Subject: Number Theory,
Stage: Fourth, Department: Mathematics.
Lecturer: Dr. Andam Ali MUSTAFA

Chapter Two

1 Prime Numbers

Prime numbers, the building blocks of integers, have been studied extensively over the centuries. Being able to present an integer uniquely as product of primes is the main reason behind the whole theory of numbers and behind the interesting results in this theory. Many interesting theorems, applications and conjectures have been formulated based on the properties of prime numbers.

In this chapter, we present methods to determine whether a number is prime or composite using an ancient Greek method invented by Eratosthenes. We also show that there are infinitely many prime numbers. We then proceed to show that every integer can be written uniquely as a product of primes.

We introduce as well the concept of diophantine equations where integer solutions from given equations are determined using the greatest common divisor. We then mention the Prime Number theorem without giving a proof of course in addition to other conjectures and major results related to prime numbers.

1.1 The Sieve of Eratosthenes

Definition 1 *A prime is an integer greater than 1 that is only divisible by 1 and itself. Example 15. The integers 2, 3, 5, 7, 11 are prime integers. Note that any integer greater than 1 that is not prime is said to be a composite number.*

We now present the sieve of Eratosthenes. The Sieve of Eratosthenes is an ancient method of finding prime numbers up to a specified integer. This method was invented by the ancient Greek mathematician Eratosthenes. There are several other methods used to determine whether a number is prime or composite. We first present a lemma that will be needed in the proof of several theorems.

Lemma 1 *Every integer greater than one has a prime divisor.*

Proof: We present the proof of this Lemma by contradiction. Suppose that there is an integer greater than one that has no prime divisors. Since the set of integers with elements greater than one with no prime divisors is nonempty, then by the well ordering principle there is a least positive integer n greater than one that has no prime divisors. Thus n is composite since n divides n. Hence

$$n = ab \text{ with } 1 < a < \text{ and } 1 < b < n.$$

Notice that $a < n$ and as a result since n is minimal, a must have a prime divisor which will also be a divisor of n. □

Theorem 1 *If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$*

Proof: Since n is composite, then $n = ab$, where a and b are integers with $1 < a \leq b < n$. Suppose now that $a > \sqrt{n}$, then

$$\sqrt{n} < a \leq b$$

and as a result

$$ab > \sqrt{n}\sqrt{n} = n.$$

Therefore $a \leq \sqrt{n}$. Also, by Lemma 2, a must have a prime divisor a_1 which is also a prime divisor of n and thus this divisor is less than $a_1 \leq a \leq \sqrt{n}$. □

We now present the algorithm of the Sieve of Eratosthenes that is used to determine prime numbers up to a given integer.

1.2 The Algorithm of the Sieve of Eratosthenes

1. Write a list of numbers from 2 to the largest number n you want to test. Note that every composite integer less than n must have a prime factor less than $\sqrt{n}$. Hence you need to strike off the multiples of the primes that are less than $\sqrt{n}$
2. Strike off all multiples of 2 greater than 2 from the list . The first remaining number in the list is a prime number.
3. Strike off all multiples of this number from the list.
4. Repeat the above steps until no more multiples are found of the prime integers that are less than $\sqrt{n}$

1.3 Exercises

1. Use the Sieve of Eratosthenes to find all primes less than 100.
2. Use the Sieve of Eratosthenes to find all primes less than 200.
3. Show that no integer of the form $a^3 + 1$ is a prime except for $2 = 1^3 + 1$.
4. Show that if $2^n - 1$ is prime, then n is prime.

Hint: Use the identity $\left(a^{kl} - 1\right) = \left(a^k - 1\right)\left(a^{k(l-1)} + a^{k(l-2)} + \ldots + a^k + 1\right)$.

1.4 The infinitude of Primes

We now show that there are infinitely many primes. There are several ways to prove this result. An alternative proof to the one presented here is given as an exercise. The proof we will provide was presented by Euclid in his book the Elements.

Theorem 2 *There are infinitely many primes.*

Proof: We present the proof by contradiction. Suppose there are finitely many primes $p_1, p_2, \ldots, p_n$, where n is a positive integer. Consider the integer Q such that

$$Q = p_1 p_2 \ldots p_n + 1$$

By Lemma 3, Q has at least a prime divisor, say q. If we prove that q is not one of the primes listed then we obtain a contradiction. Suppose now that $q = p_i$ for $1 \leq i \leq n$. Thus q divides $p_1 p_2 \ldots p_n$ and as a result q divides $Q - p_1 p_2 \ldots p_n$. Therefore q divides 1 . But this is impossible since there is no prime that divides 1 and as a result q is not one of the primes listed. □

The following theorem discusses the large gaps between primes. It simply states that there are arbitrary large gaps in the series of primes and that the primes are spaced irregularly.

Theorem 3 *Given any positive integer n, there exists n consecutive composite integers.*

Proof: Consider the sequence of integers

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n, (n+1)!+n+1$$

Notice that every integer in the above sequence is composite because k divides $(n+1)!+k$ if $2 \leq k \leq n+1$ by 4 □

1.5 Exercises

1. Show that the integer $Q_n = n!+1$, where n is a positive integer, has a prime divisor greater than n. Conclude that there are infinitely many primes. Notice that this exercise is another proof of the infinitude of primes.

2. Find the smallest five consecutive composite integers.

3. Find one million consecutive composite integers.

4. Show that there are no prime triplets other than $3, 5, 7$.

1.6 The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic is one of the most important results in this chapter. It simply says that every positive integer can be written uniquely as a product of primes. The unique factorization is needed to establish much of what comes later. There are systems where unique factorization fails to hold. Many of these examples come from algebraic number theory. We can actually list an easy example where unique factorization fails.

Consider the class C of positive even integers. Note that C is closed under multiplication, which means that the product of any two elements in C is again in C. Suppose now that the only number we know are the members of C. Then we have $12 = 2.6$ is composite where as 14 is prime since it is not the product of two numbers in C. Now notice that $60 = 2.30 = 6.10$ and thus the factorization is not unique.

We now give examples of the unique factorization of integers.

Example 1 $99 = 3 \cdot 3 \cdot 11 = 3^2 \cdot 11, \quad 32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$

1.6.1 The Fundamental Theorem of Arithmetic

To prove the fundamental theorem of arithmetic, we need to prove some lemmas about divisibility.

Lemma 2 *If a, b, c are positive integers such that $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

Proof: Since $(a, b) = 1$, then there exists integers x, y such that $ax + by = 1$. As a result, $cax + cby = c$. Notice that since $a \mid bc$, then by Theorem 4 , a divides $cax + cby$ and hence a divides c. □

We can generalize the above lemma as such: If $(a, n_i) = 1$ for every $i = 1, 2, \cdots, n$ and $a \mid n_1 n_2 \cdots n_{k+1}$, then $a \mid n_{k+1}$. We next prove a case of this generalization and use this to prove the fundamental theorem of arithmetic.

Lemma 3 *If p divides $n_1 n_2 n_3 \ldots n_k$, where p is a prime and $n_i > 0$ for all $1 \leq i \leq k$, then there is an integer j with $1 \leq j \leq k$ such that $p \mid n_j$.*

Proof: We present the proof of this result by induction. For $k = 1$, the result is trivial. Assume now that the result is true for k. Consider $n_1 n_2 \dots n_{k+1}$ that is divisible by p. Notice that either

$$(p, n_1 n_2 \dots n_k) = 1 \text{ or } (p, n_1 n_2 \dots n_k) = p$$

Now if $(p, n_1 n_2 \dots n_k) = 1$ then by Lemma 4, $p \mid n_{k+1}$. Now if $p \mid n_1 n_2 \dots n_k$, then by the induction hypothesis, there exists an integer i such that $p \mid n_i$. □

We now state the fundamental theorem of arithmetic and present the proof using Lemma 5.

Theorem 4 *The Fundamental Theorem of Arithmetic Every positive integer different from 1 can be written uniquely as a product of primes.*

Proof: If n is a prime integer, then n itself stands as a product of primes with a single factor. If n is composite, we use proof by contradiction. Suppose now that there is some positive integer that cannot be written as the product of primes. Let n be the smallest such integer. Let $n = ab$, with $1 < a < n$ and $1 < b < n$. As a result a and b are products of primes since both integers are less than n. As a result, $n = ab$ is a product of primes, contradicting that it is not. This shows that every integer can be written as product of primes. We now prove that the representation of a positive integer as a product of primes is unique. Suppose now that there is an integer n with two different factorizations say

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_r$$

where $p_1, p_2, \dots p_s, q_1, q_2, \dots q_r$ are primes,

$$p_1 \leq p_2 \leq p_3 \leq \dots \leq p_s \text{ and } q_1 \leq q_2 \leq q_3 \leq \dots \leq q_r$$

Cancel out all common primes from the factorizations above to get

$$p_{j_1} p_{j_2} \dots p_{j_u} = q_{i_1} q_{i_2} \dots q_{i_v}$$

Thus all the primes on the left side are different from the primes on the right side. Since any $p_{j_l} (l = 1, \cdots, n)$ divides $p_{j_1} p_{j_2} \dots p_{j_u}$, then p_{j_l} must divide $q_{i_1} q_{i_2} \dots q_{i_v}$, and hence by Lemma 5, p_{j_1} must divide q_{j_k} for some $1 \leq k \leq v$ which is impossible. Hence the representation is unique. □

Remmark 1 *The unique representation of a positive integer n as a product of primes can be written in several ways. We will present the most common representations. For example, $n = p_1 p_2 p_3 \dots p_k$ where p_i for $1 \leq i \leq k$ are not necessarily distinct. Another example would be*

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_j^{a_j}$$

where all the p_i are distinct for $1 \leq i \leq j$. One can also write a formal product

$$n = \prod_{all\ primes\ p_i} p_i^{\alpha_i},$$

where all but finitely many of the $\alpha_i's$ are 0.

Example 2 *The prime factorization of 120 is given by* $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$. *Notice that 120 is written in the two ways described in 1*

We know describe in general how prime factorization can be used to determine the greatest common divisor of two integers. Let

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \quad \text{and } b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where we exclude in these expansions any prime p with power 0 in both a and b (and thus some of the powers above may be 0 in one expansion but not the other). Of course, if one prime p_i appears in a but not in b, then $a_i \neq 0$ while $b_i = 0$, and vise versa. Then the greatest common divisor is given by

$$(a, b) = p_1^{\min(a_1, b_2)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

where $\min(n, m)$ is the minimum of m and n.

The following lemma is a consequence of the Fundamental Theorem of Arithmetic.

Lemma 4 *Let a and b be relatively prime positive integers. Then if d divides ab, there exists d_1 and d_2 such that $d = d_1 d_2$ where d_1 is a divisor of a and d_2 is a divisor of b. Conversely, if d_1 and d_2 are positive divisors of a and b, respectively, then $d = d_1 d_2$ is a positive divisor of ab.*

Proof: Let $d_1 = (a, d)$ and $d_2 = (b, d)$. Since $(a, b) = 1$ and writing a and b in terms of their prime decomposition, it is clear that $d = d_1 d_2$ and $(d_1, d_2) = 1$. Note that every prime power in the factorization of d must appear in either d_1 or d_2. Also the prime powers in the factorization of d that are prime powers dividing a must appear in d_1 and that prime powers in the factorization of d that are prime powers dividing b must appear in d_2. Now conversely, let d_1 and d_2 be positive divisors of a and b, respectively. Then

$$d = d_1 d_2$$

is a divisor of ab. □

1.6.2 More on the Infinitude of Primes

There are also other theorems that discuss the infinitude of primes in a given arithmetic progression. The most famous theorem about primes in arithmetic progression is Dirichlet's theorem

Theorem 5 (Dirichlet's Theorem) *Given an arithmetic progression of terms $an + b$, for $n = 1, 2, \dots$, the series contains an infinite number of primes if a and b are relatively prime,*

This result had been conjectured by Gauss but was first proved by Dirichlet. Dirichlet proved this theorem using complex analysis, but the proof is so challenging. As a result, we will present a special case of this theorem and prove that there are infinitely many primes in a given arithmetic progression. Before stating the theorem about the special case of Dirichlet's theorem, we prove a lemma that will be used in the proof of the mentioned theorem.

Lemma 5 *If a and b are integers both of the form $4n + 1$, then their product ab is of the form $4n + 1$*

Lemma 6 *Let $a = 4n_1 + 1$ and $b = 4n_2 + 1$, then*

$$ab = 16n_1n_2 + 4n_1 + 4n_2 + 1 = 4\left(4n_1n_2 + n_1 + n_2\right) + 1 = 4n_3 + 1,$$

where $n_3 = 4n_1n_2 + n_1 + n_2$.

Theorem 6 *There are infinitely many primes of the form $4n+3$, where n is a positive integer.*

Proof: Suppose that there are finitely many primes of the form $4n+3$, say $p_0 = 3, p_1, p_2, \ldots, p_n$. Let

$$N = 4p_1p_2 \ldots p_n + 3.$$

Notice that any odd prime is of the form $4n+1$ or $4n+3$. Then there is at least one prime in the prime factorization of N of the form $4n+3$, as otherwise, by Lemma $4N$ will be in the form $4n+1$. We wish to prove that this prime in the factorization of N is none of $p_0 = 3, p_1, p_2, \ldots, p_n$. Notice that if

$$3 \mid N,$$

then $3 \mid (N-3)$ and hence

$$3 \mid 4p_1p_2 \ldots p_n$$

which is impossible since $p_i \neq 3$ for every i. Hence 3 doesn't divide N. Also, the other primes $p_1, p_2, \ldots, p_n$ don't divide N because if $p_i \mid N$, then

$$p_i \mid (N - 4p_1p_2 \ldots p_n) = 3.$$

Hence none of the primes $p_0, p_1, p_2, \ldots, p_n$ divides N. Thus there are infinitely many primes of the form $4n+3$. □

1.7 Exercises

1. Find the prime factorization of 32 , of 800 and of 289.
2. Find the prime factorization of 221122 and of 9! !.
3. Show that all the powers of in the prime factorization of an integer a are even if and only if a is a perfect square.
4. Show that there are infinitely many primes of the form $6n+5$.

2 Least Common Multiple

We can use prime factorization to find the smallest common multiple of two positive integers.

Definition 2 *The least common multiple (l.c.m.) of two positive integers is the smallest positive integer that is a multiple of both.*

We denote the least common multiple of two positive integers a an b by $\langle a, b\rangle$.

Example 3 $\langle 2, 8\rangle = 8, \langle 5, 8\rangle = 40$

We can figure out $\langle a, b\rangle$ once we have the prime factorization of a and b. To do that, let

$$a = p_1^{a_1}p_2^{a_2} \ldots p_m^{a_n} \text{ and } b = p_1^{b_1}p_2^{b_2} \ldots p_m^{b_n},$$

where (as above) we exclude any prime with 0 power in both a and b. Then $\langle a, b\rangle = p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)} \ldots p_m^{\max(a_n,b_n)}$, where $\max(a, b)$ is the maximum of the two integers a and b. We now prove a theorem that relates the least common multiple of two positive integers to their greatest common divisor. In some books, this theorem is adopted as the definition of the least common multiple. To prove the theorem we present a lemma

Lemma 7 *If a and b are two real numbers, then*

$$\min(a, b) + \max(a, b) = a + b$$

Proof: Assume without loss of generality that $a \geq b$. Then

$$\max(a,b) = a \text{ and } \min(a,b) = b,$$

and the result follows.

□

Theorem 7 *Let a and b be two positive integers. Then*

1. $\langle a,b\rangle \geq 0$; 2. $\langle a,b\rangle = ab/(a,b)$;
2. *If $a \mid m$ and $b \mid m$, then $\langle a,b\rangle \mid m$*

Proof: Proof. The proof of part 1 follows from the definition.
As for part 2 , let

$$a = p_1^{a_1}p_2^{a_2}\dots p_m^{a_n} \text{ and } b = p_1^{b_1}p_2^{b_2}\dots p_m^{b_n}$$

Notice that since

$$(a,b) = p_1^{\min(a_1,b_2)}p_2^{\min(a_2,b_2)}\dots p_n^{\min(a_n,b_n)}$$

and

$$\langle a,b\rangle = p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)}\dots p_m^{\max(a_n,b_n)}$$

then

$$\begin{aligned}\langle a,b\rangle(a,b) &= p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)}\dots p_m^{\max(a_n,b_n)}p_1^{\min(a_1,b_2)}p_2^{\min(a_2,b_2)}\dots p_n^{\min(a_n,b_n)}\\ &= p_1^{\max(a_1,b_1)+\min(a_1,b_1)}p_2^{\max(a_2,b_2)+\min(a_2,b_2)}\dots p_m^{\max(a_n,b_n)+\min(a_n,b_n)}\\ &= p_1^{a_1+b_1}p_2^{a_2+b_2}\dots p_n^{(a_n+b_n)}\\ &= p_1^{a_1}p_2^{a_2}\dots p_m^{a_n}p_1^{b_1}p_2^{b_2}\dots p_m^{b_n} = ab\end{aligned}$$

Note also that we used Lemma 8 in the above equations. For part 3 , it would be a nice exercise to show that $ab/(a,b) \mid m$ (Exercise 6). Thus $\langle a,b\rangle \mid m$. □

2.1 Exercises

1. Find the least common multiple of 14 and 15.
2. Find the least common multiple of 240 and 610.
3. Find the least common multiple and the greatest common divisor of $2^5 5^6 7^2 11$ and $2^3 5^8 7^2 13$
4. Show that every common multiple of two positive integers a and b is divisible by the least common multiple of a and b.
5. Show that if a and b are positive integers then the greatest common divisor of a and b divides their least common multiple. When are the least common multiple and the greatest common divisor equal to each other.
6. Show that $ab/(a,b) \mid m$ where $m =< a,b >$.

3 Linear Diophantine Equations

In this section, we discuss equations in two variables called diophantine equations. These kinds of equations require integer solutions. The goal of this section is to present the set of points that determine the solution to this kind of equations. Geometrically speaking, the diophantine equation represent the equation of a straight line. We need to find the points whose coordinates are integers and through which the straight line passes.

Definition 3 *A linear equation of the form $ax + by = c$ where a, b and c are integers is known as a linear diophantine equation.*

Note that a solution to the linear diophantine equation (x_0, y_0) requires x_0 and y_0 to be integers. The following theorem describes the case in which the diophantine equation has a solution and what are the solutions of such equations.

Theorem 8 *The equation $ax+by = c$ has integer solutions if and only if $d \mid c$ where $d = (a, b)$. If the equation has one solution $x = x_0, y = y_0$, then there are infinitely many solutions and the solutions are given by*

$$x = x_0 + (b/d)t \quad y = y_0 - (a/d)t$$

where t is an arbitrary integer.

Proof: Suppose that the equation $ax + by = c$ has integer solution x and y. Thus since $d \mid a$ and $d \mid b$, then

$$d \mid (ax + by) = c.$$

Now we have to prove that if $d \mid c$, then the equation has integral solution. Assume that $d \mid c$. By theorem 9 , there exist integers m and n such that

$$d = am + bn.$$

And also there exists integer k such that

$$c = dk$$

Now since $c = ax + by$, we have

$$c = dk = (ma + nb)k = a(km) + b(nk).$$

Hence a solution for the equation $ax + by = c$ is

$$x_0 = km \text{ and } y_0 = kn.$$

What is left to prove is that we have infinitely many solutions. Let

$$x = x_0 + (b/d)t \text{ and } y = y_0 - (a/d)t.$$

We have to prove now that x and y are solutions for all integers t. Notice that

$$ax + by = a\left(x_0 + (b/d)t\right) + b\left(y_0 - (a/d)t\right) = ax_0 + by_0 = c.$$

We now show that every solution for the equation $ax + by = c$ is of the form

$$x = x_0 + (b/d)\,\text{tand}\, y = y_0 - (a/d)t.$$

Notice that since $ax_0 + by_0 = c$, we have

$$a(x - x_0) + b(y - y_0) = 0.$$

Hence

$$a(x - x_0) = b(y - y_0).$$

Dividing both sides by d, we get

$$a/d(x - x_0) = b/d(y - y_0).$$

Notice that $(a/d, b/d) = 1$ and thus we get by Lemma 4 that $a/d \mid y - y_0$. As a result, there exists an integer t such that $y = y_0 - (a/d)t$. Now substituting $y - y_0$ in the equation

$$a(x - x_0) = b(y - y_0).$$

We get

$$x = x_0 + (b/d)t$$

□

Example 4 *The equation* $3x+6y = 7$ *has no integer solution because* $(3, 6) = 3$ *does not divide 7.*

Example 5 *There are infinitely many integer solutions for the equation* $4x+ 6y = 8$ *because* $(4, 6) = 2 \mid 8$. *We use the Euclidean algorithm to determine* m *and* n *where* $4m + 6n = 2$. *It turns out that* $4(-1) + 6(1) = 2$. *And also* $8 = 2.4$. *Thus* $x_0 = 4.(-1) = -4$ *and* $y_0 = 4.1 = 4$ *is a particular solution. The solutions are given by*

$$x = -4 + 3t \quad y = 4 - 2t$$

for all integers t.

3.1 Exercises

1. Either find all solutions or prove that there are no solutions for the diophantine equation $21x + 7y = 147$

2. Either find all solutions or prove that there are no solutions for the diophantine equation $2x + 13y = 31$

3. Either find all solutions or prove that there are no solutions for the diophantine equation $2x + 14y = 17$. 4. A grocer orders apples and bananas at a total cost of \$8.4. If the apples cost 25 cents each and the bananas 5 cents each, how many of each type of fruit did he order.

4 The function $[x]$, the symbols "O", "o" and " $\sim$ "

We start this section by introducing an important number theoretic function. We proceed in defining some convenient symbols that will be used in connection with the growth and behavior of some functions that will be defined in later chapters.

4.0.1 The Function $[x]$

Definition 4 *The function $[x]$ represents the largest integer not exceeding x. In other words, for real $x, [x]$ is the unique integer such that*

$$x - 1 < [x] \leq x < [x] + 1.$$

We also define $((x))$ to be the fractional part of x. In other words $((x)) = x - [x]$

We now list some properties of $[x]$ that will be used in later or in more advanced courses in number theory.

1. $[x + n] = [x] + n$, if n is an integer.
2. $[x] + [y] \leq [x + y]$
3. $[x] + [-x]$ is 0 if x is an integer and -1 otherwise.
4. The number of integers m for which $x < m \leq y$ is $[y] - [x]$. 5. The number of multiples of m which do not exceed x is $[x/m]$.

Using the definition of $[x]$, it will be easy to see that the above properties are direct consequences of the definition.

We now define some symbols that will be used to estimate the growth of number theoretic functions. These symbols will be not be really appreciated in the context of this book but these are often used in many analytic proofs.

4.0.2 The "O"' and "'o' Symbols

Let $f(x)$ be a positive function and let $g(x)$ be any function. Then $O(f(x))$ (pronounced "big-oh" of $f(x)$)denotes the collection of functions $g(x)$ that exhibit a growth that is limited to that of $f(x)$ in some respect. The traditional notation for stating that $g(x)$ belongs to this collection is:

$$g(x) = O(f(x)).$$

This means that for sufficiently large x,

$$\frac{|g(x)|}{|f(x)|} < M,$$

where M is some positive number.

Example 6 $\sin(x) = O(x)$, *and also* $\sin(x) = O(1)$.

Now, the relation $g(x) = o(f(x))$, pronounced "small-oh" of $f(x)$, is used to indicate that $f(x)$ grows much faster than $g(x)$. It formally says that

$$\lim_{x \to \infty} \frac{g(x)}{f(x)} = 0.$$

More generally, $g(x) = o(f(x))$ at a point b if

$$\lim_{x \to b} \frac{g(x)}{f(x)} = 0.$$

Example 7 $\sin(x) = o(x)$ *at* ∞, *and* $x^k = o\left(e^x\right)$ *also at* ∞ *for every constant* k

The notation that $f(x)$ *is asymptotically equal to* $g(x)$ *is denoted by* $\sim$. *Formally speaking, we say that* $f(x) \sim g(x)$ *if*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

Example 8 $[x] \sim x$

The purpose of introducing these symbols is to make complicated mathematical expressions simpler. Some expressions can be represented as the principal part that you need plus a remainder term. The remainder term can be expressed using the above notations. So when you need to combine several expressions, the remainder parts involving these symbols can be easily combined. We will state now some properties of the above symbols without proof. These properties are easy to prove using the definitions of the symbols.

1. $O(O(f(x))) = O(f(x))$
2. $o(o(f(x))) = o(f(x))$
3. $O(f(x)) \pm O(f(x)) = O(f(x))$
4. $o(f(x) \pm o(f(x)) = o(f(x))$
5. $O(f(x)) \pm O(g(x)) = O(\max(f(x), g(x)))$,

There are some other properties that we did not mention here, properties that are rarely used in number theoretic proofs.

4.1 Exercises

1. Prove the five properties of the $[x]$
2. Prove the five properties of the O and o notations in Example 24.

5 Theorems and Conjectures involving prime numbers

We have proved that there are infinitely many primes. We have also proved that there are arbitrary large gaps between primes. The question that arises naturally here is the following: Can we estimate how many primes are there less than a given number? The theorem that answers this question is the prime number theorem. We denote by $\pi(x)$ the number of primes less than a given positive number x. Many mathematicians worked on this theorem and conjectured many estimates before Chebyshev finally stated that the estimate is $x/\log x$. The prime number theorem was finally proved in 1896 when Hadamard and Poussin produced independent proofs. Before stating the prime number theorem, we state and prove a lemma involving primes that will be used in the coming chapters.

Lemma 8 *Let* p *be a prime and let* $m \in \mathbb{Z}^+$. *Then the highest power of* p *dividing* $m!$ *is*

$$\sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right]$$

Proof: Among all the integers from 1 till m, there are exactly $\left[\frac{m}{p}\right]$ integers that are divisible by p. These are $p, 2p, \ldots, \left[\frac{m}{p}\right] p$. Similarly we see that there are $\left[\frac{m}{p^i}\right]$ integers that are divisible by p^i. As a result, the highest power of p dividing m ! is

$$\sum_{i\geq 1} i\left\{\left[\frac{m}{p^i}\right] - \left[\frac{m}{p^{i+1}}\right]\right\} = \sum_{i\geq 1}\left[\frac{m}{p^i}\right]$$

Theorem 20. The Prime Number Theorem Let $x > 0$ then

$$\pi(x) \sim x/\log x$$

So this theorem says that you do not need to find all the primes less than x to find out their number, it will be enough to evaluate $x/\log x$ for large x to find an estimate for the number of primes. Notice that I mentioned that x has to be large enough to be able to use this estimate. □

Several other theorems were proved concerning prime numbers. many great mathematicians approached problems that are related to primes. There are still many open problems of which we will mention some.

Conjecture 1 *Twin Prime Conjecture There are infinitely many pairs primes p and $p+2$.*

Conjecture 2 *Goldbach's Conjecture Every even positive integer greater than 2 can be written as the sum of two primes.*

Conjecture 3 *The n^2+1 Conjecture There are infinitely many primes of the form n^2+1, where n is a positive integer.*

Conjecture 4 *Polignac Conjecture For every even number $2n$ are there infinitely many pairs of consecutive primes which differ by $2n$.*

Conjecture 5 *Opperman Conjecture Is there always a prime between n^2 and $(n+1)^2$?*