# Elementary Facts About Primes

**Miliyon T.**

Abstract. Prime numbers are very important figures in number theory. They are like atom that build up a molecule by building up the integers because of the fact fundamental theorem of arithmetic. For centuries Mathematicians tried to understand prime numbers. Despite their hard work too little is known about primes. In this paper we will try to look at some of the results that have been discovered so far.

## 1. Histroy

The earliest surviving records of the explicit study of prime numbers come from the Ancient Greeks. Euclid's Elements (circa 300 BC) contain important theorems about primes, including the infinitude of primes and the fundamental theorem of arithmetic. Euclid also showed how to construct a perfect number from a Mersenne prime. The Sieve of Eratosthenes, attributed to Eratosthenes, is a simple method to compute primes.

After the Greeks, little happened with the study of prime numbers until the 17th century. In 1640 Pierre de Fermat stated Fermat's little theorem. It was proved later by Euler. Euler ever gave its generalization. Fermat also conjectured that all numbers of the form $2^{2^n} + 1$ are prime and he verified this up to $n = 4$. However, the very next Fermat number $2^{2^5} + 1$ is composite (one of its prime factors is 641), as Euler discovered later(Feramt conjectures Euler proves it!). Numbers of the form $2^{2^n} + 1$ are now called Fermat numbers. The French monk Marin Mersenne looked at primes of the form $2^p - 1$, with p a prime. They are called Mersenne primes in his honor.

Euler's work in number theory included many results about primes. Some of his major results are the divergence of the sum of the reciprocal of primes, Euler product and in 1747 he showed that the even perfect numbers are precisely the integers of the form $2^{p-1}(2^p - 1)$, where the second factor is a Mersenne prime.

At the start of the 19th century, Legendre and Gauss independently conjectured the prime number theorem. Ideas of Riemann in his 1859 paper on the zeta-function sketched a program that would lead to a proof of the prime number theorem. This

Structure in randomness of primes.

outline was completed by Hadamard and de la Valle Poussin, who independently proved the prime number theorem in 1896.

Proving a number is prime is not done (for large numbers) by trial division. Many mathematicians have worked on primality tests for large numbers, often restricted to specific number forms. This includes Ppin's test for Fermat numbers (1877), Proth's theorem (around 1878), the LucasLehmer primality test (originated 1856), and the generalized Lucas primality test. More recent algorithms like APRT-CL, ECPP, and AKS work on arbitrary numbers but remain much slower.

For a long time, prime numbers were thought to have extremely limited application outside of pure mathematics. This changed in the 1970s when the concepts of public-key cryptography were invented, in which prime numbers formed the basis of the first algorithms such as the RSA cryptosystem algorithm.

## 2. Definition and Facts

Definition 2.1. A **prime number** is a natural number greater than 1 that has no positive divisors other than 1 and itself.

Definition 2.2. If a natural number greater than 1 is not a prime, then its called **composite**.

### 2.1. Fundamental Theorem of Arithmetic.

Theorem 2.1. *Every positive integer greater than one is either prime or can be* ***uniquely*** *factored in to prime numbers.*

Proof. Either n is a prime or it is composite. In the first case there is nothing to prove. If n is composite, then there exists a prime divisor of n, as we have shown. Thus, n may be written as $n = p_1 n_1$, where $p_1$ is prime and $1 < n_1 < n$. If $n_1$ is prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number $p_2$ such that $n_1 = p_2 n_2$; that is,

$$n = p_1 p_2 n_2; 1 < n_2 < n_1 :$$

If $n_2$ is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3 n_3$, with $p_3$ a prime; hence,

$$N = p_1 \cdot p_2 \cdot p_3 \cdot n_3; 1 < n_3 < n_2 :$$

The decreasing sequence $n > n_1 > n_2 > \cdots > 1$ Cannot continue indefinitely, so that after a finite number of steps $n_k$ is a prime, say $p_k$. This leads to the prime factorization

$$n = p_1 p_2 \cdots p_k :$$

The second part of the proof the uniqueness of the prime factorization is more difficult. To this purpose let us suppose that the integer n can be represented as a product of primes in two ways; say,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s; r \leqslant s;$$

Where the $p_i$ and $q_j$ are all primes, written in increasing order, so that $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ and $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$ : Because $p_1 \mid q_1 q_2 \cdots q_s$, we know that $p_1 | q_k$ for

some value of k. Being a prime, $q_k$ has only two divisors, 1 and itself. Because $p_1$ is greater than 1, we must conclude that $p_1 = q_k$; but then it must be that $p_1 \geqslant q_1$. An entirely similar argument (starting with $q_1$ rather than $p_1$) yields $q_1 \geqslant p_1$, so that in fact $p_1 = q_1$. We can cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s :$$

Now repeat the process to get $p_2 = q_2$; cancel again, to see that

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s :$$

Continue in this fashion. If the inequality $r < s$ held, we should eventually arrive at the equation

$$1 = q_{r+1} q_{r+2} \cdots q_s;$$

Which is absurd, since each $q_i > 1$. It follows that $r = s$ and that

$$p_1 = q_1; p_2 = q_2, \cdots, p_r = q_r;$$

This makes the two factorizations of n identical. □

**Note**: It is because of this theorem that we excluded 1 from being a prime. Because if let 1 to be a prime we wouldn't get a **unique** factorization.

LEMMA 2.1 (Euclid's lemma). *Any composite number is divisible by a prime.*

PROOF. For a composite number n, there exists an integer d satisfying the conditions $d \mid n$ and $1 < d < n$. among all such integers d, choose p to be the smallest. Then p must be a prime number. Otherwise, it too would possess a divisor q with $1 < q < p$; but $q \mid p$ and $p \mid n$ implies that $q \mid n$, which contradicts our choice of p as the smallest divisor, not equal to 1, of n. Thus, there exists a prime p with $p \mid n$. □

THEOREM 2.2. *If $p$ is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

PROOF. If $p \mid a$, then we are done, so let us assume that $p \nmid a$. Since the only positive divisors of $p$ ( hence, the only candidates for the value of $gcd(a, p)$ ) are 1 and $p$ itself, this implies that $gcd(a, p) = 1$. Citing Euclid's lemma, it follows immediately that $p \mid b$. □

THEOREM 2.3. *There are an infinite number of primes.*

PROOF. Write the primes $2, 3, 5, 7, 11 \cdots$ in ascending order. For any particular prime p, consider the number $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$. That is, form the product of all the primes from 2 to p, and increase this product by one. Because $N > 1$, we can use the fundamental theorem to conclude that N is divisible by some prime q. But none of the primes $2, 3, 5, \cdots, p$ divides N . For if q were one of these primes, then on combining the relation $q \mid 2 \cdot 3 \cdot 5 \cdots p$ with $q \mid N$, we would get $q \mid (N - 2 \cdot 3 \cdot 5 \cdots p)$, or what is the same thing, $q \mid 1$. The only positive divisor of the integer 1 is 1 itself, and since $q > 1$, the contradiction is obvious. Consequently, there exists a new prime $q$ larger than $p$. □

PROPOSITION 2.1. *Some properties that govern prime numbers*

(1) *They are all odd with one exception(2).*
(2) *Their last digit is* $1, 3, 7, 9$ *with two exceptions(2,5).*
(3) *They are adjacent of multiple of six with two exceptions(2,3).*

PROOF. It is trivial to show (1) and (2). So let's show (3)

$$n = 6q + r, \text{ where } q \in \mathbb{Z}^+ \text{ and } r = \{0, 1, 2, 3, 4, 5\}$$

If $r = \{0, 2, 4\}$, then $2|n$ and $n$ can't be prime.
If $r = 3$, then $3|n$ again $n$ can't be prime.
So if n is a prime the remainder $r$ is either 1 or 5. □

THEOREM 2.4 (Bertnands postulate). *For each natural number* $n > 1$ *there is a prime* $p$ *such that* $n < p < 2n$.

### 2.2. Prime Number Theorem.

THEOREM 2.5.

## References

1. G. H. Hardy and M. Wright *An Introduction to the Theory of Numbers*, 6th ed, 2008.
2. Martin Aigner and Günter M. Ziegler, *Proofs from THE BOOK*, Springer, 4th ed, 2009.

DEPARTMENT OF MATHEMATICS, ADDIS ABABA UNIVERSITY, ADDIS ABABA, ETHIOPIA
*E-mail address*: miliyon@ymail.com