1. Natural Number

A natural number is a number that occurs commonly and obviously in nature.

Definition 1.1. *The natural numbers, denoted as N, is the set of the positive whole numbers. We denote it as follows:*

$$N = \{0, 1, 2, ...\}$$

A possible second definition for N, that addresses the above criticism, is the following:

$$N = |We\ can\ write\ x\ as\ the\ sum\ 1 + 1 + ... + 1, for\ some\ number\ of 1's.\}$$

.

Example 1.1. *Is* $5 \in N$*? Since* $5 = 1 + 1 + 1 + 1 + 1$ *then,* $5 \in N$.

Theorem 1.1. *For all natural numbers* $m, n,$ *and* p *we have*

1. $m + n \in N$ *(closure +).*
2. $(m + n) + p = m + (n + p)$ *(commutativity +).*
3. $m + n = n + m$ *(associativity +).*
4. $n + 0 = 0$ *(identity +).*
5. $nm \in N$ *(closure .).*
6. $(mn)p = m(np)$ *(commutativity .).*
7. $mn = nm$ *(associativity .).*
8. $m1 = m$ *(identity .).*

Example 1.2. *Let* n, m *and* b *be natural numbers. Then*

$$(mn)b = (mb)n.$$

Sol: Based on Theorem 1.1

$$(mn)b = m(nb)$$

then,

$$m(nb) = m(bn)$$

and,

$$m(bn) = (mb)n.$$

Then,

$$(mn)b = (mb)n.$$

Remark 1.1. *Each $n \in N$ has a successor $n+1$. For example, the successor of 5 is 6.*

Proposition 1.1. *The set N satisfies the following properties:*

N1 $0 \in N$;

N2 *if $n \in N$, then its successor $n+1 \in N$;*

N3 *0 is not the successor of any element in N;*

N4 *if n and m have the same successor, then $n = m$;*

N5 *suppose S is a subset of N satisfying: $1 \in N$ and if $n \in S$ then $n+1 \in S$, then $S = N$.*

Definition 1.2. *Natural number is either the value zero or the successor of some other natural numbers.*

Theorem 1.2. *Let m and n be natural numbers. There exactly one of the following three statement is true:*

1. $m > n$
2. $n > m$
3. $m = n$

1.1. Some result on Natural number (counting numbers)

1. Sum of all first n natural numbers is
$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$
2. Sum of square of all first n natural numbers is
$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$
3. Sum of all cube of all first n natural numbers is
$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$
4. Sum of first n odd natural numbers is
$$1 + 3 + 7 + \cdots = n^2.$$
5. Sum of first n even natural numbers is
$$2 + 4 + 6 + \cdots = n(n+1).$$

2. Mathematical Induction

2.1. The Principle of Mathematical Induction

Suppose we have some statement $P_{(n)}$ and we want to demonstrate that $P_{(n)}$ is true for all $n \in N$. Even if we can provide proofs for

$$P_{(1)}, P_{(2)}, \cdots P_{(k)}$$

where kis some large number, we have accomplished very little. However, there is a general method, the Principle of Mathematical Induction.
Induction is a defining difference between discrete and continuous mathematics.
Principle of Induction. In order to show that $\forall n, P_{(n)}$, holds, it suffices to establish the following two properties:

1. Base case: Show that $P_{(n)}$ holds.
2. Induction step: Assume that $P_{(n)}$ holds, and show that $P_{(n+1)}$ also holds.

2.2. Induction Examples

Example 2.1. *By using mathematical induction prove*

$$3^n - 1$$

a multiple of 2, $\forall n \in N$.

1. *Step one: for* $n = 1$
$$3^1 - 1 = 3 - 1 = 2$$
Since 2 is multiple of 2 then, $3^1 - 1$ *is true*
2. *Assume it is true for* $n = k$
$$3^k - 1$$
is true.
Now, prove that $3^{k+1} - 1$ *is multiple of 2*

$$3^{k+1} - 1 = 3^k 3 - 1 = 3^k(2 + 1) - 1 = 23^k + (3^k - 1)$$

Example 2.2. *Prove for* $n \geq 1$

$$1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + n \times n$$

!= (n+1)!-1

Step one: for $n = 1$ *The left hand side is* $1 \times 1! = 1$. *The right hand side is* $2! - 1 + 1$. *They are equal.*

Assume it is true for $n = k$

$$1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + k \times k! = (k+1)! - 1$$

is true.
Now, prove that for $n = k + 1$

$$\begin{aligned} 1 \times 1! + \cdots + k \times k! + (k+1) \times (k+1)! &= (k+1)! - 1 + (k+1) \times (k+1)! \\ &= [(k+1)! + (k+1) \times (k+1)!] - 1 \\ &= (k+1)![1 + (k+1)] - 1 \\ &= (k+1)![k+2] - 1 \\ &= (k+2)! - 1 \end{aligned}$$

3. Integer number

For several reasons, it is convenient to extend the set N of natural numbers to the group Z of integers by throwing in the identity element 0 and an inverse n for each natural number n. One reason for doing this is to ensure that the difference m n of any two integers is meaningful. Thus Z is a set on which all three operations +, , and × are defined. (The notation Z comes from the German "Zahlen", meaning "numbers".)

Definition 3.1. *An integer numbers is a whole number that can be positive, negative, or zero. The set of integers, denoted Z, is formally defined as follows:*

$$..., -2, -1, 0, 1, 2, ...$$

Theorem 3.1. *Let $a \in Z$ then,*

1. $a + 0 = a$
2. $a - 0 = a$
3. $a.0 = 0.a = 0$
4. $\dfrac{a}{0}$ *is not defined.*
5. $a + a = 2a$
6. $a - a = 0$
7. $a \times a = a^2$
8. $\dfrac{a}{a} = 1$ *(except for $a = 0$, which is not defined, see rule 4)*
9. $a + (-a) = 0$

10. $a - (-a) = 2a$

11. $a \times (-a) = -a^2$

12. $\dfrac{a}{-a} = -1$ *(except for $a = 0$, which is not defined, see rule 4)*

Definition 3.2. *Let $a, b \in Z$,*

1. *$a < b$ if $b - a \in Z$.*

2. *$a \leqslant b$ if $a - b \in Z$.*

Theorem 3.2. *Let $a, b, c \in Z$ then,*

1. *If $a < b$ and $b < c$ then, $a < c$.*

2. *If $a < b$ $c > 0$ then, $ac < bc$.*

Example 3.1. *By using the integers number's properties prove if $a < b$ and $b < c$ then, $ac < bc$.*

Corollary 3.1. *Let a and b be an integer numbers then,*

1. *if $a + c = b + c \rightarrow a = b$*

2. *$(-a)b = -(ab)$*

3. *$(-a)(-b) = ab$*

4. *if $a.b = a.c$ and $c \neq 0 \rightarrow a = b$*

Proof. 1.

$$a + c = b + c$$

$$a + c - c = b + c - c$$

Based on Theorem 3.1(6)

$$a + 0 = b + 0$$

Based on Theorem 3.1(1)

$$a = b$$

2. Based on Theorem 3.1(3)

$$a.0 = 0$$

Based on Theorem 3.1(6)

$$0.a = 0$$

Based on Theorem 3.1(9)

$$(b + (-b))a = -(ab) + (ab)$$

$$ba + (-b)a = (ab) - (ab)$$

Based on Corollary 3.1(1) then,

$$(-b)a = -(ab).$$

3. Based on Corollary 3.1(2) then,

$$(-a)(-b) = -(-ab) = - \cdot -(ab) = ab$$

4. if $a.b = a.c$ and $c \neq 0 \rightarrow a = b$
5. $a \cdot b = 0 \rightarrow$ either $a = 0$ or $b = 0$

□

Theorem 3.3. *Let a and b be an integer numbers then,*

1. *if $a \leqslant b \rightarrow -b \leqslant -a$*
2. *if $a \leqslant b$ $c \leqslant 0 \rightarrow bc \leqslant ac$*
3. *$0 \leqslant a$ and $0 \leqslant b \rightarrow 0 \leqslant ab$*
4. *$0 \leqslant a^2 \bigvee a$.*

Proof. 1. Based on Corollary 3.1(1)

$$a + -b \leqslant b + -b.$$

Based on Theorem 3.1(6)

$$a + -b \leqslant 0.$$
$$-a + a + -b \leqslant -a + 0.$$
$$-b \leqslant -a.$$

2. Based on Theorem 3.3(1) $0 \leqslant -c$ and based on Corollary 3.1(1) then,

$$a \cdot (-c) \leqslant b \cdot (-c)$$
$$-(ac) \leqslant -(bc)$$

Based on Theorem 3.1(1)

$$-a \leqslant -b$$

3. Homework.
4. Homework.

□

3.1. Well-ordering

In mathematics, the well-ordering principle states that every non-empty set of positive integers contains a least element. In other words, the set of positive integers is well-ordered.

1. *Every nonempty subset S of the positive integers has a least element.*
2. *The set of positive integers does not contain any infinite strictly decreasing sequences.*

Theorem 3.4. *There are no positive integers strictly between 0 and 1.*

Proof. Let S be the set of integers x such that $0 < x < 1$ Suppose S is nonempty; let n be its smallest element. Multiplying both sides of $n < 1$ by n gives $n^2 < n$ The square of a positive integer is a positive integer, so n^2 is an integer such that $0 < n < n^2 < 1$. This is a contradiction of the minimality of n. Hence S is empty. □

Theorem 3.5. *1 is the least positive integer.*

Proof. Let $A = \{x \geq 1 | x \in Z^+\}$. We proceed by induction on $n \in Z^+$.
Base Case: For $n = 1$, we have $1 \geq 1$, which works.
Induction Hypothesis: Assume that the claim is true for $n = k$, where k is a positive integer. That is, assume that $k \geq 1$.
It remains to prove the claim true for $n = k + 1$. Since $k \in Z^+$, we know by the definition of the positive integers that $k + 1 \in Z^+$. Recall that $k + 1 > k$. But by the induction hypothesis, we know that $k \geq 1$. Hence, $k + 1 \geq 1$, so the claim is true for $n = k + 1$. This completes the induction. □

Elementary Divisibility Properties

Definition 3.3. *$d \mid n$ means there is an integer k such that $n = dk$. $d \nmid n$ means that $d \mid n$ is false.*

Note that $a \mid b \neq a/b$. Recall that a/b represents the fraction $\frac{a}{b}$.
The expression $d \mid n$ may be read in any of the following ways:

1. *d divides n.*
2. *d is a divisor of n.*
3. *d is a factor of n.*
4. *n is a multiple of d.*

Thus, the following five statements are equivalent, that is, they are all different ways of saying the same thing.

1. $2 \mid 6$.

2. *2 divides 6.*

3. *2 is a divisor of 6.*

4. *2 is a factor of 6.*

5. *6 is a multiple of 2.*

Theorem 3.6. ***Division algorithm*** *Given integers m, n with $n > 0$ then, there exist positive integers q, r such that $(m = qn + rwith 0 \leqslant r < n)$*

Example 3.2. *Find the q and r of the Division Algorithm for the following values of a and b:*

1. *Let $b = 3$ and $a = 0, 1, -1, 10, -10$.*

2. *Let $b = 345$ and $a = 0, -1, 1, 344, 7863, -7863$.*

Example 3.3. *Find the q and r of the Division Algorithm for the following values of a and b:*

1. *Let $b = 3$ and $a = 0, 1, -1, 10, -10$.*

2. *Let $b = 345$ and $a = 0, -1, 1, 344, 7863, -7863$.*

Example 3.4. *Find the q and r of the Division Algorithm for the following values of a and b:*

1. *Let $b = 3$ and $a = 0, 1, -1, 10, -10$.*

2. *Let $b = 345$ and $a = 0, -1, 1, 344, 7863, -7863$.*

Example 3.5. *Use the Division Algorithm to prove that every odd integer is either of the form $4k + 1$ or of the form $4k + 3$ for some integer$k$.*
Let $n \in Z$ be odd. By the division algorithm, there exists unique q and r in Z such that $n = 4q + r$ and $0 \leqslant r < 4$. Clearly $4q$ is even, and thus $0 \neq r \neq 2$ (otherwise $n = 4q$ or $n = 4q + 2$, both of which are even). Thus we conclude that $n = 4k + 1$ or $n = 4k + 3$ as required.

Theorem 3.7. *Let a, b, c be positive integers then,*

1. *if $a|b$ and $b|c$ then, $a|c$.*

2. *if $d|m$ and $d|n$, then $d|(m + n)$.*

Proof. 1. Since $a|b$ and $b|c$ then, there are q_1, q_2 such that $b = q_1 a$ and $c = q_2 b$. It follows that $c = q_1 q_2 a$. So, $a|c$.

2. Let $m = ad$ and $n = bd$, then $(m + n) = (a + b)d$.

□

Definition 3.4. *Let $a, b \in$. If $a \neq 0$ or $b \neq 0$, we define (a, b) to be the largest integer d such that $d \mid a$ and $d \mid b$. We define $(0, 0) = 0$.*

In order not to have to avoid the special case $a = b = 0$, we also define (0,0) as the number 0. By above definition, if at least one of the numbers a and b is nonzero, then

$$d = (a, b) \iff d|a \wedge d|b \wedge (x|a \wedge x|b \Rightarrow x \leqslant d).$$

Example 3.6. *Example 1 The number 102 has the positive divisors 1, 2, 3, 6, 17, 34, 51, 102, and the number 170 has the positive divisors 1, 2, 5, 10, 17, 34, 85, and 170. The common positive divisors are 1, 2, 17, and 34. Hence (102,170) = 34. To determine the greatest common divisor by finding all common divisors is obviously not a feasible method if the given numbers are large.*

Theorem 3.8. *If $(a, b) = 1$ and $a|bc$, then $a|c$.*

Definition 3.5. *An integer n is even if $n = 2k$ for some k, and is odd if $n = 2k + 1$ for some k.*

Definition 3.6. *For $b > 0$ define $a \bmod b = r$ where r is the remainder given by the Division Algorithm when a is divided by b, that is, $a = bq + r$ and $0 \leq r < b$.*

For example $23 \bmod 7 = 2$ *since* $23 = 7 \cdot 3 + 2$ *and* $-4 \bmod 5 = 1$ *since* $-4 = 5 \cdot (-1) + 1$.

Example 3.7. *Calculate the following:*

1. $0 \bmod 10$
2. $123 \bmod 10$
3. $10 \bmod 123$
4. $457 \bmod 33$
5. $(-7) \bmod 3$
6. $(-3) \bmod 7$
7. $(-5) \bmod 5$

4. Prime numbers

Definition 4.1. *An integer > 1 is called a prime number or a prime if it has only trivial divisors. An integer > 1 which is not a prime is called composite.*
In simple language
prime numbers are all those numbers which are only divisible by it self and 1. Thus

$$\forall p > 1 \text{ is a prime number if and only if } 1 > x > p \rightarrow x \nmid p$$

A prime number is a whole number greater than 1 whose only factors are 1 and itself. A factor is a whole numbers that can be divided evenly into another number. The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29. Numbers that have more than two factors are called composite numbers. The number 1 is neither prime nor composite.

- *1 is neither a prime nor a composite number.*
- *2 is the only even number which is prime.*

utf8 One is neither a prime nor a composite number. A prime number is one with exactly two positive divisors, itself and one. One has only one positive divisor. It cannot be written as a product of two factors, neither of which is itself, so one is also not composite. It falls in a class of numbers called units. These are the numbers whose reciprocals are also whole numbers. Zero is not a prime or a composite number either. Zero has an infinite number of divisors (any nonzero whole number divides zero). It cannot be written as a product of two factors, neither of which is itself, so zero is also not composite. It falls in a class of numbers called zero-divisors. These are numbers such that, when multiplied by some nonzero
number, the product is zero.

Theorem 4.1. *Let p be a prime number. If $p|bc$, then $p|b$ or $p|c$.*

Proof. Assume that $p|bc$ but $p \nmid b$. Since p has only trivial divisors, it follows that $(p, b) = 1$. Hence $p|c$ by Theorem 3.8. □

Among the numbers 1 to 6, the numbers 2, 3, and 5 are the prime numbers, while 1, 4, and 6 are not prime. 1 is excluded as a prime number, for reasons explained below. 2 is a prime number, since the only natural numbers dividing it are 1 and 2. Next, 3 is prime, too: 1 and 3 do divide 3 without remainder, but 3 divided by 2 gives remainder 1. Thus, 3 is prime. However, 4 is composite, since 2 is another number (in addition to 1 and 4) dividing 4 without remainder: $4 = 2 \cdot 2$. 5 is again prime: none of the numbers 2, 3, or 4 divide 5. Next, 6 is divisible by 2 or 3, since $6 = 2 \cdot 3$. Hence, 6 is not prime.
Yet another way to say the same is: a number n ¿ 1 is prime if it cannot be written as a product of two integers a and b, both of which are larger than 1:

$$n = a \cdot b.$$

The smallest 168 prime numbers (all the prime numbers under 1000) are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653,

659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997

Lemma 4.1. *Any natural number $n > 1$ is divisible by some prime number.*

Proof. If n is a prime number, then it is divisible by itself. If not, then it is a composite number and is a product $q_1 p_1$ of two numbers different from n and 1. They are smaller than n. If p_1 is prime, then we are done: we found a prime divisor p_1 of n. If not, then p_1 is a composite number, and there exist natural numbers q_2 and p_2 such that $p_1 = q_2 p_2$ (and hence $n = q_1 q_2 p_2$) and $1 < q_2 < p_1, 1 < p_2 < p_1$. Acting in this way, we get eventually either a prime divisor p_k of n, or a sequence of factorizations

$$n = q_1 p_1 = q_1 q_2 p_2 = q_1 q_2 q_3 p_3 = \cdots$$

. in which

$$n > p_1 > p_2 > p_3 > \cdots > 1.$$

A decreasing sequence of natural numbers cannot be infinite. The length is not greater than $n2$. Thus we get a prime divisor of n. □

Lemma 4.2. *$p \cdot q + 1$ is not divisible by p for any natural numbers p and q with $p > 1$.*

Proof. Assume the opposite, then $pq + 1 = pr$ for some natural r. Then

$$p(rq) = 1.$$

Since $p > 1$ and rq is a natural number,

$$p(rq) > 1.$$

Contradiction. □

Theorem 4.2. *The set of prime numbers is infinite.*

Proof. Assume the opposite. Let $p_1, p_2, \cdots, p_n$ be the list of all prime numbers. Consider $N = p_1 p_2 \cdots p_n + 1$. By Lemma 4.1, N is divisible by some prime number. By Lemma 4.2, N is not divisible by any of $p_1, \cdots, p_n$. By assumption, any prime number is one of $p_1, \cdots, p_n$. Contradiction. □

5. Unique Factorization

Our goal in this chapter is to prove the following fundamental theorem.

Theorem 5.1 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be written uniquely in the form*

$$n = p_1 p_2 \cdots p_s,$$

where s is a positive integer and $p_1, p_2, \ldots, p_s$ are primes satisfying

$$p_1 \leq p_2 \leq \cdots \leq p_s.$$

Remark 5.1. *If $n = p_1 p_2 \cdots p_s$ where each p_i is prime, we call this the* ***prime factorization*** *of n. Theorem* **??** *is sometimes stated as follows:*

> *Every integer $n > 1$ can be expressed as a product $n = p_1 p_2 \cdots p_s$, for some positive integer s, where each p_i is prime and this factorization is unique except for the order of the primes p_i.*

Note for example that

$$\begin{aligned} 600 &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \\ &= 2 \cdot 3 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \\ &= 3 \cdot 5 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \\ &\quad \textit{etc.} \end{aligned}$$

Perhaps the nicest way to write the prime factorization of 600 *is*

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

In general it is clear that $n > 1$ can be written uniquely in the form $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, some $s \geq 1$, where $p_1 < p_2 < \cdots < p_s$ and $a_i \geq 1$ for all i. Sometimes $(*)$ is written

$$\boxed{n = \prod_{i=1}^{s} p_i^{a_i}}.$$

Here $\prod$ stands for product, just as $\sum$ stands for sum.

To prove Theorem **??** *we need to first establish a few lemmas.*

Lemma 5.1. *If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$ by Bezout's Lemma there are s, t such that

$$1 = as + bt.$$

If we multiply both sides by c we get

$$c = cas + cbt = a(cs) + (bc)t.$$

By assumption $a \mid bc$. Clearly $a \mid a(cs)$ so, by Theorem **??**, a divides the linear combination $a(cs) + (bc)t = c$. □

Definition 5.1. *We say that a and b are* relatively prime *if* $\gcd(a, b) = 1$.

So we may restate Lemma **??** *as follows:* If $a \mid bc$ and a is relatively prime to b then $a \mid c$.

Example 5.1. *It is not true generally that when $a \mid bc$ then $a \mid b$ or $a \mid c$. For example, $6 \mid 4 \cdot 9$, but $6 \nmid 4$ and $6 \nmid 9$. Note that Lemma* **??** *doesn't apply here since $\gcd(6, 4) \neq 1$ and $\gcd(6, 9) \neq 1$.*