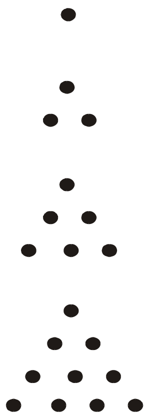
The Number of Primes: Limitless

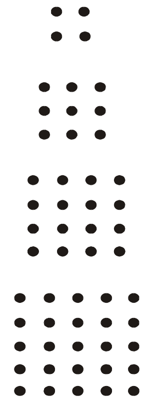
by James D. Nickel



Triangular Numbers

The ancient Greeks, being devoted to Geometry, loved to picture numbers. To them, *form* and *number* were inseparable. Triangular numbers could be represented with pebbles. The first eight triangular numbers are 1, 3, 6, 10, 15, 21, 28, 36. The list of triangular numbers continues, *ad infinitum.* They also noted that if you take the sum of any two sequential triangular numbers, you get another number that the Greeks called square numbers, another list that continues *ad infinitum.*

$1 + 3 = 4 = 2^2$
$3 + 6 = 9 = 3^2$
$6 + 10 = 16 = 4^2$
$10 + 15 = 25 = 5^2$
$15 + 21 = 36 = 6^2$
etc.



Square Numbers

Like the Greeks, we can identify patterns in the set of counting numbers in many ways. For example:

The set of odd numbers: {1, 3, 5, 7, 9, …}
The set of even numbers (or the set of numbers divisible by 2): {2, 4, 6, 8, 10, …}
The set of numbers divisible by 3: {3, 6, 9, 12, 15, …}
The set of numbers divisible by 4: {4, 8, 12, 16, …}
The set of triangular numbers: {1, 3, 6, 10, 15, 21, 28, …}
The set of square numbers: {1, 4, 9, 16, 25, 36, 49, …}

There exists a set of numbers contained within the natural or counting numbers that has defied all attempts to explicate a discernible pattern. In order to define these numbers we must first recall what is meant by determining the factors (or divisors) of a number.

The factors of 2 are: 1, 2.
The factors of 3 are: 1, 3.
The factors of 4 are: 1, 2, 4.
The factors of 5 are: 1, 5.
The factors of 6 are: 1, 2, 3, 6.
The factors of 7 are: 1, 7.
The factors of 8 are: 1, 2, 4, 8.
The factors of 9 are: 1, 3, 9.
The factors of 10 are: 1, 2, 5, 10.
The factors of 11 are: 1, 11.
The factors of 12 are: 1, 2, 3, 4, 6, 12.

Note: This essay is extracted from a Lesson from the forthcoming textbook *Mathematics: Building on Foundations*.

Note that *every* number is divisible by itself and 1. Note also (from the list above) that there are *some* numbers that are *not* divisible by any other number except itself and 1. The ancient Greeks called these numbers *linear numbers*. Today we call them *prime numbers*.[1] In the list above, 2, 3, 5, 7, and 11 are prime numbers.

The number 1 is the "odd man out" in these considerations since its only factor is 1. Because of this, 1 is not considered to be a prime number. Therefore, the first prime number is 2. Note that this number is

[1] The Greeks could not picture linear numbers as an array of either square or rectangular dots (one dot was always left over). Prime means "first in excellence, degree, or rank."

also the *only even prime number*. Why? Every even number is divisible by itself and 1 but *every even number is also divisible by 2*. Therefore, every even number has more factors other than itself and 1.

What makes prime numbers special is that they form the "building blocks" of every other number. That is, every number that is not a prime number can be "built" out of prime numbers. Therefore, these numbers are called composite numbers.[2] Every composite number (note, we are also excluding the number 1 from this consideration) can be rewritten as a *unique* product of prime numbers. This statement is known as the *Fundamental Theorem of Arithmetic* and its proof requires the use of pristine logic. For example, 99, a composite number, can be written as a *unique* product of primes in this fashion: $99 = 3 \cdot 3 \cdot 11$.

One problem that the Greeks considered was whether or not the number of primes (2, 3, 5, 7, 11, etc.) is *infinite* or *finite*.

The proof that the number of primes is *infinite* (i.e., the list of prime numbers continues, *ad infinitum*) is attributed, historically, to Euclid (ca. 300 BC), the Greek geometer, who also investigated the rudiments of number theory. Euclid's reasoning is regarded as a classical model of logical clarity and elegance. *It is one of the most beautiful proofs in mathematics.*

Euclid commenced his proof by assuming that there is a largest prime number (or, that the number of primes in *finite*). He then employed a logical methodology, called *indirect proof*, that is often used by mathematicians to justify the truth of a proposition. Indirect proof is also called proof by *reductio ad absurdum* or a reduction to an absurdity. It is the refutation of a proposition by demonstrating the inevitably absurd conclusion to which it logically leads.

Here is how this reasoning works.

Step 1. Let P = a proposition that you want to prove true.
Step 2. Assume ~P (the proposition is false).
Step 3. We reason from ~P to Q, a statement that is false and nonsensical (i.e., a contradiction; in symbols, we write $\rightarrow\leftarrow$ to represent this contradiction).
Step 4. Since $\sim P \rightarrow Q$, then, by the logical law of contraposition, $\sim Q \rightarrow P$. In other words, ~Q requires, by logical necessity, that P is true!

Not all mathematicians abide by this method of proof. These mathematicians are called *intuitionists* and they believe that mathematical proof must be entirely based upon man's intuition; i.e., man must "see" it "in an instant" if it is to be true. In other words, for an intuitionist, man must be God or see all things "instantly and completely." The ability to "intuit" (to see the truth of some things in an instant) is a gift from God. It is a moment of God's knowledge given to man by God's common grace. However, just because you cannot "intuit" something does not mean it is not true. The ability to "intuit" is never to be absolutized (take the place of God who is the only absolute). Likewise, the ability to reason is never to be absolutized. Reason is a gift from God to be used by man to order or systematize the created realm.

Back to Euclid's reasoning, we state what we want to prove. We let P be the proposition that "the number of primes is infinite." Now, we assume ~P and see where this assumption logically leads.

If ~P is true, then there is a largest prime number. We let p_n = largest prime number. Hence, we can list the number of primes where p_n is the largest prime. We let $W = \{p_1, p_2, p_3, p_4, p_5, \ldots, p_n\}$.

Now, let's create a number N by multiplying all of these prime numbers together and then add 1 to the product:

$$N = p_1 p_2 p_3 p_4 p_5 \ldots p_n + 1$$

Consider the nature of N. We know that N is greater that each of the primes in W. Hence, $N > p_n$, our assumed largest prime number. Since p_n is the largest prime number, then N *cannot* be a prime number.

[2] Composite means "made up of distinct components."

Hence, N is a composite number. By the Fundamental Theorem of Arithmetic, N can be factored into some of the prime numbers in our list. But, if we try to divide N by any of these prime numbers, p_1, p_2, p_3, p_4, p_5, …, p_n, *we will always get a remainder of 1*. Why? We add 1 to their product. Thus, N is *not* divisible by any of the primes we listed. We let Q be the proposition that "N is *not* divisible by any of the primes we listed." What conclusion can we draw from Q? If Q is true, then:

Conclusion 1: N is itself prime (and *not* listed in W).
Conclusion 2: N must have among its factors some new prime (or primes) *not* listed in W.

Either conclusion leads us to a contradiction because we assumed that W lists *all* the primes. Therefore, our assumption has led us to a logical absurdity ($\rightarrow\leftarrow$). $\sim P \rightarrow Q$ and Q is false and nonsensical. Since $\sim P \rightarrow Q$, then, by the logical law of contraposition, $\sim Q \rightarrow P$. In other words, our assumption is untenable and there is no largest prime number; i.e., the number of primes is *infinite*.

Note, in this proof, *no actual prime numbers were used*. Our list of primes, W, was purely symbolic. All we needed in our storehouse of knowledge was the nature of divisibility and the Fundamental Theorem of Arithmetic. This bears repeating: *we did not need to list any of the prime numbers to prove that the number of primes is infinite*. This is one reason why mathematical proofs like this are viewed by mathematicians as beautiful. In this proof, using logic and a few previously established truths, we were able to prove a proposition related to infinity. From finite starting points, we were able confidently explore the realm of the infinite. Take time to let this analysis suitably impact your thinking … it is truly marvelous.

In conclusion, let's illustrate our result with some actual numbers. Let W = {2, 3, 5, 7} where 7 is the largest prime number. Hence, $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. 211 is a prime number and not included in W. Now, let W = {3, 5, 7}. Hence, $N = 3 \cdot 5 \cdot 7 + 1 = 106$. 106, in this example, is a composite number; i.e., $106 = 2 \cdot 53$. By this reasoning, we have generated two new primes: 211 and 53.

Since 53 is a prime number, we can now let W = {2, 3, 5, 7, 53}. Hence, $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 53 + 1 = 11,131$, a prime number. Like a mathematical "chain reaction," this reasoning can be continued *ad infinitum* resulting in the revelation that there is no limit to the number of primes!