
   I'm not working today.
   Therefore, I'm working tomorrow.

In each case we arrive at a conclusion given a set of premises which are assumed to be true. The conclusion can only be false if at least one of the premises is false. If none of them are false, then the conclusion must be true.

Definition 2.1.1: Valid Argument

A valid argument is one in which the premises cannot all be true without the conclusion being true as well.

Note:
An invalid argument is also known as a fallacy, in this case a false conclusion can be reached even if all the premises are true.

Example 2.1.2 (Statements and their Logical Forms)

1. Either John went to the store, or we're out of eggs.
2. Joe is going to leave home and not come back.
3. Either Bill is at work and Jane isn't, or Jane is at work and Bill isn't.

Natural Language	Symbol
And	$\wedge$
Or	$\vee$
Not	$\neg$
If and only if	$\Longleftrightarrow$
Implies	$\longrightarrow$
Exclusive or	$\oplus$
True	$\top$
False	$\perp$
For all	$\forall$
There exists	$\exists$

Table 2.1: Logical Connectives

Solution:

1. $P \vee Q$
2. $P \wedge Q$
3. $(P \wedge \neg Q) \vee (\neg P \wedge Q)$

Note:

$\neg$ always applies only to the statement immediately after it. $\neg P \wedge Q$ means $(\neg P) \wedge Q$.

2.1.1 Exercises

Question 8

*1. Analyze the logical forms of the following statements:
(a) We'll have either a reading assignment or homework problems, but we won't have both homework problems and a test.
(b) You won't go skiing, or you will and there won't be any snow.
(c) $\sqrt{7} \nleq 2$

Solution: **(a)** $(P \vee Q) \wedge \neg(Q \wedge R)$
Solution: **(b)** $(\neg P) \vee (P \wedge \neg Q)$
Solution: **(c)** $\neg P \wedge \neg Q$

Question 9

2. Analyze the logical forms of the following statements:
(a) Either John and Bill are both telling the truth, or neither of them is.
(b) I'll have either fish or chicken, but I won't have both fish and mashed potatoes.
(c) 3 is a common divisor of 6, 9, and 15.

Solution: **(a)** $(P \wedge Q) \vee (\neg P \wedge \neg Q)$
Solution: **(b)** $(P \vee Q) \wedge \neg(P \wedge R)$
Solution: **(c)** $P \wedge Q \wedge R$

Question 10

3. Analyze the logical forms of the following statements:
(a) Alice and Bob are not both in the room.
(b) Alice and Bob are both not in the room.
(c) Either Alice or Bob is not in the room.
(d) Neither Alice nor Bob is in the room.

Solution: **(a)** $\neg(P \wedge Q)$
Solution: **(b)** $\neg P \wedge \neg Q$
Solution: **(c)** $\neg P \vee \neg Q$
Solution: **(d)** $\neg P \wedge \neg Q$

Question 11

4. Analyze the logical forms of the following statements:
(a) Either both Ralph and Ed are tall, or both of them are handsome.
(b) Both Ralph and Ed are either tall or handsome.
(c) Both Ralph and Ed are neither tall nor handsome.
(d) Neither Ralph nor Ed is both tall and handsome.

Solution: **(a)** $(P \wedge Q) \vee (R \wedge S)$
Solution: **(b)** $(P \vee R) \wedge (Q \wedge S)$
Solution: **(c)** $(\neg P \wedge \neg R) \wedge (\neg Q \wedge \neg S)$
Solution: **(d)** $\neg(P \wedge R) \wedge \neg(Q \wedge S)$

Question 12

5. Which of the following expressions are well-formed formulas?
(a) $\neg(\neg P \vee \neg\neg Q)$.
(b) $\neg(P, Q, \wedge R)$.
(c) $P \wedge \neg P$.
(d) $(P \wedge Q)(P \vee Q)$.

Solution: **(b)** and **(d)** are not well-formed formulas.

Question 13

*6. Let P stand for the statement "I will buy the pants" and S for the statement "I will buy the shirt." What English sentences are represented by the following formulas?
(a) $\neg(P \wedge \neg S)$.
(b) $\neg P \wedge \neg S$.
(c) $\neg P \vee \neg S$.

Solution: **(a)** I won't buy the pants but not the shirt.
Solution: **(b)** I won't buy the pants and I won't buy the shirt.
Solution: **(c)** I won't buy the pants or I won't buy the shirt.

Question 14

7. Let S stand for the statement "Steve is happy" and G for "George is happy." What English sentences are represented by the following formulas?
(a) $(S \vee G) \wedge (\neg S \vee \neg G)$.
(b) $[S \vee (G \wedge \neg S)] \vee \neg G$.
(c) $S \vee [G \wedge (\neg S \vee \neg G)]$.

Solution: **(a)** Either Steve or George is happy, but either Steve or George is not happy.
Solution: **(b)** Either Steve is happy or Steve is not happy and George is happy, or George is not happy.
Solution: **(c)** Either Steve is happy, or George is happy but Steve is not happy or George is not happy.

Question 15

8. Let T stand for the statement "Taxes will go up" and D for "The deficit will go up." What English sentences are represented by the following formulas?
(a) $T \vee D$.
(b) $\neg(T \wedge D) \wedge \neg(\neg T \wedge \neg D)$.
(c) $(T \wedge \neg D) \vee (D \wedge \neg T)$.

Solution: **(a)** Taxes will go up or the deficit will go up.
Solution: **(b)** Not both Taxes and deficit will go up, but not both taxes and deficit won't go up.
Solution: **(c)** Either taxes will go up and the deficit will go down, or the deficit will go up and taxes will go down.

Question 16

9. Identify the premises and conclusions of the following deductive arguments and analyze their logical forms. Do you think the reasoning valid? (Although you will have only your intuition to guide you in answering this last question, in the next section we will develop some techniques for determining the validity of arguments.)
(a) Jane and Pete won't both win the math prize. Pete will win either the math prize or the chemistry prize. Jane will win the math prize. Therefore, Pete will win the chemistry prize.
(b) The main course will be either beef or fish. The vegetable will be either peas or corn. We will not have both fish as a main course and corn as a vegetable. Therefore, we will not have both beef as a main course and peas as a vegetable.
(c) Either John or Bill is telling the truth. Either Sam or Bill is lying. Therefore, either John is telling the truth or Sam is lying.
(d) Either sales will go up and the boss will be happy, or expenses will go up and the boss won't be happy. Therefore, sales and expenses will not both go up.

Solution: **(a)**

$$\begin{array}{l} \neg(J_m \wedge P_m) \\ P_m \vee P_q \\ J_m \\ \hline \therefore P_q \end{array}$$

Solution: **(b)**

$$\begin{array}{l} M_f \vee M_b \\ V_p \vee V_c \\ \neg(M_f \wedge V_c) \\ \hline \therefore \neg(M_b \wedge V_p) \end{array}$$

Seems like the right conclusion would be $M_b \wedge V_P$.

Solution: (c)

$$\begin{array}{l} J \lor B \\ \neg S \lor \neg B \\ \hline \therefore (J \lor \neg S) \end{array}$$

Solution: (d)

$$\begin{array}{l} (S \land B) \lor (E \land \neg B) \\ \hline \therefore \neg(S \land E) \end{array}$$

2.2 Truth Tables

Definition 2.2.1: Truth Table

A Truth Table summarizes all possibilities for a given logic statement.

P	Q	$P \land Q$
F	F	F
F	T	F
T	F	F
T	T	T

Table 2.2: $P \land Q$

Note:

Unless specified otherwise, in mathematics $\lor$ is inclusive.

Example 2.2.1 (Truth Table)

Make a truth table for the formula $\neg(P \land Q) \lor \neg R$.

Solution:

P	Q	R	$P \land Q$	$\neg(P \land Q)$	$\neg R$	$\neg(P \land Q) \lor \neg R$
F	F	F	F	T	T	T
F	F	T	F	T	F	T
F	T	F	F	T	T	T
F	T	T	F	T	F	T
T	F	F	F	T	T	T
T	F	T	F	T	F	T
T	T	F	T	F	T	T
T	T	T	T	F	F	F

Table 2.3: $\neg(P \land Q) \lor \neg R$

Truth tables are to be used to study if an argument is valid. Consider again the following argument:
It will either rain or snow tomorrow.
It's too warm for snow.
Therefore, it will rain.
This argument is of the form:

$$\begin{array}{l} P \lor Q \\ \neg Q \\ \hline \therefore P \end{array}$$

So we can build the following truth table:

P	Q	$P \vee Q$	$\neg Q$	P
F	F	F	T	F
F	T	T	F	F
T	F	T	T	T
T	T	T	F	T

Table 2.4: Rain or Snow Tomorrow

On the previous section a valid argument was defined as one in which the conclusion is true if all premises are true. For this argument, the second to last row of the table represents this scenario. We can see that if both premises are true then the conclusion is true, therefore this is a valid argument.

Example 2.2.2 (Determine whether the following arguments are valid)

1. Either John isn't smart and he is lucky, or he's smart.
   John is smart.
   Therefore, John isn't lucky.

2. The butler and the cook are not both innocent.
   Either the butler is lying or the cook is innocent.
   Therefore, the butler is either lying or guilty.

Solution: **1.**

$$\begin{array}{l} (\neg P \wedge Q) \vee P \\ P \\ \hline \therefore \neg Q \end{array}$$

The reasoning seems faulted, lets build the truth table:

P	Q	$(\neg P \wedge Q) \vee P$	P	$\neg Q$
F	F	F	F	T
F	T	T	F	F
T	F	T	T	T
T	T	T	T	F

Table 2.5: John is Smart and Lucky, or just smart

The last row shows a case in which both premises are true but the conclusion is false, so the argument is not valid.

Solution: **2.**

$$\begin{array}{l} \neg(B_i \wedge C_i) \\ B_l \vee C_i \\ \hline \therefore \neg B_i \vee B_l \end{array}$$

B_i	C_i	B_l	$\neg(B_i \wedge C_i)$	$B_l \vee C_i$	$\neg B_i \vee B_l$
F	F	F	T	F	T
F	F	T	T	T	T
F	T	F	T	T	T
F	T	T	T	T	T
T	F	F	T	F	F
T	F	T	T	T	T
T	T	F	F	T	F
T	T	T	F	T	T

Table 2.6: The Butler is Lying or Innocent

The argument is valid.

Definition 2.2.2: Equivalent Formulas

Equivalent formulas always have the same truth values.

P	Q	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
F	F	T	T
F	T	T	T
T	F	T	T
T	T	F	F

Table 2.7: Equivalent Formulas

The following is a list of equivalences that come up often in logic.

Axiom 2.2.1 De Morgan's Laws

$\neg(P \vee Q)$ is equivalent to $\neg P \wedge \neg Q$.
$\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$.

Axiom 2.2.2 Commutative Laws

$P \wedge Q$ is equivalent to $Q \wedge P$.
$P \vee Q$ is equivalent to $Q \vee P$.

Axiom 2.2.3 Associative Laws

$P \wedge (Q \wedge R)$ is equivalent to $(P \wedge Q) \wedge R$.
$P \vee (Q \vee R)$ is equivalent to $(P \vee Q) \vee R$.

Axiom 2.2.4 Idempotent Laws

$P \wedge P$ is equivalent to P.
$P \vee P$ is equivalent to P.

Axiom 2.2.5 Distributive Laws

$P \wedge (Q \vee R)$ is equivalent to $(P \wedge Q) \vee (P \wedge R)$.
$P \vee (Q \wedge R)$ is equivalent to $(P \vee Q) \wedge (P \vee R)$.

Axiom 2.2.6 Absorption Laws

$P \vee (P \wedge Q)$ is equivalent to P.
$P \wedge (P \vee Q)$ is equivalent to P.

Axiom 2.2.7 Double Negation Law

$\neg\neg P$ is equivalent to P.

Example 2.2.3 (Find simpler formulas equivalent to these formulas)

1. $\neg(P \lor \neg Q)$.
2. $\neg(Q \land \neg P) \lor P$.

Solution: **1.** $\neg(P \lor \neg Q)$ is equivalent to $\neg P \land Q$.
Solution: **2.** $\neg(Q \land \neg P)$ is equivalent to $\neg Q \lor P$. We have $(\neg Q \lor P) \lor P$ which is equivalent to $\neg Q \lor P$.

Definition 2.2.3: Tautology

A Tautology is a formula which is always true.

Definition 2.2.4: Contradiction

A Contradiction is a formula which is always false.

Axiom 2.2.8 Tautology Laws

$P\land$(a tautology) is equivalent to P.
$P\lor$(a tautology) is a tautology.
$\neg$(a tautology) is a contradiction.

Axiom 2.2.9 Contradiction Laws

$P\land$(a contradiction) is a contradiction.
$P\lor$(a contradiction) is equivalent to P.
$\neg$(a contradiction) is a tautology.

Example 2.2.4 (Find simpler formulas equivalent to these formulas)

1. $P \lor (Q \land \neg P)$.
2. $\neg(P \lor (Q \land \neg R)) \land Q$.

Solution: **1.** $P \lor (Q \land \neg P)$ is equivalent to $(P \lor Q) \land (P \lor \neg P)$, which simplifies to $P \lor Q$.
Solution: **2.**

We start by simplifying the first part of the statement

$$\neg(P \lor (Q \land \neg R))$$
$$\neg P \land \neg(Q \land \neg R)$$
$$\neg P \land (\neg Q \lor R)$$

Then adding the second part

$$\neg P \land (\neg Q \lor R) \land Q$$
$$\neg P \land (\neg Q \land Q) \lor (R \land Q)$$
$$\neg P \land (R \land Q)$$

2.2.1 Exercises

Question 17

3. In this exercise we will use the symbol + to mean exclusive or. In other words, P + Q means "P or Q, but not both."
(a) Make a truth table for $P + Q$.
(b) Find a formula using only the connectives $\wedge$, $\vee$, and $\neg$ that is equivalent to $P + Q$. Justify your answer with a truth table.

Solution: **(a)**

P	Q	$P + Q$
F	F	F
F	T	T
T	F	T
T	T	F

Table 2.8: Exercise 3.1

Solution: **(b)** $(P \wedge \neg Q) \vee (\neg P \wedge Q)$

P	Q	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$
F	F	F
F	T	T
T	F	T
T	T	F

Table 2.9: Exercise 3.2

Question 18

4. Find a formula using only the connectives $\wedge$ and $\neg$ that is equivalent to $P \vee Q$. Justify your answer with a truth table.

Solution: Using De Morgan's Laws we reach $\neg(\neg P \wedge \neg Q)$

P	Q	$(\neg P \wedge \neg Q)$	$\neg(\neg P \wedge \neg Q)$
F	F	T	F
F	T	F	T
T	F	F	T
T	T	F	T

Table 2.10: Exercise 4

Question 19

*5. Some mathematicians use the symbol $\downarrow$ to mean nor. In other words, $P \downarrow Q$ means "neither P nor Q."
(a) Make a truth table for $P \downarrow Q$.
(b) Find a formula using only the connectives $\wedge$, $\vee$, and $\neg$ that is equivalent to $P \downarrow Q$.
(c) Find formulas using only the connective $\downarrow$ that are equivalent to $\neg P$, $P \vee Q$, and $P \wedge Q$.

Solution: **(a)**

P	Q	$P \downarrow Q$
F	F	T
F	T	F
T	F	F
T	T	F

Table 2.11: Exercise 5.1

Solution: **(b)** $\neg P \wedge \neg Q$

P	Q	$\neg P \wedge \neg Q$
F	F	T
F	T	F
T	F	F
T	T	F

Table 2.12: Exercise 5.2

Solution: **(c)** **1** $P \downarrow P$, **2** $(P \downarrow Q) \downarrow (P \downarrow Q)$, **3** $(P \downarrow P) \downarrow (Q \downarrow Q)$

P	$P \downarrow P$
F	T
T	F

Table 2.13: Exercise 5.3.1

P	Q	$P \downarrow Q$	$(P \downarrow Q) \downarrow (P \downarrow Q)$
F	F	T	F
F	T	F	T
T	F	F	T
T	T	F	T

Table 2.14: Exercise 5.3.2

P	Q	$P \downarrow P$	$Q \downarrow Q$	$(P \downarrow P) \downarrow (Q \downarrow Q)$
F	F	T	T	F
F	T	T	F	F
T	F	F	T	F
T	T	F	F	T

Table 2.15: Exercise 5.3.3

Question 20