Section 1.5 Proofs in Predicate Logic

Purpose of Section: To continue our discussion of mathematical proofs by focusing on theorems of the form $(\forall x \in U)P(x)$, $(\exists x \in U)P(x)$ as well as theorems with multiple quantifiers, such as $(\forall x \in U)(\exists y \in V)P(x, y)$.

Introduction

Most theorems in mathematics begin with quantifiers like "for all" or "there exists," or maybe a more involved version "for all *x*, there exists a *y*", although often not stated explicitly since the quantification is understood. Euclid's famous theorem about prime numbers is often stated simply as "there are an infinite number of prime numbers," begs the question, where's the "if" in the theorem? The answer is the assumption is the definition of a prime number. In this section we will always include the all-important quantifiers and prove theorems stated in the language of predicate logic.

Proofs Involving Quantifiers

Since many theorems in mathematics are stated in the form $(\forall x \in U)P(x)$ or $(\exists x \in U)P(x)$, the question we ask is how do we go about proving them. We begin by proving theorems which include a single universal quantifier.

Universal Quantifier: To prove a theorem of the form

$$(\forall x \in U)P(x)$$

one selects an *arbitrary* $x \in U$, then proves the assertion $P(x)$ is true.

Theorem 1: Universal Direct Proof All integers divisible by 6 are even.

Proof: Stated in the language of predicate logic, we have

$$(\forall n \in \mathbb{Z})(6|n \Rightarrow n \text{ is even})$$

Since n is assumed divisible by 6, there exists an integer m that satisfies $n = 6m$, which can be rewritten as $n = 2(3m) = 2k$, where $k = 3m$. Hence, n is an even integer. We could streamline this argument symbolically as

$$(6 | n) \Rightarrow (\exists m \in \mathbb{Z})(n = 6m = 2(3m))$$ ∎

Note: We could also prove Theorem 1 by contrapositive proving

$$(\forall n \in \mathbb{Z})[n \text{ is odd } \Rightarrow (6 \nmid n)]$$

where $6 \nmid n$ means 6 does *not* divide n.

Counterexample To prove a theorem containing a universal quantifier is false, one only needs to find a counterexample; i.e. an example where the theorem is invalid. At one time there was a conjecture in number theory by Fermat that stated

$$(\forall n \in \mathbb{N})\left(2^{2^n}+1 \text{ is a prime number}\right)$$

until Leonard Euler disproved the result with the embarrassing observation that for $n=5$

$$2^{2^5}+1=2^{32}+1=4294967297=641\times 6700417$$

which is sufficient to show the theorem invalid. In other words, the person proved the *negation* of the theorem

$$(\exists n \in \mathbb{N})\left(2^{2^n} \text{ is not prime}\right)3$$

Proofs involving the existential quantifier $\exists$ are often easier than ones involving universal quantifiers $\forall$ since it is only necessary to find one element in the universe that satisfies the given proposition.

Existential Sentences: To prove a theorem of the form

$$(\exists x \in U)\, P(x)$$

find one (or more) element $x \in U$ that satisfies $P(x)$.

Simply because we only have to find one object that satisfies the given condition, does not automatically mean the theorem is easy to prove. There are many unsolved conjectures related to finding just one (or more) thing. For example, a perfect number is a natural number that is equal to the sum of its proper divisors,[1] such as $6=1+2+3$, $28=1+2+4+7+14,...$ At the present time, it is unknown if there are any *odd* perfect numbers. The largest perfect number currently known (in 2011) is

$$\left(2^{2976220}\right)\left(2^{2976221}-1\right)$$

and contains 1,791,864 digits.

[1] The proper divisors of a number are the numbers that divide the number other than the number itself. For example, the proper divisors of 6 are 1,2, and 3. The proper divisors of 28 are 1, 2, 4, 7, and 14.

Theorem 2: Proof by Demonstration Show there exists an even prime number.

Proof: One should never use the word trivial in mathematics, but in this case it is. The number 2 is both even and prime. ▌

Intuitionism: In the philosophy of mathematics, there is a school of thought, called ***Intuitionism*** proposed by the Dutch mathematician L.E.J. Brouwer (1881-1961) with advocates as the German mathematician Leopold Kronecker (1823-1891). Intuitionists (or constructionists) feel that mathematics is purely the result of the constructive mental activity of humans, in contrast to discovering basic concepts existing outside of human existence. Kronecker once said, "*God made the integers, all else is the work of man.*" In the late 1800s and early 1900s several intuitionists felt that the new theories like Cantor's infinite sets, imaginary numbers, proof by contradiction and non-euclidean geometries were taking mathematics down the road to mysticism. Even the great French mathematician Henri Poincare (1854-1912) felt that Cantor's theory of infinite sets and transfinite arithmetic should be excluded from mathematics. Today, the intuitionist school of mathematics is not held in favor among many mathematicians.

Theorem 3: Use of the Law of the Excluded Middle[2] There exists irrational numbers a,b such that a^b is rational. In the language of predicate logic, if we call I the set of irrational numbers, we would write

$$(\exists a,b \in I)\left(a^b \in \mathbb{Q}\right)$$

Proof

One hesitates to call a proof "cute," but this one is strange to say the least. Consider the number

$$\sqrt{2}^{\sqrt{2}}$$

which is either rational or irrational. We consider each case.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is *rational*, then the proof is complete since we pick the irrational numbers as $a = b = \sqrt{2}$.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is *irrational,* then

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$

so we can pick

$$a = \sqrt{2}^{\sqrt{2}},\ b = \sqrt{2}$$ ▌

[2] The *Law of the Excluded Middle* states the accepted logical principle that every proposition is either true or false, unlike the weatherperson who says, rain, no rain, or maybe.

Do you accept this proof? We have not identified which pair a, b make a^b rational, but either

$$a = b = \sqrt{2} \quad \text{or} \quad a = \sqrt{2}^{\sqrt{2}},\ b = \sqrt{2}\,.$$

make a^b. Strange considering the fact we don't know if $\sqrt{2}^{\sqrt{2}}$ is rational or irrational.

Proofs by Contradiction for Quantifiers

Proofs by contradiction are important tools in a mathematician's toolkit.

Proof of $(\forall x)P(x)$ by Contradiction:
To prove a theorem of the form $(\forall x)P(x)$ by contradiction, assume the contrary, i.e. $(\exists x)[\sim P(x)]$, and arrive at a contradiction, thus proving one can't assume the contrary.

Theorem 4: Proof by Contradiction

If m, n are integers, then $14m + 21n \neq 1$, or :

$$(\forall m, n \in \mathbb{Z})(14m + 21n \neq 1)$$

Proof: Assume the proposition is false. That is

$$(\exists m, n \in \mathbb{Z})(14m + 21n = 1)$$

But this equation obviously[3] cannot hold since 7 divides the left side of the equation but not the right side. Hence, the denial of the theorem is false, so the theorem is true. ∎

Important Note: If a theorem is true for thousands of cases that doesn't prove the theorem. The equation

$$(n-1)(n-2)\cdots(n-1{,}000{,}000) = 0$$

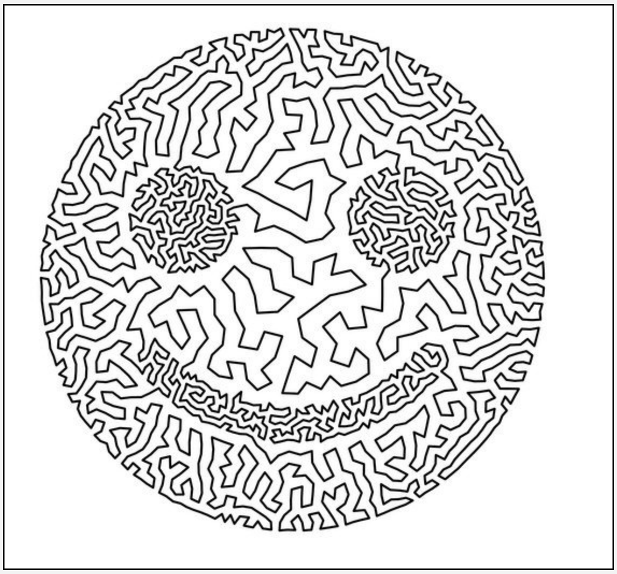
has a solution for $n = 1, 2, \ldots, 1{,}000{,}000$, but doesn't have a solution for $n = 1{,}000{,}001$.

Historical Note: Frege's 1879 seminal work *Begriffsschrift* ("Conceptual Notation") marked the beginning of a new era in logic, which allowed for the quantification of mathematical variables, just in time for the more precise

[3] There is the story about a professor who pointed to an ominous looking equation on the board and after scratching his head for fifteen minutes, said at last, "Aha, it's obvious!"

arithmetization of analysis of calculus, being carried out in the late 1800s by mathematicians like the German Karl Weierstrass (1815-1897).

Important Note: Some theorems seem obvious but are incredibly difficult to prove. One such theorem is the **Jordan Curve Theorem**, which states that every simple continuous closed curve in the plane divides the plane into three disjoint parts: an "inside" of the curve, an "outside" of the curve, and the curve itself. The theorem was first posed by German mathematician Bernard Bolzano (1781-1848) and the first person to present a proof was French mathematician Camille Jordan (1838-1922) in 1882. However, his proof was judged unsatisfactory and in 1905 it was the American geometer Oswald Veblen (1880-1960) who gave the first accepted proof. One hundred years later in 2005 an international team of mathematicians using a formal computer checking system called *Mizar* generated a 6,500 line proof of the theorem.



Can you find the inside and outside of this Jordan curve?[4]

Some theorems contain both universal and existential quantifiers. The following theorem is an example.

Unending Interesting Properties of Numbers

Is the number 10008036000540 a multiple of 9? The answer is yes and if you know a certain theorem, you can answer the question in about 5 seconds. To

[4] We thank Robert Bosch of the Dept of Mathematics at Oberlin College for the use of this image.

prove this result, one must make the observation that 10 = 9 + 1. Here is the theorem stated in the language of predicate logic.

Theorem 5: Interesting Property of Numbers (casting out 9s)

$$(\forall n \in \mathbb{N})(9 \mid n \Leftrightarrow 9 \mid \text{sum of the digits of } n)$$

Semi-Proof: Sometimes proofs are easy conceptually but the arithmetic or algebra becomes messy. This problem is such an example. We prove the result for a two-digit number and let you prove it for a 3-digit number. See Problem 9.

$(\Rightarrow)$ We assume $9 \mid d_1d_2$ which implies $d_1d_2 = 9k$ for some $k \in \mathbb{N}$, which further implies:

starting with $d_1d_2 = 9k$
hence $10 \times d_1 + d_2 = 9k$
hence $(9+1)d_1 + d_2 = 9k$
hence $d_1 + d_2 = 9k - 9d_1 = 9(k - d_1) = 9k_1$ where $k_1 = k - d_1 \in \mathbb{N}$

Hence, the sum of the digits, $d_1 + d_2$, is a multiple of 9.

$(\Leftarrow)$ Assuming the sum of the digits a multiple of 9, we can write

starting with $d_1 + d_2 = 9k$
hence $d_1 + d_2 = 9k + (9d_1 - 9d_1)$
hence $10d_1 + d_2 = 9k + 9d_1 = 9(k + d_1)$
hence $d_1d_2 = 9k_1$

where $k_1 = k + d_1$, which proves the result.

In general, to determine if a large number is a multiple of 9, one sums the digits to get a new number. If it is not immediately known if the new number is a multiple of 9, sum the digits again, and again. If the end product of all this is 9, then the answer is yes, otherwise no. Try a few numbers yourself.

It is also possible to prove theorems involving the existential quantifier by contradiction.

Proof of $(\exists x)P(x)$ by Contradiction:

To prove $(\exists x)P(x)$ by contradiction, assume the contrary $(\forall x)[\sim P(x)]$, then continue until you reach a contradiction of some kind. A more common statement involving $\exists$ is a statement of the form $(\sim \exists x)P(x)$. To prove this proposition by contradiction, one assumes $(\exists x)P(x)$ and arrives at the contradiction.

Theorem 6: No largest even integer

There is no largest even integer.

Proof: Assume there is a largest even integer we call n, and it is even we write $n = 2k$ for some $k \in \mathbb{Z}$. Now consider $n+2$, which we can write as

$$n+2 = 2k+2 = 2(k+1)$$

But this says $n+2$ is an even integer greater than n, which contradicts the claim that n is the largest even integer. Hence, we cannot claim there is a largest even integer. ∎

Unique Existential Quantification $\exists!$

A special type of existential quantifier is the **unique existential quantification**

Proving Unique Existential Theorems: A theorem of the form

$$(\exists! x \in U)P(x)$$

with an *exclamation point* ! after the $\exists$ states "*there exists a unique element* x *such that* $P(x)$ *is true,*" the emphases being on unique. To prove a theorem of this form, we must show $P(x)$ is true for exactly one element of the universe. A common strategy is to first show $P(x)$ is true for *some* $x \in U$, then if $P(x)$ is true for another element $y \in U$, then $x = y$.

The concept of uniqueness is important in mathematics. For many problems the first step is to first show existence, and the second step is to show uniqueness.

Theorem 7: Uniqueness : Diophantine Equation

There exist unique natural numbers m and n that satisfy

$$m^2 - n^2 - 12$$

or

$$(\exists! m \in \mathbb{N})(\exists! n \in \mathbb{N})(m^2 - n^2 = 12) .$$

.

Proof: An equation that only allows integer solutions is called a **Diophantine equation**. We begin by factoring

$$m^2 - n^2 = (m+n)(m-n) = 12$$

and note that the difference between the factors is $2n$, which implies that both factors must be even or both must be odd. But the only factors of 12 that meets this requirement is $12 = 2 \times 6$. Hence, we are left with

$$m+n=6$$
$$m-n=2$$

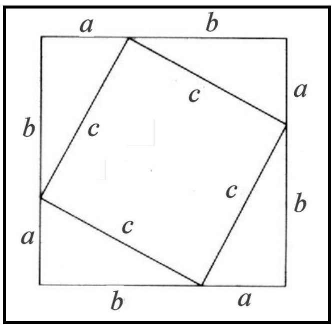
which has solution $m=4, n=2$. ▌

Historical Note: In the late 1800s and early 1900s, there was a shift in the philosophy of mathematics: from thinking that logic was simply a tool for mathematics, to thinking that logic was the foundation or precursor of mathematics. This thesis, called the "logistic thesis" (or "Frege-Russell thesis") contends that mathematics is but an extension of logic, as described in Russell and Whitehead's seminal work, ***Principia Mathematica***. To others, such as Giuseppe Peano, symbolic logic is only a tool of mathematics, which is probably the philosophy of most mathematicians today.

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

Theorem 8: Proof by Pictures

Does the drawing in Figure 1 constitute a proof of the Pythagorean Theorem $a^2+b^2=c^2$ for a right triangle with legs having length a, b and a hypotenuse of length c? Some people say yes, some say no, but the best way to think about "visual" proofs is that they provide an idea that can be turned into a valid logical proofs.



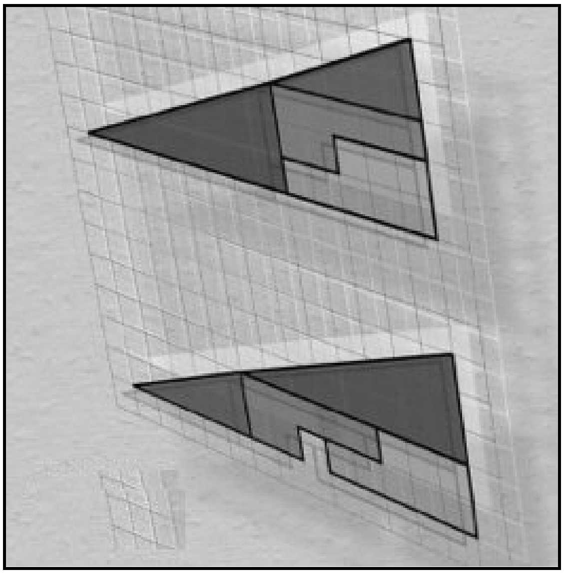
Visual proof of the Pythagorean theorem
Figure 1

Proof by Picture:

Setting the area of the large square equal to the sum of the areas of the four triangles plus the area of the smaller square yields

$$(a+b)^2 = 2ab + c^2 \Rightarrow a^2 + b^2 = c^2$$ ▌

Caution: One must be cautious in accepting "proof by picture" arguments. Look at the following visual "proof" that demonstrates you can create space from nothing[5]. To find out the flaw in the picture, google "Curry paradox."



Curry paradox

Important Note: A great mathematical proof is one that is distinguished by beauty and economy. There are some proofs that get the job done but do not lift ones' intellectual spirit. On the other hand, some proofs overwhelm one with creative and novel insights. You might grade the proofs in this section according to those principles.

Problems

1. **True or False?** Which of the following are true?

a) $(\forall x \in \mathbb{R})(x^2 + x + 1 > 0)$ Ans: T

b) $(\forall x \in \mathbb{R})[x^2 > 0 \vee x^2 < 0]$ Ans: F

[5] This drawing was taken from the cover of *Paradoxes in Mathematics* by Jerry Farlow, Dover Publications, 2014.

c) $(\forall x \in \mathbb{Z})(x^2 > x)$ Ans: F

d) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y = \sin x)$

e) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y = \tan x)$

f) $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(y = \sin x)$

g) $(\exists x, y \in \mathbb{N})(\exists n > 2)(x^n + y^n = 1)$

h) $(\exists x \in \mathbb{R})(\forall a,b,c \in \mathbb{R})(ax^2 + bx + c = 0)$

i) $(\exists x \in \mathbb{C})(\forall a,b,c \in \mathbb{R})(ax^2 + bx + c = 0)$

j) $(\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall n > N)\left(\frac{1}{n} < \varepsilon\right)$

k) $(\forall \varepsilon > 0)(\exists \delta > 0)\left(|x-2| < \delta \Rightarrow |x^2 - 4| < \varepsilon\right)$

2. **Predicate Logic Form** Write the following theorems in the language of predicate logic.

a) A number is divisible by 4 if and only if its last two digits are divisible by 4.

b) A natural number is divisible by 2^n if and only if its last n digits are divisible by 2^n.

c) There exists irrational numbers x, y such that x^y is rational.

d) $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

e) For positive real numbers a, b, we have $\sqrt{ab} \le \frac{a+b}{2}$.

f) If a, b are integers and $b \neq 0$, then there exists unique integers q, r such that $a = qb + r$ where $0 \le r < |b|$.

g) If p is a prime number that does not divide an integer a, then p divides $a^p - a$.

h) The square of any natural number has each prime factor occurring an even number of times in its the prime factorization.

i) All prime numbers p greater than 2 are of the form either $p = 2n+1$ or $p = 2n+3$ for some natural number n.

j) Every even number greater than 4 can be expressed as the sum of two prime numbers.

k) **Euler's Conjecture**: There are no natural numbers a,b,c,d that satisfy $a^4 + b^4 + c^4 = d^4$.

3. **Negation** Negate the following theorems, and tell whether the original statement or the negation is true. Let x and y be real variables.

a) $(\exists x)(\forall y)(xy < 1)$
b) $(\forall x)(\forall y)(\exists z)(xyz = 1)$
c) $(\forall x)(\forall y)(\forall z)(\exists w)(x^2 + y^2 + z^2 + w^2 = 0)$
d) $\sim(\exists x)(\forall y)(x < y)$
e) $(\forall x)(\exists y)(xy < 1 \wedge xy > 1)$
f) $(\exists x)(\exists y)(xy = 0 \vee xy \neq 0)$

4. **Counterexamples** All the following statements are wrong. Prove them wrong by finding a counterexample[6].

a) All mathematicians make tons of money writing textbooks.
b) For all positive integers n, $n^2 + n + 41$ is prime [7].
c) Every continuous function defined on the interval (0,1) has a maximum and minimum value.
d) Every continuous function is differentiable.
e) If the terms of an infinite series approach zero, then the series converges.
f) The perimeter of a rectangle can never be an odd integer.
g) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x = y^2)$
h) Every even natural number is the sum of two primes.
i) If m and n are positive integers such that m divides $n^2 - 1$, then m divides $n-1$ or m divides $n+1$.
j) If $\{f_n : n = 1, 2, ...\}$ is a sequence of continuous functions defined on $(0,1)$ that converge to a function f, then f is continuous.

5. **If and Only If Theorems** State each of the following theorems in the language of predicate logic. Take the function f to be a real- valued function of a real variable.

---

[6] A nice book outlining many counterexamples in mathematics is *Counterexamples in Mathematics* by Bernard R. Gelbaum and John Olmsted (Holden Day, Inc), 1964.

[7] A famous mathematician once said that he was once x^2 years old in the year x. Can you determine the year this person was born?

a) A function f is even if and only if for every real number x we have $f(x) = f(-x)$.

b) A function f is odd if and only if for every real number x we have $f(x) = -f(-x)$.

c) A function f is periodic if and only if there exists a real number p such that $f(x) = f(x+p)$ for all real numbers x.

d) A function is increasing if and only if for every real numbers x and y we have $x \le y \Rightarrow f(x) \le f(y)$.

e) A function f is continuous at x_0 if and only if for any $\varepsilon > 0$ there exists a $\delta > 0$ such that

$$\left|x - x_0\right| < \delta \Rightarrow \left|f(x) - f(x_0)\right| < \varepsilon \quad .$$

f) A function f is uniformly continuous on a set E if and only if for any $\varepsilon > 0$ there exists a $\delta > 0$ such that $\left|f(x) - f(y)\right| < \varepsilon$ for any x, y in E that satisfy $\left|x - y\right| < \delta$.

6. **Hard or Easy?** Prove that if there is a real number $a \in \mathbb{R}$ that satisfies $a^3 + a + 1 = 0$, then there is a real number $b \in \mathbb{R}$ that satisfies $b^3 + b - 1 = 0$. This problem is either very hard or very easy. It is your job to determine which is true.

7. **Predicate Logic in Analysis** The so-called $\varepsilon - \delta$ proofs in analysis were originated by the German mathematician Carl Weierstrass in the 1800s. They involve inequalities and universal and existential quantifiers. They often start with $(\forall \varepsilon > 0)$ followed by $(\exists \delta > 0)$. The idea is that your adversary can pick $\varepsilon > 0$ as small as one pleases, but you have the advantage of picking the δ second. Of course, your choice of δ will most likely depend on ε.

a) Show that for every real number $\varepsilon > 0$ there exists a real number $\delta > 0$ such that $2\delta < \varepsilon$. In the language of predicate logic, prove

$$(\forall \varepsilon > 0)(\exists \delta > 0)(2\delta < \varepsilon).$$

b) For every real number $\varepsilon > 0$, there exists an integer $N > 0$ such that for $n > N$ one has $1/n < \varepsilon$. In the language of predicate logic, prove

$$(\forall \varepsilon > 0)(\exists N > 0)(\forall n > N)(1/n < \varepsilon).$$

c) Show that for every real number $\varepsilon > 0$, there exists a real number $\delta > 0$ such that if $|x| < \delta$ then $x^2 < \varepsilon$. In the language of predicate logic, prove

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in \mathbb{R})\left(|x| < \delta \Rightarrow x^2 < \varepsilon\right)$$

.

d) Show that for every positive integer M there is a positive integer N such that

$$x > N \Rightarrow \sqrt{x} > M .$$

In the language of predicate logic, prove

$$(\forall M > 0)(\exists N > 0)(\forall x \in \mathbb{R})\left(x > N \Rightarrow \sqrt{x} > M\right).$$

8. **Doing Mathematics** Textbooks sometimes lead one to believe theorems appear out of thin air for mathematicians to prove. If this were so, mathematics would be a purely deductive science, but in fact "doing mathematics" and mathematical research is as much an inductive science as deductive. Table 2 below lists the number of divisors $\tau(n)$ of n for the first 24 natural numbers. Looking at the table, can you think of questions to ask about the number of divisors of the natural numbers? A couple of candidates are

Theorem 1: $\tau(n)$ is odd if and only if n is a square, like 4, 9, 16, ...

Theorem 2: If m and n have no common factor, then $\tau(m)\tau(n) = \tau(mn)$.

n	$\tau(n)$		n	$\tau(n)$
1	1		13	2
2	2		14	4
3	2		15	4
4	3		16	5
5	2		17	2
6	4		18	6
7	2		19	2
8	4		20	6
9	3		21	4
10	4		22	4
11	2		23	2
12	6		24	8

Divisors of a few natural numbers
Table 2

9. **Casting Out 9's** Show that if the number $d_1d_2d_3$ is a multiple of 9 if and only if $d_1 + d_2 + d_3$ is a multiple of 9.

ΓΣΘΨΞΠΩ