Prime Numbers

The natural numbers, or the counting numbers, 1, 2, 3, … are the first numbers that every one encounters and learns from an early stage in our life. The first use of these numbers is in counting things. The simplest operations that we apply on natural numbers are addition, subtraction, multiplications and division. Of these operations, the division operation is of a special interest. We observe that for any given two numbers, the smaller number will either divide or will not divide the second number. For example, taking the numbers 2 and 6, we note that 2 divides 6. But when we take the numbers 3 and 10, we note that 3 does not divide 10. In fact, when we divide 10 by 3, we get a quotient of 3 and a remainder of 1. We describe the situation of these two examples by saying that 6 is divisible by 2 and 10 is not divisible by 3. We also say that 2 is a divisor or a factor of 6 and 3 is not a divisor or not a factor of 10. We note that every natural number is divisible by 1 and itself. Some natural numbers are divisible only by one and themselves, like 2 and 5. Other natural numbers are divisible by some number different from 1 and the original number itself. The number 10 is such a number. It is not only divisible by 1 and 10, but also by 2 and 5. A natural number that is divisible only by 1 and itself is called a **prime number**. If a natural number is divisible by some number different from 1 and itself, then we call this number a **composite number**. So the number 5 is a prime number since it is divisible only by 1 and 5 itself. But 10 is a composite number since it is also divisible by 2 and 5 in addition to 1 and 10.

In mathematics, it is agreed that the number 1 is neither a prime number nor a composite number. Thus, in this case, we note that every natural number, except 1, can be classified as either a prime number or a composite number. Composite numbers have a very interesting property. Each composite number can be written as a product of prime numbers. For instance, the composite number 18 can be written as $18 = 2 \times 3 \times 3$, or, using exponential notation, as $18 = 2 \times 3^2$. For another example, the composite number 120 can be written as $120 = 2^3 \times 3 \times 5$. The order in which the factors are written in the product is not important. Thus, we can write $120 = 2^3 \times 3 \times 5 = 3 \times 2^3 \times 5 = 5 \times 2^3 \times 5 = 2 \times 5 \times 2 \times 3 \times 2$ or we can use any order we like. The main thing is that in any order we choose to write the product, the same primes will appear the same number of times, or to the same exponent. Observing that the prime numbers 2 and 7 can be written in the form $2 = 2^1$ and $7 = 7^1$, we can also say that every prime number can be written as a product of prime numbers; namely, as a product of itself only. Thus, we have the following important property of natural numbers: *Except for the order of the factors, every natural number greater than 1 can be written in only one way as a product of primes*. This fact is known as **The Fundamental Theorem of Arithmetic.** This theorem tells us that the prime numbers form the building blocks of natural numbers.

Which of the natural numbers 1, 2, 3, … is a prime number? It is possible to list all prime numbers that are less than a given number. Let us illustrate how this can be done by finding all prime numbers less than 40. Ignoring 1, we start by listing all numbers less than or equal to 40:

2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,

21, 22, 23, 24, 25, 26, 27, 28, 29, 30
31, 32, 33, 34, 35, 36, 37, 38, 39, 40

The first number in the list is 2. We keep 2 underlined and delete all multiples of 2 in the list. This will give us the following list:

$\underline{2}$, 3, 5, 7, 9
11, 13, 15, 17, 19
21, 23, 25, 27, 29
31, 33, 35, 37, 39

Now the first number not underlined is 3. We keep 3 underlined and delete all multiples of 3. This will yield the following list:

$\underline{2}$, $\underline{3}$, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37 .

The first number not underlined in the above list is 5. We keep 5 underlined and delete all multiples of 5. This will give the list:

$\underline{2}$, $\underline{3}$, $\underline{5}$, 7, 11, 13, 17, 19, 23, 29, 31, 37 .

We continue the process in exactly the same way we did above. At the end, we will get all prime numbers less than 40 underlined. One can observe that the process is lengthy. In fact, one does not need to continue further than what we did above. One needs only to apply the process for all prime numbers less than $\sqrt{40}$, the square root of 40. In our example, $\sqrt{40} \approx 6.32$. The prime numbers less than 6.32 are 2, 3 and 5. So we need only delete the multiples of the primes 2, 3 and 5 from the original list we started with. The list that we will end up with will consist of all prime numbers less than or equal to 40; namely,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 .

The method we just described is a very old one. It is attributed to the Greek mathematician Eratosthenes (276-194 B. C.), the chief librarian of the famous library of Alexandria. The method is known as the **Sieve of Eratosthenes**. It is the first and oldest method used to list all the prime numbers less than a given number.

How many prime numbers are there? The answer is that there are infinitely many numbers. How did we get this answer? Did we find all prime numbers and then we observe that their number is infinite. This is impossible; for this amount to testing each natural number to see whether it is prime or not. In general, testing whether a number is prime or not is not easy especially if the number is very large. We find that the number of primes is infinite by using a mathematical proof. This mathematical proof is called *a proof by contradiction*. The main idea of a proof by contradiction can be described briefly as follows: Assume that we want to prove the validity of some mathematical statement S_1. We start by assuming the contrary; that is, we assume S_1 is false. Then we show, via logical reasoning, that this assumption leads to a new statement S_2 which is known to be false or which contradicts the assumption that S_1 is false. This means that our original assumption (that S_1 is false) is not correct.

Let us use this method of proof to show that there are infinitely many primes. We assume that there are a finite number of primes. Let us denote these primes by $p_1, p_2, p_3, ..., p_n$. We form the number $N = p_1 \times p_2 \times p_3 \times ... \times p_n + 1$. Now N is a natural number greater than 1; so N can be classified as either prime or composite. If N is prime, then it is a new prime since it is different from the only assumed primes $p_1, p_2, p_3, ..., p_n$. If N is composite, then N has to be divisible by some prime p. But p is different from the primes $p_1, p_2, p_3, ..., p_n$ since none of them divides N. This means that, in either case, we will get a new prime different from the list of primes we started with. This shows that our assumption, that there are a finite number of primes, is false. This contradiction implies that there are infinitely many primes.

How to determine whether a number is prime or not? In general, this important question is not easy to answer particularly if the number is large, say, for example, if the number consists of 200 digits. There are many tests to determine whether a number is prime or not. The oldest one states as follows: *If n is not divisible by any prime number less than $\sqrt{n}$, then n is prime*. In fact, the sieve of Eratosthenes, mentioned above, is based on this test. Let us use this test to show that 61 is prime. First, the prime numbers less than $\sqrt{61} \approx 7.81$ are 2, 3, 5 and 7. Next, none of these primes divide 61; hence 61 is a prime number. As another example, the prime numbers less than $\sqrt{101} \approx 10.04$ are 2, 3, 5 and 7. Again, none of these primes divides 101. This implies that 101 is a prime number. The non-practical side of this test is that it takes a long time if the number is large. There are more practical tests that can be used to test the primality of a given number. Some of these tests are of a general character; others are specific to certain classes of numbers.

Prime numbers are a source of interesting and challenging problems. One example is the problem of finding a general formula that gives all prime numbers. Another example is the problem that investigates the distribution of prime numbers in the set of natural numbers. Such problems, and others, helped in advancing number theory. Mathematicians tackled many problems about prime numbers. In many occasions, the main motive of these mathematicians was scientific curiosity. It was not of any concern whether the study of primes will be of any usefulness in our daily life. However, nowadays, prime numbers prove to be of utmost importance in our life. One of their important applications is their use in cryptography, the art of secret (coded) writing.

May 18, 2005 (10 Rabi-II, 1426)