Chapter 4 Basic Concepts of Number Theory

Pierre De Fermat (1601 – 1665)

From earliest times the ancient Greeks and Chinese mathematicians interested in the study of relationships among numbers. Until the seventeenth century the famous French mathematician Pierre De Fermat (1601 – 1665) first serious studied of the subject, who is considered the founder of the theory of numbers. The theory of numbers is regarded as the purest branch of pure mathematics. National Council of Teachers of Mathematics [NCTM] (2000) proposed Grade 9-12 expectation to use number theory arguments to justify relationships involving whole number.

Carl Friedrich Gauss (1777 – 1855) made many original contributions to the number theory by systematizing all materials in the form we have today. Gauss referred to mathematics as the "Queen of Sciences" and number theory as "Queen of Mathematics" (Flood, 2013).

Natural Numbers-Whole Numbers-Integers

We begin with the definition of three sets: natural numbers, whole number, and integers.

Definition 1: The set of ***natural numbers*** is $N = \{1, 2, 3, 4, 5, \dots\}$. N is also called the set of ***positive integers***.

Definition 2: The set of ***whole numbers*** is $W = \{0, 1, 2, 3, 4, 5, \dots\}$. W is also referred to the set of ***non-negative integers***.

Definition 3: The set of ***integers*** is $I = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. I is also denoted by Z.

The relationship between the set $N, W,$ and I are as follows:

$$N \subset W \subset I$$

Properties of Integers

Let I be a set on which addition (+) and multiplication (·) are defined. Integers have main properties under addition and multiplication as the following:

Properties of Addition

Property 1 Closure under Addition:

Closure property of integers under addition states that:

$a + b$ is in I for all a and b in I.

Property 2 Associative Law of Addition:

Associative property of integers under addition states that:

$a + (b + c) = (a + b) + c$ for all a, b and c in I.

Property 3 Commutative Law of Addition:

Commutative property of integers under addition states that:

$a + b = b + a$ for all a and b in I.

Property 4 Additive Identity

Identity property states that:

There is an element 0 in I such that $a + 0 = 0 + a = a$ for all a in I.

Property 5 Additive Inverse

Inverse property states that:

For each element a in I, there is an element $-a$ in I such that
$a + (-a) = (-a) + a = 0$.

Properties of Multiplication

Property 6 Closure under Multiplication:

Closure property of integers under multiplication states that:

$a \cdot b$ is in I for all a and b in I.

Property 7 Associative Law of Multiplication:

Associative property of integers under multiplication states that:

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b and c in I.

Property 8 Commutative Law of Multiplication:

Commutative property of integers under multiplication states that:

$a \cdot b = b \cdot a$ for all a and b in I.

Property 9 Multiplicative Identity

Identity property states that:

There is an element 1 in I such that $a \cdot 1 = 1 \cdot a = a$ for all a in I.

Remark: The inverse property is not satisfied for every element *a* in *I*. Because the identity element is equal to 1, but no two integers multiply to give 1 except 1 itself.

Property Relating Addition and Multiplication

Property 10 Distributive Laws

Distributive property of multiplication over addition states that:

i. $c \cdot (a + b) = c \cdot a + c \cdot b$ for all a, b and c in I. (left distributive law)

ii. $(a + b) \cdot c = a \cdot c + b \cdot c$ for all a, b and c in I. (right distributive law)

Even numbers and odd numbers

The set of integers can be separated into two disjoint subsets, namely a set of even numbers and a set of odd numbers.

Definition 4: A number is ***even*** if it can be written in the form 2*n*, where *n* is an integer; a number is ***odd*** if it can be written in the form 2*n* + 1.

The set of even numbers is $E = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$.

The set of odd numbers is $O = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$.

Theorem 1: The sum of two odd numbers is even.

Proof: Let *a* and *b* be odd numbers. Then there exist integers *m* and *n* such that $a = 2m + 1$ and $b = 2n + 1$.

Thus, $a + b = (2m + 1) + (2n + 1) = 2m + 2n + 2 = 2(m + n + 1)$.

Since, $m + n + 1$ is an integer. (Closure law of integer addition)

Then, $a + b = 2p$ with $p = m + n + 1 \in I$.

Therefore, $a + b$ is even. (Definition of even integer) #

Theorem 2: Let *n* be an integer. If *n* is even, then $n^2$is even.

Proof: Assume *n* is an even integer.

Then $n = 2k$ for some $k \in I$. (Definition. of an even integer)

Squaring both sides, we get $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since *k* is an integer, so is $2k^2$. (Closure law of integer multiplication)

Hence $n^2 = 2p$ with $p = 2k^2 \in I$.

Therefore $n^2$is even (Definition. of an even integer) #

The sum of consecutive odd numbers

Adding consecutive odd numbers obtains the interesting results as follows:

$1 + 3 = 4 = 2^2$

$1 + 3 + 5 = 9 = 3^2$

$1 + 3 + 5 + 7 = 14 = 4^2$; and so on.

It is true that the sum of the first *n* odd numbers is equal to n^2. Thus, the sum of the first 10 odd numbers is equal to $10^2 = 100$. This result can be illustrated by using square shape as shown in Figure 4.1:

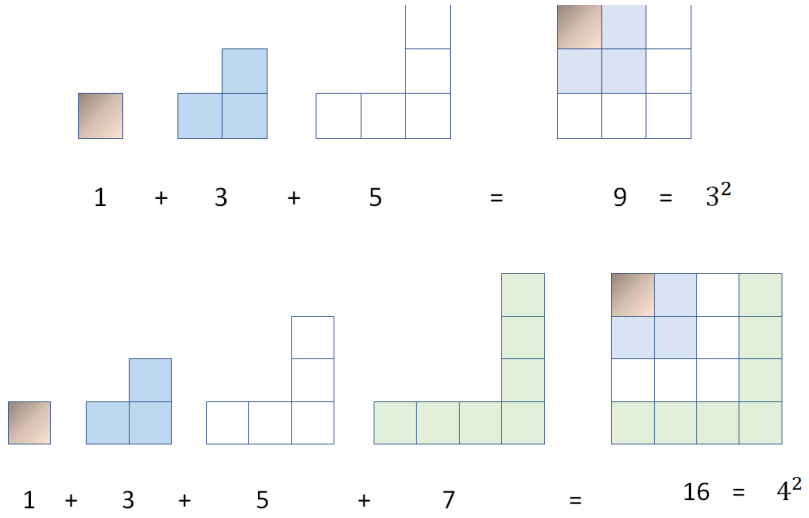


Figure 4.1 Sum of the consequence of odd numbers

The Fibonacci Sequence

The ***Fibonacci sequence*** is another interesting sequence of natural number created by Leonardo Pisano Bogolo, and he lived between 1170 – 1250 in Italy. "Fibonacci" was his nickname, since he was the son (*figlio*) of Bonaccio (NTCM, 1967).

The Fibonacci sequence of natural numbers is listed as follows:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, …,

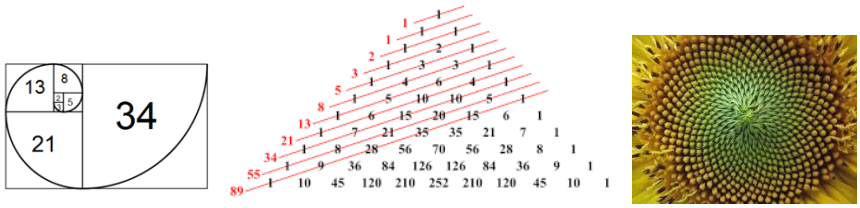
Where each new term is formed by adding the last term to its predecessor. Thus, 2 = 1 + 1, 3 = 2 + 1, 5 = 3 + 2, 8 = 5 + 3, …. So, we can write the rule:

$$x_n = x_{n-1} + x_{n-2}$$

Where: x_n is term number "*n*", x_{n-1} is the previous term "$n - 1$", x_{n-2} is the term before that "$n - 2$"

The Fibonacci sequence plays very important in mathematics (code theory) and appears in arts and nature. When we make squares with those widths, we get a nice spiral (Figure 4.2(a)). When we add the coefficients of $(a + b)^n$, where n is a natural number as

shown in Pascal Triangle, we will get the Fibonacci sequence (Figure 4.2 (b)). In addition, another example of the Fibonacci can be found in the nature such as the number of petals of flowers (Figure 4.2 (c)).



(a) (b) (c)

Figure 4.2 Fibonacci sequence

Practice 4.1

1. Prove the following statements:
   (a) If p and q are both even, then $p + q$ is even.
   (b) If p is odd and q is even, then $p + q$ is odd.
   (c) If p and q are both even, then pq is even.
   (d) If p and q are both odd, then pq is odd.
   (e) If p is odd and q is even, then pq is even.
2. Prove the following statements:
   (a) Let n be an integer. If n^2 is odd, then n is odd.
   (b) Let n be an integer. If n^2 is even, then n is even.
   (c) Let n be an integer. Then n^2 is odd if and only if n is odd.

Primes and Composites

The positive integers **greater than 1** can be distinguished into two sets, i.e., the set of prime numbers as 2, 3, 5, 7, 11, 13, 17, … and the set of composite numbers as 4, 6, 8, 9, 10, 12, 14, …. The prime numbers and composite numbers are defined as follows:

Definition 5: A ***prime number*** p is a positive integer greater than 1 whose only factors are 1 and itself.

Definition 6: A ***composite number*** q is a positive integer greater than 1 which is not prime.

Look at the numbers 1 through 10 in Table 4.1 as examples:

Table 4.1 Prime numbers and composite number from 1 through 10

Number	Explanation	Prime/Composite
1	not a prime number by definition	-
2	factors are 1 and 2	Prime
3	factors are 1 and 3	Prime
4	factors are 1, 2, and 4	Composite
5	factors are 1 and 5	Prime
6	factors are 1, 2, 3, and 6	Composite
7	factors are 1 and 7	Prime
8	factors are 1, 2, 4, and 8	Composite
9	factors are 1, 3, 9	Composite
10	factors are 1, 2, 5, and 10	Composite

The Sieve of Eratosthenes

Eratosthenes (about 230 BC) developed a sieve method for finding all prime numbers by iteratively marking the multiples of primes and composite, starting from 1.

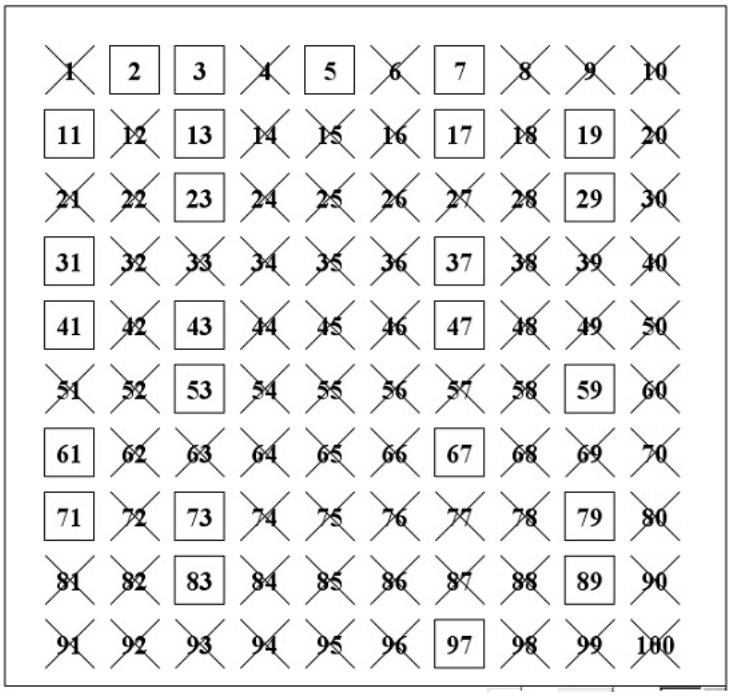


Figure 4.3 The sieve of Eratosthenes method

Source: https://www.cut-the-knot.org/Curriculum/Arithmetic/Eratosthenes.shtml

The Distribution of Primes

From Figure 4.3, 2 is the smallest prime number. It also the only even prime number. The primes are very irregularly distributed as shown in Table 4.2.

Table 4.2 The distribution of primes among the natural numbers up to 1,000

Number from	1	100	200	300	400	500	600	700	800	900
to	100	200	300	400	500	600	700	800	900	1000
Number of primes	25	21	16	16	17	14	16	14	15	14

In Table 4.2, the primes seem to occur less frequently as go farther out in the sequence of natural numbers. Upon ingenious calculations, the number of primes in the interval from 10^{12} (one trillion) to $10^{12} + 1000$ occur less frequently as shown in Table 4.3.

Table 4.3 The distribution of primes in the range from 10^{12} to $10^{12} + 1000$

Number from	$10^{12}+$	0	100	200	300	400	500	600	700	800	900
to	$10^{12}+$	100	200	300	400	500	600	700	800	900	1000
Number of primes		4	6	2	4	2	4	3	5	1	6

The smallest interval between two consecutive primes is 2 and 3, but nobody yet knows the prime that immediately follows $2^{2317} - 1$ which contains 969 digits (NTCM, 1967). However, we can write consecutive composite numbers as we please. If we wish to have 1000 consecutive numbers, we can start from 1001! as follows:

$$1001! + 2, 1001! + 3, 1001! + 4, \ldots, 1001! + 1001$$

Where the notation 1001! means $(1001)(1000)(999)(998)(997) \ldots (5)(4)(3)(2)(1)$.

Since 1001! contains the factor 2, then 1001!+2 is exactly divisible by 2. Likewise the term 1001!+3 until the thousandth term 1001!+1001 can be exactly divisible by 3, 4, …, 1001, respectively. In this way we can show that there exist two prime numbers that are arbitrarily far apart.

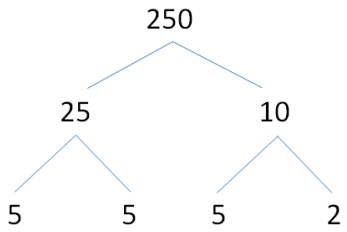
The Fundamental Theorem of Arithmetic

Fundamental theorem of arithmetic proved by Carl Friedrich Gauss in 1801. It states that:

Any integer greater than 1 can be expressed as the product of prime numbers in only one way.

The fundamental theorem of arithmetic is a very useful method to understand the prime factorization of any number.

Example: Prime factorization of 250



From the above diagram, we get $250 = 5 \times 5 \times 5 \times 2$. This theorem tells us that this factorization must be unique. However, we can change the order in which the prime factors occur but the set of prime factors is unique. For example, the prime factorization of 250 can be written as: $250 = 2 \times 5^3$ or $250 = 2 \times 5 \times 5 \times 5$. We see now why the number 1 is not called a prime; it may multiply 1 into a factorization as frequently as we wish without changing the value of the number, and the uniqueness of factorization does not apply.

The Number of Primes is Infinite

Euclid was the first to prove there are infinite of primes with simple method as follows:

1. Assume there are a finite number n of primes $p_i, i = 1, 2, 3, \dots, n$, i.e. $p_1, p_2, p_3, \dots, p_n$, where the largest prime is p_n.
2. Consider the number that is the product of these, plus one:
   $N = p_1 p_2 p_3 \dots p_n + 1$
3. Divide N by $p_1, p_2, p_3, \dots, p_n$ leaves a remainder of 1.
4. Hence it is either prime itself, or divisible by another prime greater than p_n, contradicting the assumption.
5. Therefore, we reject the assumption of the largest prime and conclude that the number of primes is infinite.

There are many attempts to give formulas that yield only prime as the following examples.

Example 1: Formula: $x^2 - x + 41$ will give a prime for every value of *x*.

Proof: By using counter example, $x = 41$

Substitute $x = 41$ in the formula,

$41^2 - 41 + 41 = 41^2$ which is composite.

Therefore, this formula may hold in many instances and yet not be true in all cases. #

Example 2: A polynomial is a sum of terms each of which has a numerical factor multiplied by non-negative integral power of *x* as the following form:

$$a + bx + cx^2 + \cdots + lx^n$$

where $a, b, c, \ldots, l$ are numerical coefficients. The number *n*, the highest power of *x*, is called the degree of the polynomial.

This polynomial may not be true in all cases, for example of the case $x^2 - x + 41$ or $x^2 + x + 17$.

It has been illustrated that *no polynomial with integral coefficients, irrespective of its degree, can yield only prime values when all possible natural numbers are substituted for x in the polynomial*. #

Mersenne Primes

At the beginning of the 17th century, French monk Marin Mersenne defined the prime numbers $M_p = 2^p - 1$, where p is a prime number. Mersenne prime numbers are named for his name.

In 1964, Alexander Hurwitz and John L. Selfridge, two American mathematicians, discovered $2^{11213} - 1$ is the largest prime contains nearly 3400 digits. However, finding Mersenne primes is computationally very challenging because of the remarkable properties that every Mersenne prime corresponds to exactly one perfect number. In 1996, George Woltman, from the Massachusetts Institute of Technology (MIT) founded the Great Internet Mersenne Prime Search (GIMPS), a distributed computing project that searches for new Mersenne primes and allows any user can participate by downloading the software Prime95, created by Woltman.

In 2018, Patrick Laroche of the Great Internet Mersenne Prime Search (GIMPS) found the largest known prime number $2^{82,589,933} - 1$, a number which has 24,862,048 digits when written in base 10.

Practice 4.2

1. Express the numbers from 21 to 30 as the difference of two squares, if possible. Example: $21 = 11^2 - 10^2$
2. Prove this conjecture: Every positive odd number *m* can be expressed as the different of the square of two consecutive numbers that sum to the original number *m*.
3. Express the prime number 31 in the form $2^p - 1$, where *p* is a prime number and as a different of two perfect squares using the identity $(a + b)(a - b) = a^2 - b^2$.

Divisibility

Divisibility is one of the most fundamental concepts in number theory such as the concept of prime numbers and composite numbers.

Definition 8: Let $a, b \in I$ and $a \neq 0$, *a* ***divides*** *b* if there is an integer *k* such that $b = ak$. This is denoted by $a| b$.

A consequence of this definition is that *b* is ***divisible*** by *a* (without remainder). Alternative terms for *a* ***divides*** *b* are: *a* is a ***divisor*** of *b*, or *a* is a ***factor*** of *b*, or *b* is a ***multiple*** of *a*. The symbol $a \nmid b$ means *a* ***does not divide*** *b*.

Example: $8| 72$ because $8 \cdot 9 = 72$.

Divisibility of Integers and Properties

Property 1: If $a| b$ and $a| c$, then $a| (b + c)$.

Proof: Since $a| b$, there exists an integer $k_1$such that $b = ak_1$ (Def. of divisor) … (1)

Since $a| c$, there exists an integer $k_2$such that $c = ak_2$ (Def. of divisor) … (2)

(1) + (2); $b + c = ak_1 + ak_2$	(Addition property)
$= a(k_1 + k_2)$	(Distributive law for addition)
Since, $k_1 + k_2$ is an integer	(Closure law for addition)
Then, $a| (b + c)$.	(Def. of divisor) #

Property 2: If $a| b$ and $a| c$, then $a| bc$.

Property 3: If $a|\ b$ and $b|\ c$, then $a|\ c$.

Property 4: If $a|\ b$ and $a|\ c$, then $a|\ (mb + nc)$ whenever *m* and *n* are integers.

The Number of Divisors of a Number

In considering the divisors or factors of a natural number, we found that the prime number or prime factors may occur once, twice, and more often as illustrated in Table 4.4

Table 4.4 The divisors and prime factorizations of natural numbers

No.	Divisor/Factor	No. of Divisors/Factors	Factorization
15	1, 3, 5, 15	4	3×5
30	1, 2, 3, 5, 6, 10, 15, 30	8	$2 \times 3 \times 5$
60	1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60	12	$2^2 \times 3 \times 5$
144	1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 36, 48, 72, 144	15	$2^4 \times 3^2$

The number of divisors or factors is found for the following rule:

Let the natural number *N* have the factorization

$$N = p^a q^b r^c \ldots$$

Where *p, q, r, …* are the prime factors raised to the powers *a, b, c, …*, respectively. The number of divisors of *N*, denoted by $d(N)$, is found by the formula

$$d(N) = (a + 1)(b + 1)(c + 1) \ldots$$

Example: $144 = 2^4 \times 3^2$

Since, $p = 2, q = 3, a = 4, b = 2$

Then, $d(144) = (4 + 1)(2 + 1) = 15$ #

The Sum of the Divisors

In considering the factorization of a natural number, we will find the sum of the divisors of the natural number as following method:

Let the natural number *N* have the factorization

$$N = p^a q^b r^c \ldots$$

Where $p, q, r, \ldots$ are the prime factors raised to the powers $a, b, c, \ldots$, respectively. The sum of divisors of N, denoted by $\sigma(N)$, is found by the formula

$$\sigma(N) = (p^0 + p^1 + p^2 + \cdots + p^a)(q^0 + q^1 + q^2 + \cdots + q^b)(r^0 + r^1 + r^2 + \cdots + r^c) \ldots$$

or

$$\sigma(N) = (1 + p^1 + p^2 + \cdots + p^a)(1 + q^1 + q^2 + \cdots + q^b)(1 + r^1 + r^2 + \cdots + r^c) \ldots$$

Example 1: $15 = 3 \times 5$

$$\sigma(15) = (1 + 3)(1 + 5) = 4 \times 6 = 24$$

Check the divisors from Table 4.4: $1 + 3 + 5 + 15 = 24$ #

Example 2: $30 = 2 \times 3 \times 5$

$$\sigma(30) = (1 + 2)(1 + 3)(1 + 5) = 3 \times 4 \times 6 = 72$$

Check the divisors from Table 4.4: $1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72$ #

Example 3: $144 = 2^4 \times 3^2$

$$\sigma(144) = (1 + 2 + 2^2 + 2^3 + 2^4)(1 + 3 + 3^2) = 31 \times 13 = 403$$

Check the divisors from Table 4.4:

$1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 16 + 18 + 24 + 36 + 48 + 72 + 144 = 403$ #

Remark: The formula for $\sigma(N)$ involves not only the exponents but also the prime factors themselves.

Practice 4.3

1. Prove the following properties:

   Property 2: If $a \mid b$ and $a \mid c$, then $a \mid bc$.

   Property 3: If $a \mid b$ and $b \mid c$, then $a \mid c$.

   Property 4: If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever *m* and *n* are integers.
2. Find all integers *n* such that $n \mid (2n + 3)$.
3. Find $d(75) and\ \sigma(75)$.