How To Prove It: A Structured Approach

Christian Quintanar

May 2025

Chapter 0

Introduction

0.1 Introduction

0.1.1 Recapitulation

High school mathematics is concerd mostly with solving equations and computing answers to numerical questions. College mathematics deals with a wider variety of questions, involving not only numbers, but also sets, functions, and other mathematical objects. What ties them together is the use of deductive reasoning to find the answers to questions.

Deductive reasoning uses general ideas to come to a specific conclusion. Deductive reasoning in mathematics is usually presented in the form of a *proof*.

A number is *prime* of it cannot be written as a product of two smaller positive integers. If it can be written as a product of two smaller positive integers, then it is *composite*

A *conjecture* is a conclusion that is proffered on a tentative basis without proof.

Conjecture 1. *Suppose n is an integer larger than 1 and n is prime. Then $2^n - 1$ is prime.*

Conjecture 2. *Suppose n is an integer larger than 1 and n is not prime. Then $2^n - 1$ is not prime.*

A *counterexample* is a specific instance that demonstrates the falsity of a general statement, argument or theory.

The existence of even one counterexample establishes that a conjecture is incorrect. However, failure to find a counterexample to a conjecture does not show that the conjecture is correct.

We can never be sure that the conjecture is correct if we only check examples. No matter how many examples we check, there is always the possibility that the next one will be the first counterexample.

Once a conjecture has been proven, we can call it a *theorem*.

Theorem 3. *Suppose n is an integer larger than 1 and n is not prime. Then $2^n - 1$ is not prime*

Prime numbers of the form $2^n - 1$ are called *Mersenne primes*. Although many Mersenne primes have been found, it is still not know if there are infinitely many of them.

A positive integer n is said to be *perfect* if n is equal to the sum of all positive integers smaller than n that divide n.

For any two integers m and n, we say that m *divides* n if n is divisible by m; in other words, if there is an integer q such that $n = qm$.

For any positive integer n, the product of all integers from 1 to n is called n *factorial* and is denoted $n!$.

Theorem 4. *For every positive integer n, there is a sequence of n consecutive positive integers containing no primes*

Pairs of primes that differ by only two are called *twin primes*

0.1.2 Problems

1. (a)
$$2^{ab} - 1 = (2^b - 1)(1 + 2^b + 2^{2b} + ... + 2^{(a-1)b})$$
$$n = ab = 15; a = 3; b = 5$$
$$2^{(3)(5)} = (2^5 - 1)(1 + 2^5 + 2^{10}) = (31) \cdot (1057)$$

   (b)
$$2^{ab} - 1 = (2^b - 1)(1 + 2^b + 2^{2b} + ... + 2^{(a-1)b})$$
$$n = ab = 32767; a = 1057; b = 31$$
$$2^{1057 \cdot 31} - 1 = (2^{31} - 1)(1 + 2^{31} + ... + 2^{1056 \cdot 31})$$
$$1 < 2^{31} - 1 < 2^{32767} - 1$$

2.

	$3^n - 1$	
$n=1$	$3^1 - 1 = 2$	Prime
$n=2$	$3^2 - 1 = 8$	Not Prime
$n=3$	$3^3 - 1 = 26$	Not Prime
$n=4$	$3^4 - 1 = 80$	Not Prime
$n=5$	$3^5 - 1 = 242$	Not Prime
$n=6$	$3^6 - 1 = 728$	Not Prime
$n=7$	$3^7 - 1 = 2186$	Not Prime
$n=8$	$3^8 - 1 = 6560$	Not Prime
$n=9$	$3^9 - 1 = 19682$	Not Prime
$n=10$	$3^{10} - 1 = 59048$	Not Prime

For all $n > 1$, $3^n - 1$ is not a prime

	$3^n - 2^n$	
$n=1$	$3^1 - 2^1 = 1$	Prime
$n=2$	$3^2 - 2^2 = 5$	Prime
$n=3$	$3^3 - 2^3 = 19$	Prime
$n=4$	$3^4 - 2^4 = 65$	Not Prime
$n=5$	$3^5 - 2^5 = 211$	Prime
$n=6$	$3^6 - 2^6 = 665$	Not Prime
$n=7$	$3^7 - 2^7 = 2059$	Not Prime
$n=8$	$3^8 - 2^8 = 6305$	Not Prime
$n=9$	$3^9 - 2^9 = 19171$	Not Prime
$n=10$	$3^{10} - 2^10 = 58025$	Not Prime

If n is not prime, then $3^n - 2^n$ is not prime. If n is prime, then $3^n - 2^n$ is either prime or composite.

3. (a)
$$m = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$$
$$m = 2 \cdot 3 \cdot 5 \cdot 7 + 1$$
$$m = 211$$

(b)

$$m = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$$

$$m = 2 \cdot 5 \cdot 11 + 1$$

$$m = 111 = 3 \cdot 37$$

4.

$$x = (n+1)! + 2; n = 5$$

$$x = (5+1)! + 2 = 6! + 2 = 722$$

$$[722, 723, 724, 725, 726]$$

5.

$n = 3$	$2^{n-1}(2^n - 1) = 2^{3-1}(2^3 - 1) = 28$
$n = 5$	$2^{n-1}(2^n - 1) = 2^{5-1}(2^5 - 1) = 496$

6.

$$mod(n, 3) = \begin{cases} 0, \text{n is divisible by 3;} \\ 1, \text{n + 2 is divisible by 3} \\ 2, \text{n + 4 is divisible by 3} \end{cases} \tag{1}$$

7.

$$220 : [1, 2, 4, 5, 10, 11, 22, 44, 55, 110]$$

$$1 + 2 + 4 + 5 + 10 + 11 + 22 + 44 + 55 + 110 = 284$$

$$284 : [1, 2, 4, 71, 142]$$

$$1 + 2 + 4 + 71 + 142 = 220$$

Chapter 1

Sentential Logic

1.1 Deductive Reasoning and Logical Connectives

1.1.1 Recapitulation

Profs play a central role in mathematics, and deductive reasoning is the foundation on which proofs are based.

We arrive at a *conclusion* from the assumption that some other statements, called *premises*, are true.

We will say that an argument is *valid* if the premises cannot all be true without the conclusion being true as well. And is *invalid* otherwise.

Connective symbols are symbols used to combine statements to form more complex statements.

Symbol	Meaning
$\vee$	or
$\wedge$	and
$\neg$	not

The statement $P \vee Q$ is called the disjunction of P and Q, the statement $P \wedge Q$ is called the conjunction of P and Q, and $\neg P$ is called the negation of P.

1.1.2 Problems

1. (a)

$$P : \text{We'll have reading assignment}$$

$$Q : \text{We'll have homework problems}$$

$$R : \text{We'll have a test}$$

$$(P \vee Q) \wedge \neg(Q \wedge R)$$

(b)

$$P : \text{You will go skiing}$$
$$Q : \text{There will snow}$$
$$\neg P \vee (P \wedge \neg Q)$$

(c)

$$\neg((\sqrt{7} < 2) \vee (\sqrt{7} = 2))$$

2. (a)

$$P : \text{John is telling the truth}$$
$$Q : \text{Bill is telling the truth}$$
$$(P \wedge Q) \vee (\neg P \wedge \neg Q)$$

(b)

$$P : \text{I'll have fish}$$
$$Q : \text{I'll have chicken}$$
$$R : \text{I'll have mashed potatoes}$$
$$(P \vee Q) \wedge \neg(P \wedge R)$$

(c)

$$P : \text{3 is a common divisor of 6}$$
$$Q : \text{3 is a common divisor of 9}$$
$$R : \text{3 is a common divisor of 15}$$
$$P \wedge Q \wedge R$$

3. (a)

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

(b)

$$\neg P \wedge \neg Q$$

(c)

$$\neg P \vee \neg Q$$

(d)

$$\neg(P \vee Q)$$

4. (a)

$$(P \wedge Q) \vee (R \wedge S)$$

(b)

$$(P \vee R) \wedge (Q \vee S)$$

(c)

$$\neg(P \vee R) \wedge \neg(Q \vee S)$$

(d)
$$\neg((P \wedge R) \vee (Q \wedge S))$$

5. (a) Well-formed
   (b) Not well-formed
   (c) Well-formed
   (d) Not well-formed

6. (a) I won't buy the pants without a shirt
   (b) I won't buy the pants nor the shirt
   (c) Either I won't buy the pants or I won't buy the shirt

7. (a) Either Steve or George is happy, and Either Steve or George is not happy
   (b) Either Steve is happy, or George is happy and Steve isn't happy or George is not happy
   (c) Either Steve is happy, or George is happy and Either Stever or George are not happy

8. (a) Either taxes will go up or The deficit will go up
   (b) The taxes and the deficit won't go up and it is not the case that the taxes and the deficit won't go up
   (c) Either the taxes will go up and the deficit won't go up, or the deficit will go up and the taxes won't go up

9. (a) Conclusion: Pete will win the chemistry prize
   (b) Conclusion: We will not have both beef as a main course and peas as a vegetable.
   (c) Conclusion: Either John is telling the truth or Sam is lying.
   (d) Conclusion: Sales and expenses will not both go up.

1.2 Truth Tables

1.2.1 Recapitulation

When we evaluate the truth or falsity of a statement, we assign to it one of the labels *true* or *false*, and this label is called its *truth value*.

A *Truth table* is a table in which each of its rows shows one of the possible combinations of truth values for a statement or a compound statement.

To verify the validity of arguments, we can arrage the truth values of the premises and the conclusion in a truth table, in the rows where the premises are all true it must follow that the conclusion is also true, thus the argument is valid, otherwise it is invalid.

Equivalent formulas always have the same truth value no matter what the truth value of those statements are.

Formulas that are always true, are called *tautologies*, formulas that are always false are called *contradictions*.

1.2.2 Problems

1. (a)

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

(b)

S	G	$(S \vee G) \wedge (\neg S \vee \neg G)$
F	F	F
F	T	T
T	F	T
T	T	F

2. (a)

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

(b)

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

3. (a)

P	Q	$P \oplus Q$
F	F	F
F	T	T
T	F	T
T	T	F

(b)

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

4.

$$P \vee Q \equiv \neg(\neg P \wedge \neg Q)$$

5. (a)

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

(b)

$$P \downarrow Q \equiv \neg P \wedge \neg Q \equiv \neg(P \vee Q)$$

(c)

$$\neg P \equiv P \downarrow P$$
$$P \vee Q \equiv (P \downarrow Q) \downarrow (P \downarrow Q)$$
$$P \wedge Q \equiv (P \downarrow P) \downarrow (Q \downarrow Q)$$

6. (a)

P	Q	$P \mid Q$
F	F	T
F	T	T
T	F	T
T	T	F

(b)

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

(c)

$$\neg P \equiv P \mid P$$
$$P \vee Q \equiv (P \mid P) \mid (Q \mid Q)$$
$$P \wedge Q \equiv (P \mid Q) \mid (P \mid Q)$$

7. (a) Valid
   (b) Invalid
   (c) Valid
   (d) Invalid

8.

$$(a) \equiv (c), (b) \equiv (e)$$

9. (b) is a contradiction; (c) is a tautology

10. Not needed

11. (a)

$$\neg(\neg P \wedge \neg Q) \equiv P \vee Q$$

(b)

$$(P \wedge Q) \vee (P \wedge \neg Q) \equiv P$$

(c)

$$\neg(P \wedge \neg Q) \vee (\neg P \wedge Q) \equiv \neg P \vee Q$$

12. (a)
$$\neg(\neg P \vee Q) \vee (P \wedge \neg R \equiv P \wedge \neg(Q \wedge R)$$
(b)
$$\neg(\neg P \wedge Q) \vee (P \wedge \neg R) \equiv \neg Q \vee P$$
(c)
$$(P \wedge R) \vee (\neg R \wedge (P \vee Q)) \; equiv \neg P \wedge \neg Q$$
13. Not needed
14. Not needed
15.
$$2^n$$
16.
$$P \vee \neg Q$$
17.
$$(P \wedge \neg Q) \vee (\neg P \wedge Q)$$
18. (1) That it is valid; (2) That it is invalid if there is a combination where all premises are true; (3) Could be either valid or invalid for a tautology, if it is a contradiction then it is valid

1.3 Variables and Sets

1.4 Operations on Sets

1.5 The Conditional and Biconditional Connectives

Chapter 2

Quantificational Logic

Chapter 3

Proofs

Chapter 4

Relations

Chapter 5

Functions

Chapter 6

Mathematical Induction

Chapter 7

Number Theory

Chapter 8

Infinite Sets