Section 1.4 Mathematical Proofs

Purpose of Section: Most theorems in mathematics take the form of a conditional statement $P \Rightarrow Q$ or a biconditional $P \Leftrightarrow Q$, where the biconditional can be verified by proving both $P \Rightarrow Q$ and $P \Leftarrow Q$. In this section, we describe a variety of ways of proving $P \Rightarrow Q$ including a **direct proof**, and three variations of **proof by contradiction**, one of which is called proof by **reductio ad absurdum**

Introduction

Often one hears that a **mathematical proof** is an argument that convinces others that something is true. But mathematics is not a court of law where "beyond a reasonable doubt" is a measure of validity and so a more precise definition is required. A more formal definition of a proof is as follows:

A **proof** is a chain of reasoning using accepted rules of inference, based on a set of assumptions that lead to a conclusion.

The history of what constitutes a mathematical proof has gone through many refinements, each refinement attaining a higher level of precision or "rigor" than its predecessors.[1] Some mathematical proofs proposed by such greats as Newton and Euler[2] do not hold up to today's level of scrutiny.

As an example of a mathematical proof, consider the proposition:

For all real numbers a,b,c with $a \neq 0$, if $ax^2 + bx + c = 0$ then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

or in the language of predicate logic[3]:

$$(\forall a,b,c \in \mathbb{R})\left[a \neq 0 \text{ and } ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right]$$

[1] Although a mathematical argument must be logically precise, the American mathematician George Simmons once said, "Mathematical rigor is like clothing, it ought to suit the occasion."
[2] Euler often manipulated infinite series without regard to convergence of the series.
[3] Although theorems can be written in strict predicate logic notation, it is often more useful (as in this example) to use natural language..

The hypothesis is $ax^2+bx+c=0$ where a,b,c are real numbers with $a\neq 0$, and the conclusion is

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}\ .$$

It is important to note that in a statement of the form $P\Rightarrow Q$, we have said *nothing* about whether the hypothesis P is true, only that *if it is* true, *then* the conclusion Q is true. A proof of the solutions of the quadratic equation simply consists of writing the following equations:

$$ax^2+bc+c=0 \quad (a\neq 0)$$

$$x^2+\frac{b}{a}x=-\frac{c}{a} \quad \left(\text{divide by } a \text{ and transpose a term}\right)$$

$$x^2+\frac{b}{a}x+\left(\frac{b}{2a}\right)^2=\left(\frac{b}{2a}\right)^2-\frac{c}{a} \quad \left(\text{add } \left(\frac{b}{2a}\right)^2 \text{ to each side}\right)$$

$$\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2} \quad \left(\text{complete the square on the left}\right)$$

$$x+\frac{b}{2a}=\pm\frac{\sqrt{b^2-4ac}}{2a} \quad \left(\text{take the square root}\right)$$

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a} \quad \left(\text{isolate } x \text{ and simplify}\right)$$

Is this proof convincing, or is there something about the argument that seems lacking? You might also ask if the converse holds. That is, can you go backwards by starting with the conclusion and reproduce the quadratic equation? The answer is yes so the quadratic formula holds if and only if the solution holds.

The previous statement is an example of a mathematical theorem.

*A **theorem**[4] is a mathematical statement that can be demonstrated to be true by accepted mathematical operations and arguments, and the chain of reasoning used to demonstrate the theorem is called a **proof** of the theorem*[5].

Theorems are ultimately based on a collection of principles considered so self-evident that their truth value is taken as fact. Such accepted maxims are called **axioms**, and every area of mathematics, be it real or complex analysis, algebra, geometry, topology and even arithmetic is based on a collection of self-evident truths.

Types of Proofs

Many theorems in mathematics have the form of a conditional statement or implication $P \Rightarrow Q$, where one assumes the validity of P, then with the aid of existing mathematical facts and accepted rules of inference, arrives at Q. Although the goal is always to "go from P to Q," there is more than one way of achieving this goal. They are:

Five Equivalent Forms of the Implication	
$P \Rightarrow Q$	Direct proof
$\sim Q \Rightarrow \sim P$	Proof by contrapositive
$(P \wedge \sim Q) \Rightarrow Q$	Proof by contradicting the conclusion
$(P \wedge \sim Q) \Rightarrow \sim P$	Proof by contradicting the hypothesis
$(P \wedge \sim Q) \Rightarrow (R \wedge \sim R)$	Proof by *reductio ad absurdum*

Five ways to prove $P \Rightarrow Q$

Table 1

Note that the five columns numbered (4) through (8) in Table 2 contain the same truth values of TFTT, which verifies the equivalence of these five forms of the basic implication.

		(1)	(2)	(3)
P	Q	$\sim P$	$\sim Q$	$P \wedge \sim Q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	T	F

[4] The Hungarian mathematician Paul Erdos (1913-1996) once said that a mathematician is a machine for converting coffee into theorems.

[5] Keep in mind that there may be more than one proof of a theorem. There are over 200 independent proofs of the Pythagorean Theorem.

(4)	(5)	(6)	(7)	(8)
$P \Rightarrow Q$	$\sim Q \Rightarrow \sim P$	$(P \wedge \sim Q) \Rightarrow Q$	$(P \wedge \sim Q) \Rightarrow \sim P$	$(P \wedge \sim Q) \Rightarrow (R \wedge \sim R)$
T	T	T	T	T
F	F	F	F	F
T	T	T	T	T
T	T	T	T	T

Five equivalent sentences for implication
Table 2

In this and the next section we will demonstrate different methods of proof. Before presenting some theorems and proofs we begin by stating a few definitions. Definitions are very important in mathematics since they give precise meaning to mathematical concepts.

Primes, Composites, Even and Odd Natural Numbers

Prime number: A prime number is a natural number $n \in \mathbb{N}$ greater than 1 that is divisible only by 1 and itself. In the language of predicate logic, a natural number p is prime if and only if

$$(\forall n \in \mathbb{N})\left[n \mid p \Rightarrow \left[(n = 1) \vee (n = p) \right] \right]$$

A natural number $n \in \mathbb{N}$ is **composite** if it greater than 1 and not prime. In the language of predicate logic, a natural number $n \in \mathbb{N}$ is **composite** if and only if

$$(\exists k \in \mathbb{N}, k \neq 1, n)(k \mid n)$$

Odd integer: A natural number $n \in \mathbb{N}$ is an **odd integer** if it is not divisible by 2. In the language of predicate logic, a natural number $n \in \mathbb{N}$ is odd if and only if

$$(\exists k \in \mathbb{N})(n = 2k + 1)$$

Even integer: A natural number $n \in \mathbb{N}$ is an **even integer** if it is divisible by 2, In the language of predicate logic, a natural number $n \in \mathbb{N}$ is even if

$$(\exists k \in \mathbb{N})(n = 2k)$$

Proof in Experimental Sciences: Experimental sciences (as in .biology, physics, chemistry,…) use laboratory experiments to *prove* results, which are then verified by repeated experimentation. Most of these experimental sciences are not based on fundamental axioms as they are in mathematics, the net result being that over time more sophisticated experiments often change accepted beliefs. In mathematics, which is based on fundamental axioms and definitions, what was proven true 2000 years ago is just as valid today.

Analysis of Proof Techniques

▪ **Direct Proofs** $[P \Rightarrow Q]$ A direct proof starts with an assumption P, then uses existing accepted facts and rules of inference to establish the truth of the conclusion Q.

Indirect proofs[6] refer to proof by contrapositive or proof by contradiction.

• **Proof by Contrapositive** $[\sim Q \Rightarrow \sim P]$ Here, one assumes the conclusion Q false, then proves the hypothesis P is false.

• **Proofs by Contradiction** The two proofs by contradiction have the form

$$(P \wedge \sim Q) \Rightarrow \sim P$$
$$(P \wedge \sim Q) \Rightarrow Q$$

In each case, one assumes the hypotheses P to be true and the conclusion Q false and then arrives at a contradiction. In the first case contradicting the assumption P, whereas in the second case contradicting the denial $\sim Q$. Proof by contradiction[7] is a common method of proof.

▪ ***Reductio ad absurdum***

$$\left[(P \wedge \sim Q) \Rightarrow (R \wedge \sim R)\right]$$

This is another form of proof by contradiction. Here, one assumes P is true and Q false, and then seeks to prove some kind of contradiction[8] (like $1 = 0$ or $x^2 < 0$), which we denote by $R \wedge \sim R$.

Modus Operandi for Proving Theorems

Before you get into the nitty-gritty of proving a theorem, the following steps are always useful, maybe crucial.

1. Be sure you understand the terms and expressions in the theorem.
2. Ask yourself if you believe the theorem is true or false.

[6] The formal name for an indirect proof is m*odus tollens* (Latin for "mode that denies").
[7] The English mathematician, G. H. Hardy, said proof by contradiction is one of the finest weapons in the mathematician's arsenal.

[8] Hence the name *reductio ad absurdum* (reduction to the absurd).

3. Write the theorem in the language of first-order logic so you understand the logical structure of the theorem.
4. Determine how the proof should proceed; i.e. should you use a direct proof, proof by contrapositive, or one of the proofs by contradiction.
5. Start the proof.

Theorem 1: Direct Proof If n is an odd natural number, then n^2 is odd.

Proof: Direct Proof Since $n \in \mathbb{N}$ is odd it can be written in the form $n = 2k+1$ for some integer $k \in \mathbb{Z}$. Squaring both sides of this equation yields

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Since $k \in \mathbb{Z}$ is an integer so is $2k^2 + 2k$. Hence, n^2 has the form of an odd integer. ∎

Lemmas and Corollaries: In addition to theorems there are lemmas and corollaries. Although theorems, lemmas and corollaries are similar from a logical point of view, it is how they are used and their importance that distinguishes them.

A **lemma** is a statement that is proven as an aid in proving a theorem. Often, unimportant details are put in a lemma so as not to clutter a theorem. Occasionally, lemmas take on a life of their own and become as or more important then the theorem they supported (i.e. Zorn's lemma, Burnside's lemma, Urysohn's lemma, ...)

A **corollary** is a statement that follows easily from a theorem and whose results are generally secondary to the theorem. Often it easily follows from the theorem, and doesn't require a proof of its own. The statement: "if a, b are the sides of a right isosceles triangle, then the hypotenuse has length $c = \sqrt{2}\, a$ " is a simple corollary of the Pythagorean theorem.

Someone once remarked, we plant the lemmas, grow the theorems, and harvest the corollaries.

Historical Note: The American logician Charles Saunders Pierce (1839-1914) introduced **second-order logic**, which in addition to quantifying variables like $x, y, \ldots$ also quantifies functions and entire sets of variables. However, for mathematics, first-order logic is adequate. Pierce also developed first-order logic on his own, but Frege carried out his research earlier and is generally given credit its development. It was Pierce who coined the word "first-order" logic.

Theorem 2: Proof by Contapositive

$$(\forall n \in \mathbb{N})\left(n^2 \text{ even} \Rightarrow n \text{ even}\right)$$

Proof:

Since its more natural to start with n rather than n^2, we try a proof by contrapositive, where we assume the conclusion false and prove the assumption false. Hence, we assume n is odd and prove n^2 odd. But we proved this result in Theorem 1, hence the proof is complete.

Important Note: Note the important equivalences of the conditional

$$\sim(P \Rightarrow Q) \equiv \sim(\sim P \vee Q) \equiv (P \wedge \sim Q).$$

Theorem 3: Proof by Contrapositive

If $a, b \in \mathbb{N}$, then

$$(a+b \geq 15) \Rightarrow \left[(a \geq 8) \vee (b \geq 8)\right].$$

Proof: The contrapositive form of this implication is

$$\sim\left[(a \geq 8) \vee (b \geq 8)\right] \Rightarrow \sim(a+b \geq 15)$$

Using one of De Morgan's laws, the above implication becomes

$$\left[(a < 8) \wedge (b < 8)\right] \Rightarrow (a+b < 15)$$

But $a < 8$ and $b < 8$ implies $a \leq 7$ and $b \leq 7$, which gives the desired result $a+b \leq 14 < 15$. ∎

There is no magic bullet for proving theorems. Sometimes the result to be proven provides the starting point, and the theorem can be proven by working backwards. The following theorem provides a good example when this strategy can be carried out.

Theorem 4 Backwards Proof

Prove for any two positive real numbers x and y, the algebraic mean is greater than or equal to the geometric mean. That is

$$\frac{x+y}{2} \geq \sqrt{xy}$$

Proof:

This result is a prime example of "working backwards." We begin by writing the conclusion as

$$x+y \geq 2\sqrt{xy}$$

or

$$x+y-2\sqrt{x}\sqrt{y} \geq 0$$

and factoring gives

$$\left(\sqrt{x}-\sqrt{y}\right)^2 \geq 0.$$

But this statement is true so to prove the desired result, we simply carry out the above steps in reverse order. ∎

Important Note: A **conjecture** is a mathematical statement which is believed to be true but has not been proven. Once proven it is called a theorem. The **Goldbach conjecture** is one of the oldest unsolved problems in mathematics, which claims that every even integer greater than 2 can be written as the sum of two (not necessarily distinct) primes. For example

$$4=2+2,\ \ 6=3+3,\ \ 8=3+5,\ 10=3+7=5+5,...$$

and so on. There are many conjectures in number theory, including Legendre's Conjecture (unsolved as of 2015) which claims there exists a prime number between n^2 and $(n+1)^2$ for all natural numbers n (check out some yourself). The Poincare Conjecture[9], was proved by Russian mathematician Grigori Perelman in 2002, should be retired from conjecture status and be called Poincare's Theorem, but will probably keep its original name as a conjecture.

Important Note: *Not* Mathematical Proofs:

- The proof is so easy we'll skip it.
- Don't be stupid, of course it's true!
- It's true because I *said* it's true!
- scribble, scribble QED
- God let it be true!
- I have this gut feeling.
- I did it last night.
- It works for 2 and 3.

[9] Every simply-connected, closed 3-manifold is homeomorphic to the 3-sphere.

- I *define* it to be true!
- Sounds good to me.
- All in favor … ?
- My boyfriend said it/s true.

Although we suspect readers of this book would never be guilty of applying one of the aforementioned proof techniques, there is one habit, however, almost equally heinous that is often used and that's the overuse of the word "obvious." If something is so "obvious," then go ahead a prove it.

Fundamental Theorem of Arithmetic

The **Fundamental Theorem of Arithmetic** states that any natural number greater than 1 can be uniquely factored as the product of prime numbers. For example

$$21 = 3 \times 7$$

$$40 = 2^3 \times 5$$

$$180 = 2^2 \times 3^2 \times 5$$

$$235 = 5 \times 47$$

$$453,569,345 = 5 \times 773 \times 117,353$$

We might think of the prime numbers of as the building blocks for the natural numbers.

The Prime Number Theorem (PNT) We now prove there are an infinite number of prime numbers, a proof that goes back to 300 B.C to the Greek mathematician Euclid of Alexandra (present day Egypt). Although Euclid proved the theorem by *reductio ad absurdum*, the German mathematician Dirichet (DEER-a-shlay) later developed a direct proof using analytic function theory. Before proving the prime number theorem, we use the fact that

every natural number greater than 1 is divisible by a prime number.

which is a corollary of the Fundamental Theorem of Arithmetic. We also prove this result in Section 1.6 by mathematical induction.

Theorem 5 Infinite Number of Prime Numbers There are an infinite number of prime numbers[10].

Proof: Stated in the form $P \Rightarrow Q$, the statement P defines a prime number and the conclusion Q says there are a finite number of such primes. The proof is by *reductio ab adsurdum*

$$(P \wedge \sim Q) \Rightarrow (R \wedge \sim R)$$

where we assume the conclusion false and then arrive at a contradiction. Hence, we assume there are only a finite number of prime numbers, which we enumerate in increasing order $p_1 = 2, p_2 = 3, p_3 = 5, \cdots, p_n$, where the nth prime p_n is the largest prime number. We now construct the product of the primes plus 1, or

$$\boxed{M = p_1 p_2 \cdots p_n + 1}$$

Since M is larger than the largest prime number p_n, it must be a composite number, and so it is divisible by a prime number, which we call p. (The fact any composite number is divisible by a prime is a also corollary of the Prime Number Theorem.) But the only prime numbers are $p_1, p_2, ..., p_n$ and so p must be one of them. But p can't be one of these primes since none of the primes $p_1, p_2, ..., p_n$ divide M since division M by any prime always yields a remainder of one as can be seen from the following:

$$\boxed{\begin{aligned}
\frac{p_1 p_2 \cdots p_n + 1}{p_1} &= p_2 p_3 \cdots p_n + \frac{1}{p_1} \\
\frac{p_1 p_2 \cdots p_n + 1}{p_2} &= p_1 p_3 \cdots p_n + \frac{1}{p_2} \\
\cdots \quad & \cdots \quad \cdots \\
\frac{p_1 p_2 \cdots p_n + 1}{p_n} &= p_1 p_2 \cdots p_{n-1} + \frac{1}{p_n}
\end{aligned}}$$

[10] Again, you might ask where is the assumption in this theorem? A more explicit statement of the theorem might be, if *p* is a natural number divisible only by 1 and itself, then there are an infinite number of such numbers. Often the hypothesis is implicit.

Hence, we have proven that p is both a prime number and not a prime number, so by *reductio ad absurdum*, we cannot make the claim there are only a finite number of primes. Hence, there are an infinite number of prime numbers. ∎

Euler's Proof of the PNT: Another proof that there are an infinite number of prime numbers can also be obtained from the identity

$$\left(\frac{2}{2-1}\right)\left(\frac{3}{3-1}\right)\left(\frac{5}{5-1}\right)\cdots\left(\frac{p}{p-1}\right)\cdots = \sum_{n=1}^{\infty}\frac{1}{n} = \infty$$

proved by **Leonard Euler** (1707-1783), which uses the fact that the fact that the harmonic series on the right diverges, when the product on the left is taken over prime numbers $p = 2,3,5,7,\ldots$. If there are only a finite number of prime numbers, the product on the left would be finite.

The Prime Number Theorem The next question to ask after knowing there are an infinite number of prime numbers is what proportion of the natural numbers are prime? It was observed by Karl Friedrich Gauss (1777-1856) and A. M. Legendre that although prime numbers do not occur in any regularity, the proportion of prime numbers among the first n natural numbers is approximately $1/\ln(n)$. For example, of the first million numbers the fraction of primes is $1/\ln(1,000,000) \doteq 0.07$. It took almost a hundred years after Gauss and Legendre made their conjecture for French and Belgian mathematicians Jacques Hadamard (1865-1963) and de la Vallee Poussin (1866-1962) to simultaneously and independently prove the **Prime Number Theorem** correct.

Important Note: Indirect arguments or proof by contradiction are not foreign to our psyche. They go back to our earliest days. When a parent tells a child not to do something, the child thinks the contrapositive, "If I do it, what will they do to me?"

We now come to one of the most famous theorem of antiquity, the proof of the irrationality of $\sqrt{2}$.

Theorem 6 : $\sqrt{2}$ is Irrational - Proof by Contradiction

$$\sqrt{2} \text{ is an irrational number}^{11}$$

Proof Assume the contrary, which says $\sqrt{2}$ is rational. Hence, we can write $\sqrt{2} = p/q$, where p and q are integers reduced to lowest form (i.e. canceling common factors in the numerator and denominator). Squaring both sides of this equation, gives

$$\left(\sqrt{2}\right)^2 = \left(\frac{p}{q}\right)^2 \Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2$$

which means p^2 is even. But we saw from Theorem 2 if p^2 is even so is p, hence p can be written $p = 2k$ or $p^2 = 4k^2$ where k is an integer. Hence, the above equation $p^2 = 2q^2$ can be written

$$4k^2 = 2q^2 \Rightarrow 2k^2 = q^2$$

which means q^2 is even and thus q is even. Hence, we have shown p and q are both even and hence both contain a fact of 2. But this contradicts the fact we reduced p/q to lowest terms. Hence, the assumption that $\sqrt{2} = p/q$ can be expressed as a rational number leads to a contradiction. Thus by *reductio ad absurdum,* $\sqrt{2}$ is irrational ∎

Ugh: There is the story about a student who was asked to prove a given theorem or find a counterexample. The student asked the teacher if extra credit was given for doing both.

Quicker Proof: If we *assume* the Fundamental Theorem of Arithmetic that all natural numbers can be uniquely factored as a product of prime numbers, then we can argue that the equation $p^2 = 2q^2$ cannot hold and is contradictory. The argument being there cannot be the same number of 2s on each side of the equation.

Historical Note: The reader should know the story of poor Hippasus, the Pythagorean who first proved that $\sqrt{2}$ is irrational. The Pythagoreans were a religious sect that flourished in Samos, Greece around 500 B.C. and founded by the Greek philosopher and mathematician Pythagoras. They believed that

[11] It may not be obvious but this theorem is of the form $P \Rightarrow Q$. The theorem simply says $\sqrt{2}$ is irrational so where is the "if" in the theorem? The "if" would define the square root. We generally don't say it here in the theorem since it is understood by everyone.

all numbers were either natural numbers 1,2,3,…or fractions. So when Hippasus proved $\sqrt{2}$ was *irrational*, which according to legend was made at sea, the Pythagoreans considered the proof an act of heresy and threw him overboard. So much for making one of the greatest mathematical discoveries of all time. *Of course, there is no historical proof the incident ever occurred, so you can make your own decision as to its authenticity.*

Important Note: Many important theorems in mathematics are proven by contradiction. Three of the most famous are :

- Cantor's seminal theorem: the real numbers are uncountable.
- Euclid's proof: there are an infinite number of primes. .
- Pythagoras'proof: $\sqrt{2}$ is irrational.

Tips for Proving Theorems: Here are a few guidelines that might be useful for proving theorems.

- Draw figures to visualize the concepts.
- Construct examples that illustrate the general principles.
- Try working backwards
- For "$\Rightarrow$" theorems ask if the converse "$\Leftarrow$" is true.
- Modify the theorem to make it easier.
- Generalize, does the theorem hold in more general cases.
- Did you actually *use* all the assumptions?

Necessary and Sufficient Conditions (NASC)

Often in mathematics you hear the phrase, *it is necessary but not sufficient,* such as when your calculus professor says having a zero derivative is necessary when a function has a maximum value. (A zero derivative is not sufficient for a maximum value.) Necessary and sufficient conditions are important for the progress of science. Conditions that are only necessary are simply properties that must be true for a theory to be true. What a scientist really seeks are sufficient properties.

Historical Note: When Newton found the derivative (which he called the **fluxion**) of x^2 (which he called the **fluent**), he arrived at the expression $2x+\Delta x$. The Δx was referred to as an "infinitely small" quantity and thus omitted, giving the derivative (or fluxion) of $2x$. It wasn't until a hundred

years later when mathematicians in the 19th century, such as Cauchy, Dedekind, Cantor and Weierstrass, put mathematics on a more solid logical footing, and the old mathematical expressions like "*infinitely small*" were laid to rest, replaced by "limits" and "$\varepsilon-\delta$ arguments."

This discussion motives logical statements of the form $P \Leftrightarrow Q$, which means "P is true if and only if Q is true", and stated as P is a necessary and sufficient condition for Q. Since we have the logical equivalence

$$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (P \Leftarrow Q)$$

the methodology for proving theorems of this type is to prove $P \Rightarrow Q$ and $Q \Rightarrow P$. The following theorem illustrates this idea.

Theorem 7: If and Only If Let n be any natural number, then we have that

$$3 \text{ divides } n^2-1 \Leftrightarrow 3 \text{ does not divide } n.$$

Proof

$(\Rightarrow)$ We first prove.

$3 \text{ divides } n^2-1 \Rightarrow 3 \text{ does not divide } n$:

Since 3 is a prime number and divides $n^2-1=(n-1)(n+1)$ it must divide $n-1$ or $n+1$. If 3 divides $n-1$, it cannot divide n (it will have a remainder of 1), and if 3 divides $n+1$ it cannot divide n (it will have a remainder of 2). Hence 3 does not divide n.

$(\Leftarrow)$ We now prove the other way that

$$3 \text{ divides } n^2-1 \Leftarrow 3 \text{ does not divide } n:$$

If 3 does not divide n, we can write

$$\frac{n}{3}=q+\frac{r}{3}$$

or $n=3q+r$, where the remainder r is either 1 or 2. If $r=1$ then $n-1=3q$ which means 3 divides $(n-1)(n+1)=n^2-1$. If $r=2$ then $n-2=3q$ or $n+1=3q+3=3(q+1)$, which also means 3 divides $n^2-1=(n-1)(n+1)$ ∎

Who Has Proven the Stronger Theorem?
Jerry and Susan have each proven an important theorem with the same conclusion *C,* and each hopes to win a *Fields Medal*.[12] But although their conclusions are the same, their hypotheses are different. Jerry has assumed a hypothesis J so his theorem has the form $J \Rightarrow C$, whereas Susan has assumed a hypothesis S, so her theorem has the form $S \Rightarrow C$. In their battle to see who has the stronger theorem (which theorem implies the other), Jerry makes the discovery that his hypothesis J is *sufficient* for Susan's hypothesis S. That is, $J \Rightarrow S$ and hence he claims his theorem is the stronger theorem. Is Jerry correct? The answer is no! Susan's weaker hypothesis means she has the stronger theorem as can be seen by the implication

$$(J \Rightarrow S) \Rightarrow \left[(S \Rightarrow C) \Rightarrow (J \Rightarrow C) \right]$$

The validity of this tautology is left to the reader.

Sometimes a lemma is used as a helper to help prove a more important theorem.
.

Lemma Every natural number n can be written in the form $n = s + 3m$, where s is the sum of the digits of n and m is some natural number. For example, $675 = 18 + 3(219)$.

Proof: Writing n as

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + 10a_1 + a_0$$

and the sum of its digits by $s = a_0 + a_1 + \cdots + a_k$, the difference is

$$\begin{aligned} n - s &= \left(a_k 10^k + a_{k-1} 10^{k-1} + \cdots + 10a_1 + a_0 \right) - \left(a_k + a_{k-1} + \cdots + a_0 \right) \\ &= 999...9a_k + \cdots + 99a_2 + 9a_1 \\ &= 3\left(333...3a_k + \cdots + 33a_2 + 3a_1 \right) \\ &= 3m \end{aligned}$$

which proves the lemma. . ∎

We now use the lemma to prove the following theorem.

Theorem 8: If and only If

---

[12] The Fields Medal is regarded as the "Nobel Prize" of mathematics, awarded every four years to one or more outstanding researchers under the age of forty.

$$(\forall n \in \mathbb{N})\left[(3 \mid n) \Leftrightarrow (3 \mid \text{ sum of the digits of } n)\right]$$

Proof: $(\Rightarrow)$ If 3 divides n we can write $n = 3k$, where k is a natural number. Then using Lemma 1 we have $3k = s + 3m$ and solving for the sum s gives

$$s = 3k - 3m = 3(k - m)$$

which proves that the sum of the digits of n is divisible by 3.

$(\Leftarrow)$ Assuming 3 divides the sum of the digits of n, we write $s = 3k$, where k is a natural number. Appealing to the lemma, we have

$$n = s + 3m = 3k + 3m = 3(k + m)$$

which proves n is divisible by 3. ∎

Corollary: 3 divides 9031827540918.

Note: Mathematical rigor refers to the "degree of logical precision" in mathematics and like most things, rigor can be carried to extremes. Over preciseness tends to dampen the imagination rather than produce a glimpse into the beauty of mathematics. On the other hand, too little rigor leads to careless thinking and a degeneration of what is correct until reaching a state of nonsense. Rigor changes with time. Much of what was mathematically rigorous 200 years ago are considered defective today. It might be said that mathematicians use "sufficient" rigor for the standards of the time.

Problems

1. **Direct Proof** Prove the following by a direct proof. Feel free to use at your disposal the properties of number systems already introduced, algebraic laws, laws of logic, and so on. Just do not use laws like "it's obvious, the law of skipping the details," and similar laws.

a) The sum of two even integers is even.
b) The sum of an even an odd integer is odd.
c) If a divides b, and b divides c, then a divides c.
d) The product of two consecutive natural numbers plus the larger number is a perfect square.
e) Every odd integer n greater than 1 can be written as the difference between two perfect squares. Give examples.

f) If n is an even positive integer, then n is the difference of two positive integer squares if and only if $n = 4k$ for some integer $k > 1$.

g) If a, b are real numbers, then $a^2 + b^2 \geq 2ab$.
h) The sum of two rational numbers is rational.

i) Let $p(x)$ be a polynomial where E is the sum of the coefficients of the even powers, and O is the sum of the coefficients of the odd powers. Show that $E + O = p(1)$ and $E - O = p(-1)$.

2. **Divisibility by 4** Show that a natural number is divisible by 4 if and only if its last two digits are divisible by 4. For example both 256 and 56 are divisible by 4. The same holds for 3459567820964 and 64.

3. **Divisibility by 3** Show that a natural number is divisible by 3 if and only if the sum of its digits is divisible by 3. For example, the number 9003186 is divisible by 3.

4. **Proof by Contradiction** Prove the following by contradiction.

a) If n is an integer and $5n + 2$ is even, then n is even.

b) If m and n are integers and $m + n$ is even, then m and n have the same parity (i.e. both are even or both are odd).

c) If m and n are integers and mn is even, then either m or n is even.

d) If I is an irrational number and R is a rational number, then $I + R$ is irrational.

5. **Divisibility Problem** Prove the following theorems for integers m, n.

a) 5 divides $n^4 - 1$ if and only if 5 does not divide n.
b) $9 \mid n$ if and only if 9 divides the sum of the digits of n.
c) mn is even if and only if at least one of m, n is even.

6. **Counterexamples** A counterexample[13] is a special kind of example that disproves a statement or proposition. Counterexamples are used in mathematics to probe the boundaries of a given result. Find counterexamples for the following faulty theorems and tell how you could add new hypothesis to make the claim valid.

a) If $a > b$ then $|a| > |b|$.

[13] A nice reference book for any mathematician is *Counterexamples in Mathematics* by Bernard Geldbaum and John Olmsted, Springer-Verlag (1990).

b) If $(a-b)^2=(m-n)^2$ then $a-b=m-n$.

c) If x and y are real numbers, then $\sqrt{xy}=\sqrt{x}\sqrt{y}$.

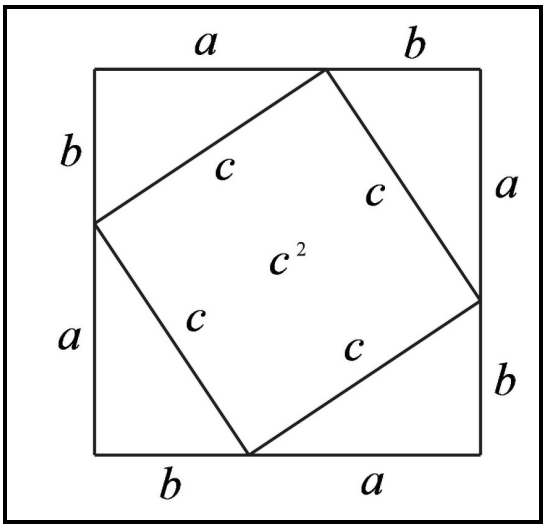
d) If f is a continuous function defined on $[a,b]$, then there exists a $c\in(a,b)$ such that

e)

$$f'(c)=\frac{f(b)-f(a)}{b-a}$$

7. **Valid Proof – Invalid Conclusion** If the assumption of a theorem is false, then the conclusion can be false even if the proof of the theorem is valid. For example, if you assume there exists a largest positive integer *N,* it is possible to prove $N=1$. Can you find such a proof?

8. **Pythagorean Theorem** Prove the Pythagorean theorem that states if a,b,c are the sides of a right triangle where c is the hypotenuse, then $a^2+b^2=c^2$. Use the diagram in Figure 1 to prove the Pythagorean theorem.



Visual proof of the Pythagorean theorem
Figure 1

9. **Comparing Theorems** Verify the statement

$$(J\Rightarrow S)\Rightarrow\big[(S\Rightarrow C)\Rightarrow(J\Rightarrow C)\big]$$

showing if $J\Rightarrow S$, then $J\Rightarrow C$ is the weaker theorem.

10. **Comparing Theorems** Verify that theorem $J \Rightarrow C_1$ is stronger (implies) than theorem $J \Rightarrow C_2$ if conclusion C_1 is stronger than conclusion C_2. In other words, show that

$$(C_1 \Rightarrow C_2) \Rightarrow \left[(J \Rightarrow C_1) \Rightarrow (J \Rightarrow C_2) \right]$$

is a tautology.

11. **Hmmmmmmmm** Infinite decimal expansions are sometimes needed to represent certain fractions. Prove that $1/3 = 0.333....$ by writing the decimal form 0.333... as the infinite series

$$0.333\ldots = \frac{3}{10} + \frac{3}{100} + \frac{3}{1000} + \cdots$$

and showing the sum of this series is $1/3$. .

12. **Analysis of the Structure of Proofs** There is a theorem in topology that states that a compact set of real numbers is both closed and bounded. Use one of DeMorgan's laws to state the contrapositive form of this theorem.

13. **Another Irrational Number** Prove that $\log_{10} 3$ is irrational.

14. **Not Proofs** The following are not considered valid proofs by most mathematicians. Maybe the reader knows of a few other ones.

a) Proof by obviousness: *Too trivial to prove.*
b) Proof by plausibility: *It sounds good, so it must be true.*
c) *Proof by intimidation: Don't* be stupid; of course it's true!
d) Proof by definition: *I define it to be true.*
e) Proof by tautology: *It's true because it's true.*
f) Proof by majority rule: *Everyone I know says it's true.*
g) Proof by divine words: A*nd the Lord said, 'Let it be true' and it was true.*
h) Proof by generalization*: It works for me, that's enough.*
i) Proof by hope: *Please, let it be true*.
j) Proof by intuition: *I got this gut feeling.*

15. **Just a Little Common Sense** You are given a column of 100 ten-digit numbers and after adding them you get an answer of 2437507464567. Is your answer correct?

16**. Syllogisms** The Greek philosopher Plato is recognized as the first person associated with the concept a logical argument. His arguments took the form of

two premises followed by a conclusion. This basic logical form is called a **syllogism**, the most famous being the "Socrates syllogism":

- **First premise:** *All men are mortal,*
- **Second premise:** *Socrates is a man,*
- **Conclusion:** *Therefore, Socrates is mortal.*

which has the general form

First premise: All M is R
Second premise: All S is M

Conclusion: All S is R

where

M = "being a man"
S = "being Socrates"
R = "being mortal"

are called the **subject** and **predicate** of the syllogism, and M is called the **middle term** of the syllogism.

Plato classified each premise and conclusion as one of the four basic types[14]:

E Every A is B (example: Every dog has a tail)
S Some A is B (example: Some dogs have black hair)
N No A is B (example: No dog has orange hair)
SN Some A are not B (example: Some dogs are not poodles)

which means each of the first and second premise and conclusion can be one of four types which means there are a total of $4\times4\times4=64$ possible syllogisms, some logically true, some false. For example, a syllogism of type NEN means the first premise is of type N (No A is B), the second premise of type E (Every A is B) above, and the conclusion of type N (No A is B). Which of the following syllogism types are valid and which are invalid? Draw Venn diagrams to illustrate A and B to support your conclusion.

a) NEN Ans: true
b) ESS Ans: true
c) NSSn Ans: true
d) SSS Ans: false
e) EES Ans: false
f) SES Ans: false

[14] We use A and B to denote the properties S, P, and M.

17. **Euler's Totient Function** Euler's totient function, denoted by $\phi(n)$, gives the number of natural numbers less than a given number n, including 1, that are relatively prime to n, where two numbers are relatively prime if their greatest common divisor is 1. For example $\phi(p) = p-1$ for any prime number since $1, 2, 3, ..., p-1$ are all relatively prime with p. On the other hand $\phi(12) = 4$ since 1, 5, 7, and 11 are relatively prime with 12. Prove that for a power of a prime number $p^k, k = 1, 2, ...$ the Euler totient function is $\phi(p^k) = p^{k-1}(p-1)$ by proving the following results.

a) Find the number of natural numbers strictly between 1 and p^k that are not relatively prime with p^k; i.e. divide p^k.

b) Subtract the result from a) from $p^k - 1$ to obtain $\phi\left(p^k\right)$

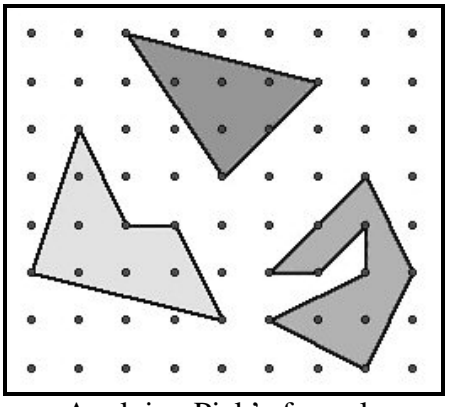
18. **Pick's Amazing Formula** In 1899 an Austrian mathematician, Georg Pick devised a fastinating formula for finding the area A inside a simple polygon whose vertices lie on grid points (m, n) where m and n are integers. The formula he came up with was

$$A = \frac{B}{2} + I - 1$$

where B is the number of vertices that lie on the boundary, and I is the number of vertices that lie on the interior.

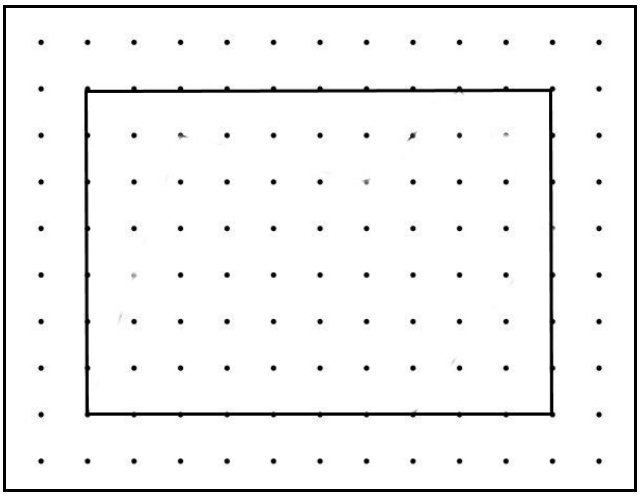
a) Verify that Pick's formula yields an area of 1 for a simple square bounded by four adjacent vertices.

b) Use Pick's formula to find the area inside the polygons in Figure 2.



Applying Pick's formula
Figure 2

c) Prove that Pick's formula yields the correct the area of mn inside a rectangle with m rows and n columns. We draw a $m=8$ by $n=11$ rectangle in Figure 3 for illustration



The area of mn inside an $m \times n$ rectangle
Figure 3

ΓΣΘΨΞΠΩ