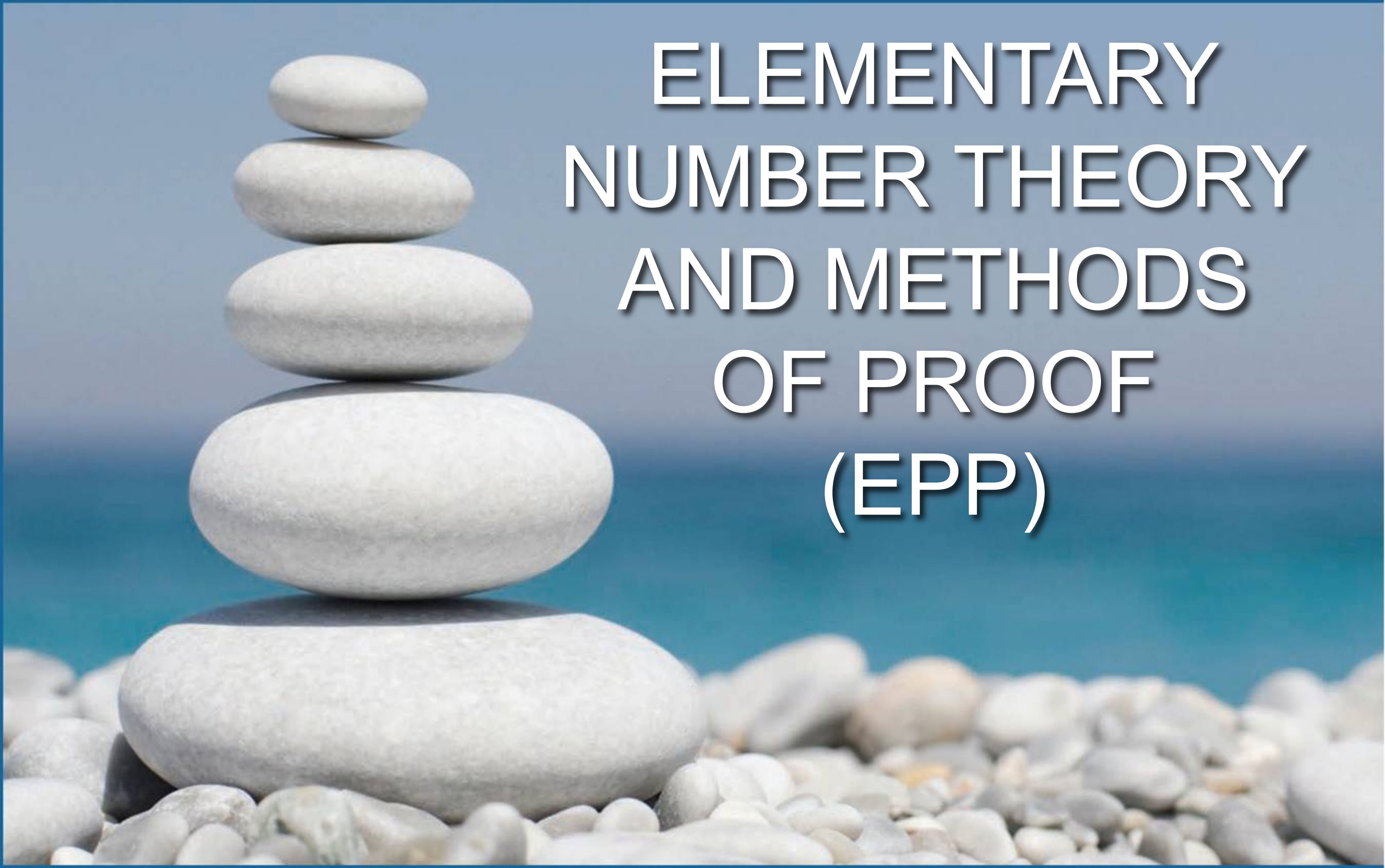


ELEMENTARY NUMBER THEORY AND METHODS OF PROOF (EPP)

Alessandro Artale – UniBZ - http://www.inf.unibz.it/~artale/

EPP: 4.1

Direct Proof and Counterexample I:Introduction

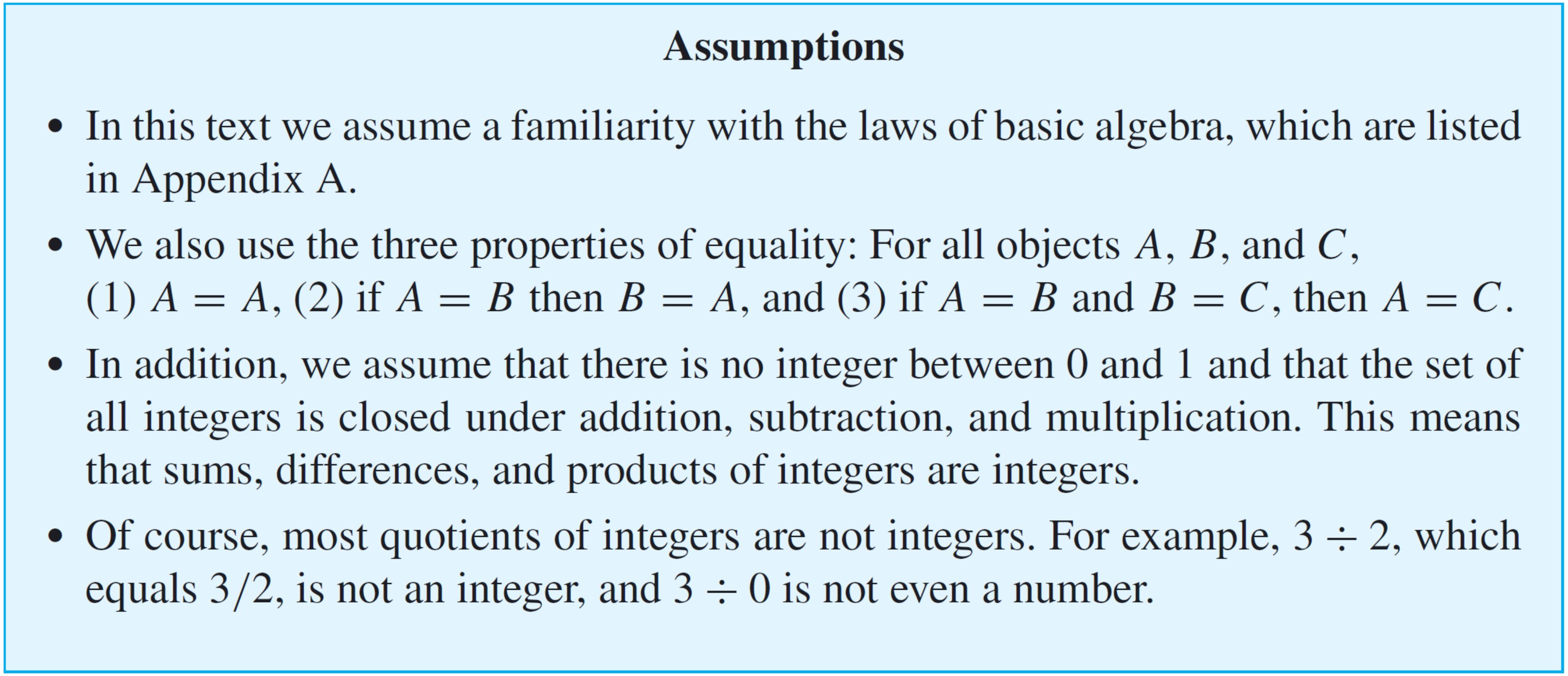
Direct Proof and Counterexample I: Introduction

Both discovery and proof are integral parts of problem solving. When you think you have discovered that a certain statement is true, try to figure out why it is true.

If you succeed, you will know that your discovery is genuine. Even if you fail, the process of trying will give you insight into the nature of the problem and may lead to the discovery that the statement is false.

"Details are crucial": writing a proof forces us to be aware of weakness in our arguments and on unconscious assumptions.

Direct Proof and Counterexample I: Introduction



Assumptions

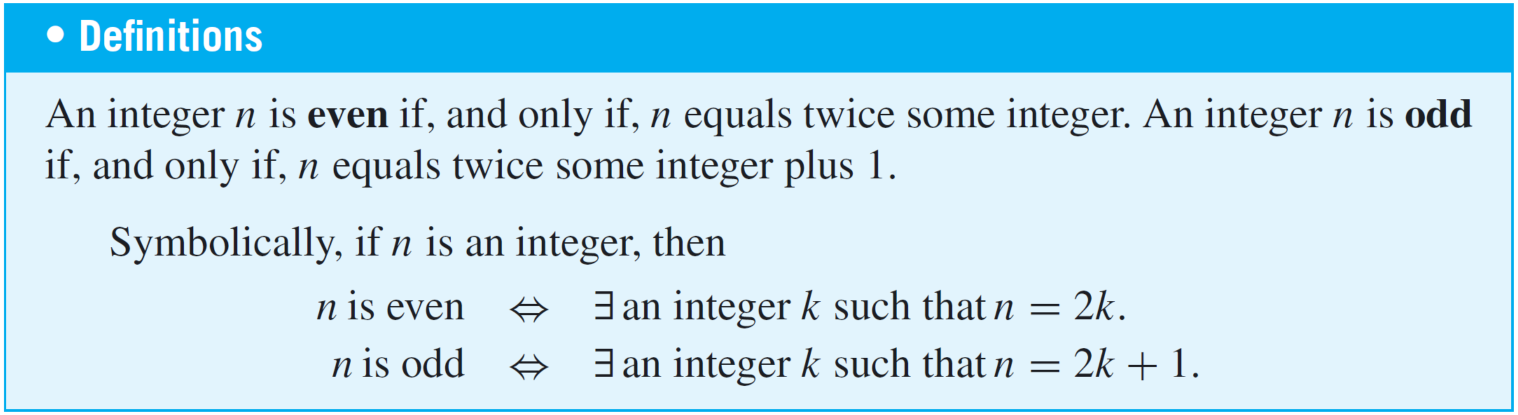
- In this text we assume a familiarity with the laws of basic algebra, which are listed in Appendix A.
- We also use the three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$ then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.
- Of course, most quotients of integers are not integers. For example, $3 \div 2$, which equals $3/2$, is not an integer, and $3 \div 0$ is not even a number.

Definitions

Definitions – Even Vs. Odd

In order to evaluate the truth or falsity of a statement, you must understand what the statement is about. In other words, you must know the meanings of all terms that occur in the statement.

Mathematicians define terms very carefully and precisely and consider it important to learn definitions virtually word for word.



- **Definitions**

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

Symbolically, if n is an integer, then

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

Example 1 – *Even and Odd Integers*

Use the definitions of *even* and *odd* to justify your answers to the following questions.

a. Is 0 even?

b. Is −301 odd?

c. If *a* and *b* are integers, is $6a^2b$ even?

d. If *a* and *b* are integers, is $10a + 8b + 1$ odd?

e. Is every integer either even or odd?

Example 1 – *Solution*

cont’d

Solution:

a. Yes, $0 = 2 \cdot 0$.

b. Yes, $-301 = 2(-151) + 1$.

c. Yes, $6a^2b = 2(3a^2b)$, and since a and b are integers, so is $3a^2b$ (being a product of integers).

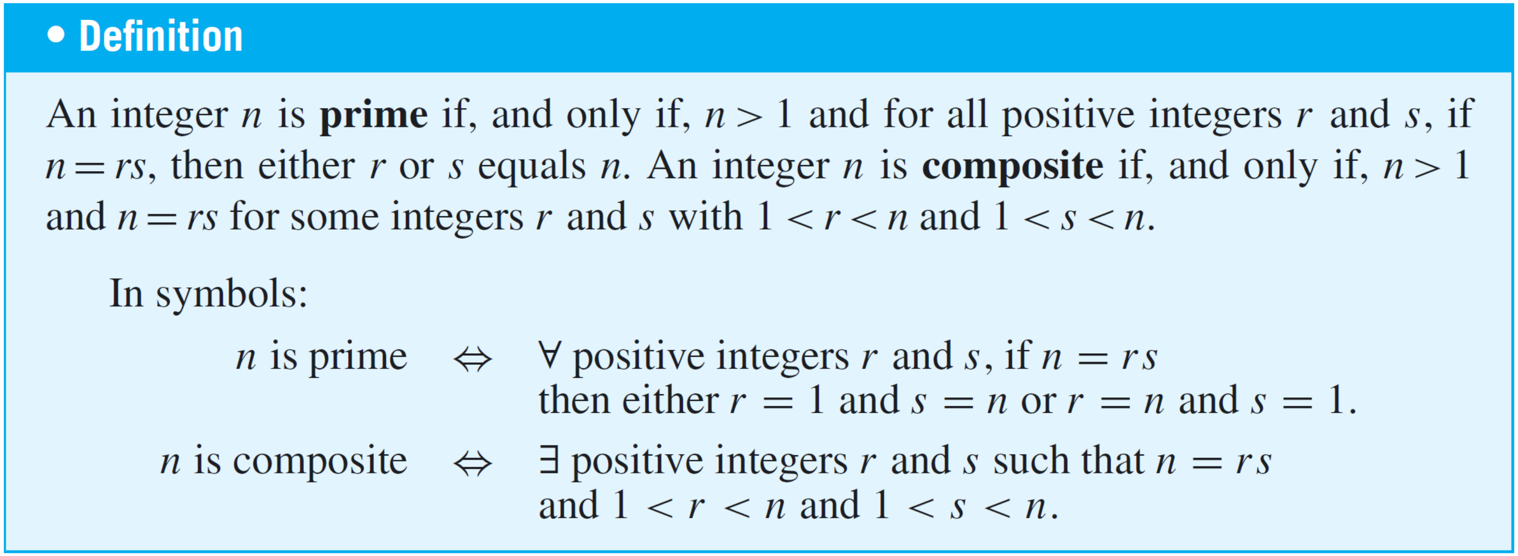
d. Yes, $10a + 8b + 1 = 2(5a + 4b) + 1$, and since a and b are integers, so is $5a + 4b$ (being a sum of products of integers).

e. The answer is yes, although the proof is not obvious.

Definitions – Prime Numbers

The integer 6, which equals 2 • 3, is a product of two smaller positive integers.

On the other hand, 7 cannot be written as a product of two smaller positive integers; its only positive factors are 1 and 7. A positive integer, such as 7, that cannot be written as a product of two smaller positive integers is called *prime*.



- **Definition**

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

Example 2 – *Prime and Composite Numbers*

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

Example 2 – *Solution*

Solution:

a. No. A prime number is required to be greater than 1.

b. Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely $r = n$ and $s = 1$ and $r = 1$ and $s = n$.

Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \leq r \leq n$ and $1 \leq s \leq n$. If n is prime, then the two displayed pairs are the only ways to write n as rs.

Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

Example 2 – *Solution*

cont’d

c. 2, 3, 5, 7, 11, 13

d. 4, 6, 8, 9, 10, 12

Proving Existential Statements

Proving Existential Statements

A statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if and only if,

$Q(x)$ is true for at least one x in D.

One way to prove this is to find an x in D that makes $Q(x)$ true: called **constructive proofs of existence**.

Example 3 – *Constructive Proofs of Existence*

a. Prove the following: $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.

b. Suppose that r and s are integers. Prove the following: $\exists$ an integer k such that $22r + 18s = 2k$.

Example 3 – *Solution*

cont'd

Solution:

a. Let n = 10. Then 10 = 5 + 5 = 3 + 7 and 3, 5, and 7 are all prime numbers.

b. Let $k = 11r + 9s$.

Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra.

Proving Existential Statements

A **non-constructive proof of existence** involves showing either that :

(a) the existence of a value of *x* that makes *Q*(*x*) true is guaranteed by an axiom or a previously proved theorem, or

(b) the assumption that there is no such *x* leads to a contradiction.

The disadvantage of a non-constructive proof is that it may give virtually no clue about where or how *x* may be found. Thus, constructive proofs are preferred.

Disproving Universal Statements by Counterexample

Disproving Universal Statements by Counterexample

To disprove a statement means to show that it is false.

Consider the question of disproving a statement of the form

$\forall x$ in D, if $P(x)$ then $Q(x)$.

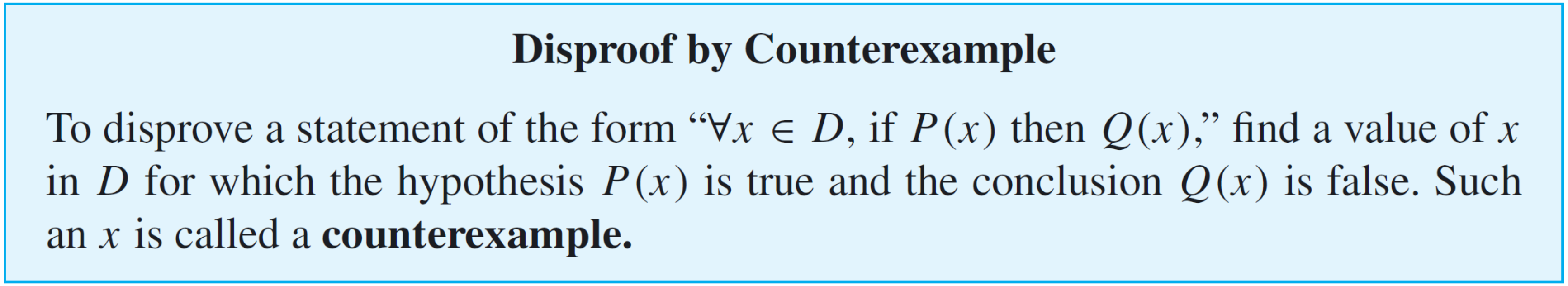
Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

$\exists\, x$ in D such that $P(x)$ and not $Q(x)$.

Disproving Universal Statements by Counterexample

But to show that an existential statement is true, we generally give an example, and because the example is used to show that the original statement is false, we call it a *counterexample*.

Thus the method of *disproof by counterexample* can be written as follows:



Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample.**

Example 4 – *Disproof by Counterexample*

Disprove the following statement by finding a counterexample:

∀ real numbers a and b, if $a^2 = b^2$ then $a = b$.

Solution:

To disprove this statement, you need to find real numbers a and b such that the hypothesis $a^2 = b^2$ is true and the conclusion $a = b$ is false.

The fact that both positive and negative integers have positive squares helps in the search.

If you flip through some possibilities in your mind, you will quickly see that 1 and –1 will work (or 2 and –2, or 0.5 and –0.5, and so forth).

Proving Universal Statements

Proving Universal Statements

The vast majority of mathematical statements to be proved are universal. In discussing how to prove such statements, it is helpful to imagine them in a standard form:

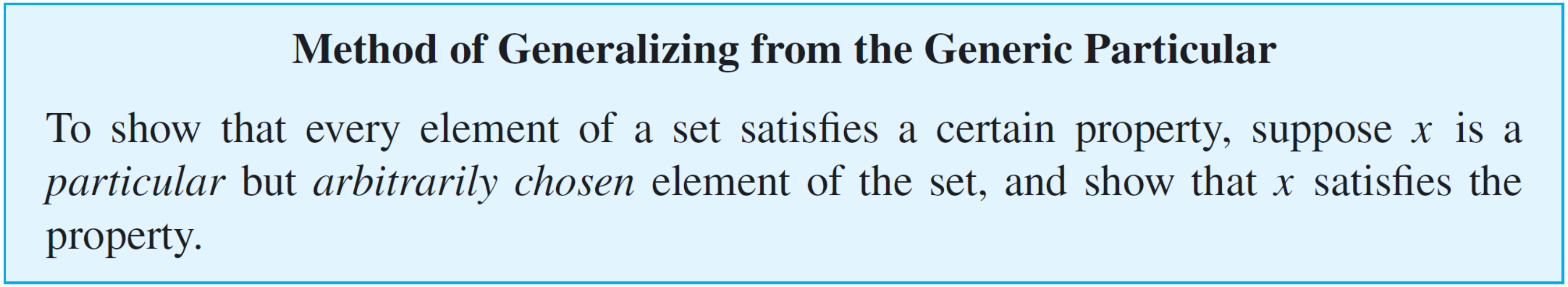
$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

Note. When *D* is finite or when only a finite number of elements satisfy *P*(*x*), such a statement can be proved by the method of exhaustion.

Proving Universal Statements

The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified.

It is called the *method of generalizing from the generic particular*. Here is the idea underlying the method:



Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Example 6 – *Generalizing from the Generic Particular*

At some time you may have been shown a “mathematical trick” like the following.

You ask a person to pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number.

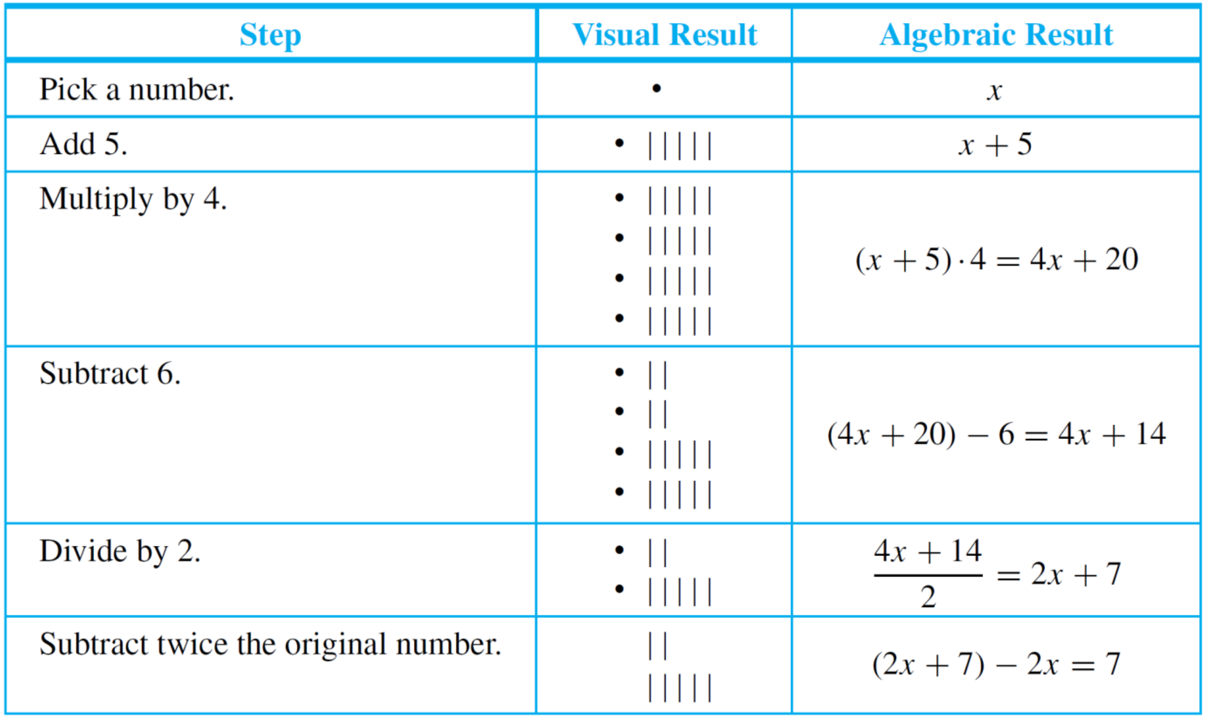
Then you astound the person by announcing that their final result was 7. How does this “trick” work?

Example 6 – *Generalizing from the Generic Particular*

cont’ d

Let an empty box • or the symbol *x* stand for the number the person picks.

Here is what happens when the person follows your directions:



Step	Visual Result	Algebraic Result
Pick a number.	•	x
Add 5.	• |||||	$x + 5$
Multiply by 4.	• ||||| • ||||| • ||||| • |||||	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	• || • || • ||||| • |||||	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	• || • |||||	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	|| |||||	$(2x + 7) - 2x = 7$

Example 6 – *Generalizing from the Generic Particular* cont’d

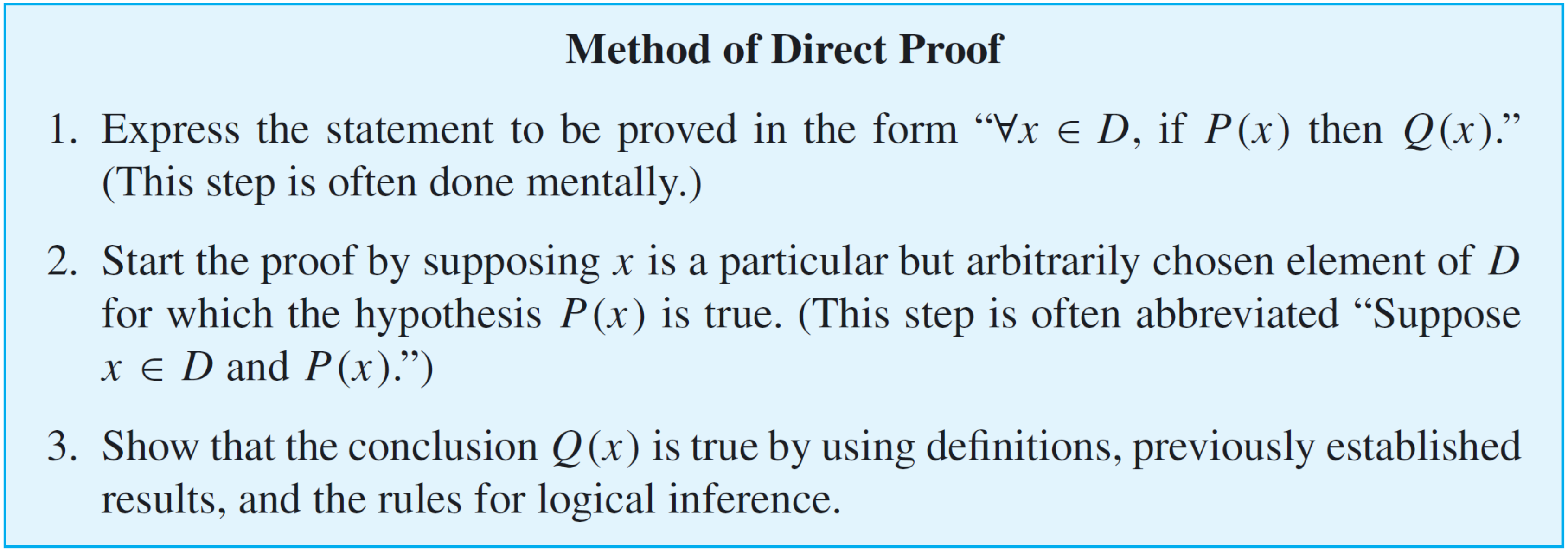
Thus no matter what number the person starts with, the result will always be 7.

Note that the *x* in the analysis above is *particular* (because it represents a single quantity), but it is also *arbitrarily chosen* or *generic* (because any number whatsoever can be put in its place).

This illustrates the process of drawing a general conclusion from a particular but generic object.

Proving Universal Statements

When the method of generalizing from the generic particular is applied to a property of the form "If $P(x)$ then $Q(x)$," the result is the method of *direct proof*.



Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example 7 – *A Direct Proof of a Theorem*

Theorem. The sum of any two even integers is even.

Direct Proof:

Whenever you are presented with a statement to be proved, it is a good idea to ask yourself whether you believe it to be true.

In this case you might imagine some pairs of even integers, say 2 + 4, 6 + 10, 12 + 12, 28 + 54, and mentally check that their sums are even.

Example 7 – *Solution*

cont' d

To prove this statement in general: we need to show that no matter what even integers are given, their sum is even.

It is possible to represent two even numbers as $2r$ and $2s$ for some integers r and s. By the distributive law of algebra;

$$2r + 2s = 2(r + s),$$

which is even. Thus the statement is true in general.

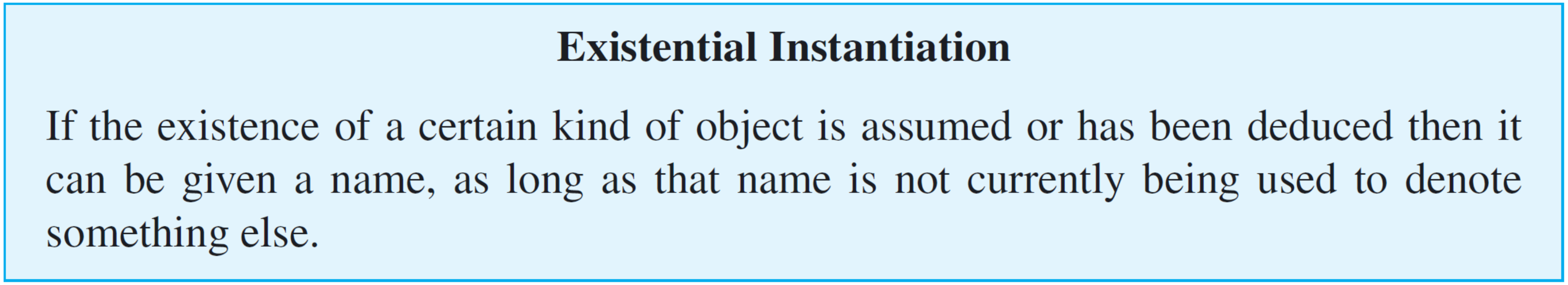
Example 7 – *Solution*

cont’d

Remark

One of the basic laws of logic, called *existential instantiation*, says that if you know something exists, you can give it a name.

However, you cannot use the same name to refer to two different things, both of which are currently under discussion.



Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced then it can be given a name, as long as that name is not currently being used to denote something else.

Showing That an Existential Statement Is False

Showing That an Existential Statement Is False

We have known that the negation of an existential statement is universal.

It follows that to prove an existential statement is false, you must prove a universal statement (its negation) is true.

Example 9 – *Disproving an Existential Statement*

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Solution:

Proving that the given statement is false is equivalent to proving its negation is true.

The negation is

For all positive integers n, $n^2 + 3n + 2$ is not prime.

Because the negation is universal, it is proved by generalizing from the generic particular.

Example 9 – *Solution*

cont’ d

Claim: The statement “There is a positive integer *n* such that $n^2 + 3n + 2$ is prime” is false.

Proof:

Suppose *n* is any *[particular but arbitrarily chosen]* positive integer. *[We will show that* $n^2 + 3n + 2$ *is not prime.]*

We can factor $n^2 + 3n + 2$ to obtain

$$n^2 + 3n + 2 = (n + 1)(n + 2).$$

We also note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$).Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime.

Common Mistakes

Common Mistakes

The following are some of the most common mistakes people make when writing mathematical proofs.

1. **Arguing from examples.**

   Looking at examples is one of the most helpful practices a problem solver can engage in and is encouraged by all good mathematics teachers.

   However, it is a mistake to think that a general statement can be proved by showing it to be true for some special cases. A property referred to in a universal statement may be true in many instances without being true in general.

Common Mistakes

2. **Using the same letter to mean two different things.**

   Some beginning theorem provers give a new variable the same name as a previously introduced variable.

3. **Jumping to a conclusion.**

   To jump to a conclusion means to allege the truth of something without giving an adequate reason.

4. **Circular reasoning.**

   To engage in circular reasoning means to assume what is to be proved; it is a variation of jumping to a conclusion.

Common Mistakes

5. **Confusion between what is known and what is still to be shown.**

   A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable.

6. **Use of *any* rather than *some*.**

   There are a few situations in which the words *any* and *some* can be used interchangeably.

Conjecture, Proof, and Disproof

Conjecture, Proof, and Disproof

More than 350 years ago, the French mathematician Pierre de Fermat claimed that it is impossible to find positive integers x, y, z with $x^n + y^n = z^n$, if n is an integer that is at least 3. (For $n = 2$, the equation has many integer solutions, such as $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$.)

Fermat wrote his claim in the margin of a book, along with the comment "I have discovered a truly remarkable PROOF of this theorem which this margin is too small to contain."

Conjecture, Proof, and Disproof

No proof, however, was found among his papers, for what came to be known as Fermat' s last theorem. The proof was only recently released in 1994 by Andrew Wiles, and formally published in 1995, after 358 years of effort by mathematicians.

One of the oldest problems in mathematics that remains unsolved is the Goldbach conjecture.

More than 250 years ago, Christian Goldbach (1690–1764) conjectured that every even integer greater than 2 can be represented as the sum of two prime numbers.

Conjecture, Proof, and Disproof

Explicit computer-aided calculations have shown the conjecture to be true up to at least 10^{18}. But there is a huge chasm between 10^{18} and infinity.

As pointed out by James Gleick of the *New York Times*, many other plausible conjectures in number theory have proved false.

Conjecture, Proof, and Disproof

Leonhard Euler (1707–1783), for example, proposed in the eighteenth century that $a^4 + b^4 + c^4 = d^4$ had no nontrivial integer number solutions.

In other words, no three perfect fourth powers add up to another perfect fourth power. For small numbers, Euler’ s conjecture looked good.

But in 1987 a Harvard mathematician, Noam Elkies, proved it wrong. The smallest counterexample, found by Roger Frye of Thinking Machines Corporation in a long computer search, is $95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 422{,}481^4$.