Number Theory # 1

From the very beginning of mathematics, people have been interested in the mysterious objects known as prime numbers. Although at first they can seem so simple, there are many seemingly simple problems about them that have remained unsolved for hundreds of years.

DEFINITION Prime Number

A prime number is a positive integer that has exactly two positive divisors, 1 and itself.

The first 10 prime numbers are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

EXERCISE 1 List the next 10 prime numbers.

Solution: 31, 37, 41, 43, 47, 53, 59, 61, 67, 71

How did you figure these out? There are numerous different methods for doing this. The most basic one is trial and error. That is, take the next number x and determine if it is divisible by any prime number less than or equal to $\sqrt{x}$.

A better method for determining all prime numbers from 2 to a given number n is the **Sieve of Erastothenes**.

Algorithm

1. Make a list of all integers 2 to n.
2. Circle the first number in the list that has not been crossed out.
3. Cross out all multiples of this number from the list.
4. Repeat steps 2 to 4 until all numbers are crossed out or circled.
5. The circled numbers are all the primes from 2 to n.

EXERCISE 2 Use the Sieve to find all prime numbers from 2 to 196. (handout)

Notice that the Sieve is relying on the fact that every integer greater than 1 is either a prime number or a composite number. Let us now prove that this is true.

THEOREM 1 Every integer greater than 1 is a prime number or a product of prime numbers.

Proof: Suppose that the result is false. Then there exists some numbers that are not prime and cannot be written as a product of prime numbers. Let n be the smallest such number. Since n is not prime, that means it has two positive divisors other than 1 and itself. Say $n = rs$. But, since r and s are smaller than n, they must either be prime or can be written as a product of prime numbers. But this means that n can also be written as a product of prime numbers. This contradicts our assumption. Hence, the result is true. $\square$

What do we call a positive integer that is not prime? This is actually a bit of a trick question. A positive integer greater than 1 that is not prime is called **composite**. What about 1? The number 1 is very special and is called a **unit**.

We can in fact prove a very important result that is slightly stronger.

THEOREM 2 **Fundamental Theorem of Arithmetic**
Every integer greater than 1 is either prime or can be written as a unique product (up to order) of prime numbers.

EXAMPLE 1 For the first few numbers we have

$$
\begin{aligned}
2 &\quad \text{prime} \\
3 &\quad \text{prime} \\
4 &= 2 \times 2 \\
5 &\quad \text{prime} \\
6 &= 2 \times 3 \\
7 &\quad \text{prime} \\
8 &= 2^3 \\
9 &= 3^2 \\
10 &= 2 \times 5 \\
11 &\quad \text{prime} \\
12 &= 2^2 \times 3
\end{aligned}
$$

The product of prime numbers which makes up a number is called the **prime factorization** of the number. Recall, to find the prime factorization of a number we often use a factor tree to help us.

EXAMPLE 2 Find the prime factorization of 1000.

Solution: We have $1000 = 40 \times 25 = (8 \times 5) \times (5 \times 5) = 2^3 \times 5^3$.

EXERCISE 3 Find the prime factorization for the following numbers: 210, 4725, 10!

Solution: $210 = 2 \times 3 \times 5 \times 7$

$4725 = 3^3 \times 5^2 \times 7$

$10! = 2^8 \times 3^4 \times 5^2 \times 7$

We will look a little more at prime factorizations next class.

The Number of Primes

A natural question to ask is if there is a largest prime number. Does the fact that every integer larger than 1 is either prime or can be written as a product of primes indicate that there are infinitely many primes? No, it doesn't. Perhaps all very large numbers are just written as a product of lots of primes. Moreover, notice that our table of primes less than 196 seems to show that the primes numbers become less dense. For example, there are 10 primes numbers between 1 and 30, only 8 primes numbers between 150 and 190, and there are no primes between 19610 and 19660.

Despite the fact that the prime numbers do become less dense, their density never goes to 0. The most famous proof that there are infinitely many primes is found in Euclid's Elements.

THEOREM 3 There are infinitely many prime numbers.

Proof: Assume there are finitely many primes, say $p_1, p_2, \ldots, p_n$. Consider the number $p_1 \cdots p_n + 1$. This number is not on our list of primes, so it must be composite. But, it is not a multiple of any of our prime numbers either. This contradicts the fact that every integer is either prime or can be written as a product of primes. Hence, there must be infinitely many primes. $\square$

Note that the number $p_1 \cdots p_n + 1$ may be prime or composite. For example,

$2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$ is prime, but

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 59 \times 509$

Distribution of Prime Numbers

We have just proven that even though the prime numbers are becoming less dense, we can always keep finding another prime number. Some mathematicians are interested in the distance between consecutive prime numbers. We now look at the two extreme cases.

Twin Prime Conjecture

If you look at your table of primes less than 196 you will see that every once in awhile there are two primes numbers which are 2 apart. For example, 3 and 5, 71 and 73, 191 and 193 (and many more). Two primes numbers p and q are called twin primes if $p - q = 2$.

It is conjectured that there are infinitely many twin primes (called, the Twin Prime Conjecture). The largest twin primes found as of August 2009 were

$$65516468355 \times 2333333 \pm 1.$$

EXERCISE 4 List all of the twin primes less than 196.

Large Gaps

On the other hand, we also see from our table that the space between consecutive prime numbers can continue to get larger. We call the distance between two consecutive prime numbers a **prime gap**. For example, the prime gap between 11 and 13 is 2, while the prime gap between 31 and 37 is 6. The largest prime gap under 20 is 4, while there is a prime gap of size 6 from 23 to 29. The first occurrence of a prime gap of size n is called a maximal gap.

The first few maximal gaps are:

size	prime numbers
1	2, 3
2	3, 5
4	7, 11
6	23, 29

EXERCISE 5 Find the next two maximal gaps.

As we expect, we can make prime gaps arbitrarily large. We will leave the proof of this as an exercise.

An Interesting Unsolved Problem

From all this we see that, using multiplication, the prime numbers are the "building blocks" of the positive integers greater than 1. What about for addition?

EXAMPLE 3 For the first few numbers we have

$$\begin{aligned}
2 &\quad \text{prime} \\
3 &\quad \text{prime} \\
4 &= 2+2 \\
5 &\quad \text{prime} \\
6 &= 3+3 \\
7 &\quad \text{prime} \\
8 &= 3+5 \\
9 &= 2+2+5 = 3+3+3 \\
10 &= 5+5 = 3+7 \\
11 &\quad \text{prime} \\
12 &= 5+7 \\
13 &\quad \text{prime} \\
14 &= 3+11 \text{ or } 7+7
\end{aligned}$$

It has been proven that every integer greater than 4 can be written as a sum of at most seven primes. However, some mathematicians are interested in trying to prove a stronger result called Goldbach's Conjecture: "Every even integer greater than 4 can be written as a sum of two primes."

If you try many examples, you quickly see that this should be true. Moreover, you begin to see that as you choose larger numbers, there becomes multiple ways of writing the numbers as a sum of two primes (for example, 10 and 14 can be written as a sum of two primes in two ways). However, despite the overwhelming evidence we still do not know if this conjecture is true or not. It is possible that there is some very large even integer that cannot be written as a sum of two primes. If you are able to prove Goldbach's Conjecture or to find an even integer that cannot be written as a sum of two prime numbers, then you will be famous! Note that as of Nov 6, 2010 all even integers less than 2×10^{18} have already been checked!

Problems

1. Modify your Sieve to make a list all of the prime numbers from 197 to 250.

2. We define $\Omega(n)$ to be the number of prime factors of the number n. For example

$$
\begin{aligned}
\Omega(8) &= 3 \quad \text{since } 8 = 2^3 \\
\Omega(9) &= 2 \quad \text{since } 9 = 3^2 \\
\Omega(10) &= 2 \quad \text{since } 10 = 2 \times 5 \\
\Omega(11) &= 1 \quad \text{since } 11 \text{ is prime} \\
\Omega(180) &= 5 \quad \text{since } 180 = 2^2 \times 3^2 \times 5
\end{aligned}
$$

   (a) Find $\Omega(n)$ for $n = 2, \ldots, 20$.

   (b) Find $\Omega(100)$, $\Omega(400)$, and $\Omega(800)$.

   (c) Show that $\Omega(mn) = \Omega(m) + \Omega(n)$

   (d) Find $\Omega(210000)$.

   (e) Find $\Omega(20!)$.

3. For any positive integer n there is a prime gap of length at least n. [Hint: Think of how to make n numbers in a row that are all composite.]

4. Observe that 10 is the smallest even number that can be written as a sum of two prime numbers in two different ways. Find the smallest even number that can be written as a sum of two primes in three different ways and the smallest even number that can be written as a sum of two primes in four different ways.

5. Explain why if Goldbach's Conjecture is true, then every integer greater than 5 can be written as a sum of three primes.