Chapter 1

Introduction

Integers are the building blocks of the theory of numbers. This chapter contains somewhat very simple and obvious observations starting with properties of integers and yet the proofs behind those observations are not as simple. In this chapter we introduce basic operations on integers and some algebraic definitions that will be necessary to understand basic concepts in this book. We then introduce the Well ordering principle which states basically that every set of positive integers has a smallest element. Proof by induction is also presented as an efficient method for proving several theorems throughout the book. We proceed to define the concept of divisibility and the division algorithm. We then introduce the elementary but fundamental concept of a greatest common divisor (gcd) of two integers, and the Euclidean algorithm for finding the gcd of two integers. We end this chapter with Lame's Lemma on an estimate of the number of steps in the Euclidean algorithm needed to find the gcd of two integers.

1.1 Algebraic Operations With Integers

The set $\mathbb{Z}$ of all integers, which this book is all about, consists of all positive and negative integers as well as 0. Thus $\mathbb{Z}$ is the set given by

$$\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}. \tag{1.1}$$

While the set of all *positive* integers, denoted by $\mathbb{N}$, is defined by

$$\mathbb{N} = \{1, 2, 3, 4, ...\}. \tag{1.2}$$

On $\mathbb{Z}$, there are two basic binary operations, namely **addition** (denoted by $+$) and **multiplication** (denoted by $\cdot$), that satisfy some basic properties from which every other property for $\mathbb{Z}$ emerges.

1. **The Commutativity property for addition and multiplication**

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

2. **Associativity property for addition and multiplication**

$$\begin{aligned} (a + b) + c &= a + (b + c) \\ (a \cdot b) \cdot c &= a \cdot (b \cdot c) \end{aligned}$$

3. **The distributivity property of multiplication over addition**

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

In the set $\mathbb{Z}$ there are "identity elements" for the two operations $+$ and $\cdot$, and these are the elements 0 and 1 respectively, that satisfy the basic properties

$$a + 0 = 0 + a = a$$
$$a \cdot 1 = 1 \cdot a = a$$

for every $a \in \mathbb{Z}$.

The set $\mathbb{Z}$ allows **additive inverses** for its elements, in the sense that for every $a \in \mathbb{Z}$ there exists another integer in $\mathbb{Z}$, denoted by $-a$, such that

$$a + (-a) = 0. \tag{1.3}$$

While for multiplication, only the integer 1 has a **multiplicative inverse** in the sense that 1 is the only integer a such that there exists another integer, denoted by a^{-1} or by $1/a$, (namely 1 itself in this case) such that

$$a \cdot a^{-1} = 1. \tag{1.4}$$

From the operations of addition and multiplication one can define two other operations on $\mathbb{Z}$, namely **subtraction** (denoted by $-$) and **division** (denoted by $/$). Subtraction is a binary operation on $\mathbb{Z}$, i.e. defined for any two integers in $\mathbb{Z}$, while division is not a binary operation and thus is defined only for some specific couple of integers in $\mathbb{Z}$. Subtraction and division are defined as follows:

1. $a - b$ is defined by $a + (-b)$, i.e. $a - b = a + (-b)$ for every $a, b \in \mathbb{Z}$
2. a/b is defined by the integer c if and only if $a = b \cdot c$.

1.2 The Well Ordering Principle and Mathematical Induction

In this section, we present three basic tools that will often be used in proving properties of the integers. We start with a very important property of integers called

the well ordering principle. We then state what is known as the pigeonhole principle, and then we proceed to present an important method called mathematical induction.

1.2.1 The Well Ordering Principle

The Well Ordering Principle: A least element exist in any non empty set of positive integers.

This principle can be taken as an axiom on integers and it will be the key to proving many theorems. As a result, we see that any set of positive integers is well ordered while the set of all integers is not well ordered.

1.2.2 The Pigeonhole Principle

The Pigeonhole Principle: If s objects are placed in k boxes for $s > k$, then at least one box contains more than one object.

Proof. Suppose that none of the boxes contains more than one object. Then there are at most k objects. This leads to a contradiction with the fact that there are s objects for $s > k$. □

1.2.3 The Principle of Mathematical Induction

We now present a valuable tool for proving results about integers. This tool is the principle of mathematical induction .

Theorem 1. ***The First Principle of Mathematical Induction:*** *If a set of positive integers has the property that, if it contains the integer k, then it also contains*

$k+1$, and if this set contains 1 then it must be the set of all positive integers. More generally, a property concerning the positive integers that is true for $n=1$, and that is true for the integer $n+1$ whenever it is true for the integer n, must be true for all positive integers.

We use the well ordering principle to prove the first principle of mathematical induction

Proof. Let S be the set of positive integers containing the integer 1, and the integer $k+1$ whenever it contains k. Assume also that S is not the set of all positive integers. As a result, there are some integers that are not contained in S and thus those integers must have a least element α by the well ordering principle. Notice that $\alpha \neq 1$ since $1 \in S$. But $\alpha - 1 \in S$ and thus using the property of S, $\alpha \in S$. Thus S must contain all positive integers. □

We now present some examples in which we use the principle of induction.

Example 1. *Use mathematical induction to show that* $\forall n \in \mathbb{N}$

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}. \tag{1.5}$$

First note that

$$\sum_{j=1}^{1} j = 1 = \frac{1 \cdot 2}{2}$$

and thus the the statement is true for $n = 1$. For the remaining inductive step, suppose that the formula holds for n, that is $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$. We show that

$$\sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2}.$$

to complete the proof by induction. Indeed

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

and the result follows.

Example 2. *Use mathematical induction to prove that* $n! \leq n^n$ *for all positive integers* n*.*

Note that $1! = 1 \leq 1^1 = 1$. We now present the inductive step. Suppose that

$$n! \leq n^n$$

for some n, we prove that $(n+1)! \leq (n+1)^{n+1}$. Note that

$$(n+1)! = (n+1)n! \leq (n+1).n^n < (n+1)(n+1)^n = (n+1)^{n+1}.$$

This completes the proof.

Theorem 2. ***The Second Principle of Mathematical Induction:*** *A set of positive integers that has the property that for every integer* k*, if it contains all the integers 1 through* k *then it contains* $k+1$ *and if it contains 1 then it must be the set of all positive integers. More generally, a property concerning the positive integers that is true for* $n = 1$*, and that is true for all integers up to* $n+1$ *whenever it is true for all integers up to* n*, must be true for all positive integers.*

The second principle of induction is also known as **the principle of strong induction**. Also, the first principle of induction is known as **the principle of weak induction**.

To prove the second principle of induction, we use the first principle of induction.

Proof. Let T be a set of integers containing 1 and such that for every positive integer k, if it contains $1, 2, ..., k$, then it contains $k+1$. Let S be the set of all positive integers k such that all the positive integers less than or equal to k are in T. Then 1 is in S, and we also see that $k+1$ is in S. Thus S must be the set of all positive integers. Thus T must be the set of all positive integers since S is a subset of T. □

Exercises

1. Prove using mathematical induction that $n < 3^n$ for all positive integers n.
2. Show that $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$.
3. Use mathematical induction to prove that $\sum_{j=1}^{n}(-1)^{j-1}j^2 = (-1)^{n-1}n(n+1)/2$.
4. Use mathematical induction to prove that $\sum_{j=1}^{n} j^3 = [n(n+1)/2]^2$ for every positive integer n.
5. Use mathematical induction to prove that $\sum_{j=1}^{n}(2j-1) = n^2$
6. Use mathematical induction to prove that $2^n < n!$ for $n \geq 4$.
7. Use mathematical induction to prove that $n^2 < n!$ for $n \geq 4$.

1.3 Divisibility and the Division Algorithm

We now discuss the concept of divisibility and its properties.

1.3.1 Integer Divisibility

Definition 1. *If a and b are integers such that $a \neq 0$, then we say "a divides b" if there exists an integer k such that $b = ka$.*

If a divides b, we also say "a is a factor of b" or "b is a multiple of a" and we write $a \mid b$. If a doesn't divide b, we write $a \nmid b$. For example $2 \mid 4$ and $7 \mid 63$, while $5 \nmid 26$.

Example 3. *a) Note that any even integer has the form $2k$ for some integer k, while any odd integer has the form $2k+1$ for some integer k. Thus $2|n$ if n is even, while $2 \nmid n$ if n is odd.*

b) $\forall a \in \mathbb{Z}$ *one has that* $a \mid 0$.
c) If $b \in \mathbb{Z}$ *is such that* $|b| < a$, *and* $b \neq 0$, *then* $a \nmid b$.

Theorem 3. *If* a, b *and* c *are integers such that* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

Proof. Since $a \mid b$ and $b \mid c$, then there exist integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$. As a result, we have $c = k_1 k_2 a$ and hence $a \mid c$. □

Example 4. *Since* $6 \mid 18$ *and* $18 \mid 36$, *then* $6 \mid 36$.

The following theorem states that if an integer divides two other integers then it divides any linear combination of these integers.

Theorem 4. *If* a, b, c, m *and* n *are integers, and if* $c \mid a$ *and* $c \mid b$, *then* $c \mid (ma + nb)$.

Proof. Since $c \mid a$ and $c \mid b$, then by definition there exists k_1 and k_2 such that $a = k_1 c$ and $b = k_2 c$. Thus

$$ma + nb = mk_1 c + nk_2 c = c(mk_1 + nk_2),$$

and hence $c \mid (ma + nb)$. □

Theorem 4 can be generalized to any finite linear combination as follows. If

$$a \mid b_1, a \mid b_2, ..., a \mid b_n$$

then

$$a \mid \sum_{j=1}^{n} k_j b_j \tag{1.6}$$

for any set of integers $k_1, \cdots, k_n \in \mathbb{Z}$. It would be a nice exercise to prove the generalization by induction.

1.3.2 The Division Algorithm

The following theorem states somewhat an elementary but very useful result.

Theorem 5. ***The Division Algorithm*** *If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.*

Proof. Consider the set $A = \{a - bk \geq 0 \mid k \in \mathbb{Z}\}$. Note that A is nonempty since for $k < a/b$, $a - bk > 0$. By the well ordering principle, A has a least element $r = a - bq$ for some q. Notice that $r \geq 0$ by construction. Now if $r \geq b$ then (since $b > 0$)

$$r > r - b = a - bq - b = a - b(q + 1) =\geq 0.$$

This leads to a contradiction since r is assumed to be the least positive integer of the form $r = a - bq$. As a result we have $0 \leq r < b$.

We will show that q and r are unique. Suppose that $a = bq_1 + r_1$ and $a = bq_2 + r_2$ with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Then we have

$$b(q_1 - q_2) + (r_1 - r_2) = 0.$$

As a result we have

$$b(q_1 - q_2) = r_2 - r_1.$$

Thus we get that

$$b \mid (r_2 - r_1).$$

And since $-\max(r_1, r_2) \leq |r_2 - r_1| \leq \max(r_1, r_2)$, and $b > \max(r_1, r_2)$, then $r_2 - r_1$ must be 0, i.e. $r_2 = r_1$. And since $bq_1 + r_1 = bq_2 + r_2$, we also get that $q_1 = q_2$. This proves uniqueness. □

Example 5. *If $a = 71$ and $b = 6$, then $71 = 6 \cdot 11 + 5$. Here $q = 11$ and $r = 5$.*

Exercises

1. Show that $5 \mid 25, 19 \mid 38$ and $2 \mid 98$.

2. Use the division algorithm to find the quotient and the remainder when 76 is divided by 13.

3. Use the division algorithm to find the quotient and the remainder when -100 is divided by 13.

4. Show that if a, b, c and d are integers with a and c nonzero, such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.

5. Show that if a and b are positive integers and $a \mid b$, then $a \leq b$.

6. Prove that the sum of two even integers is even, the sum of two odd integers is even and the sum of an even integer and an odd integer is odd.

7. Show that the product of two even integers is even, the product of two odd integers is odd and the product of an even integer and an odd integer is even.

8. Show that if m is an integer then 3 divides $m^3 - m$.

9. Show that the square of every odd integer is of the form $8m + 1$.

10. Show that the square of any integer is of the form $3m$ or $3m + 1$ but not of the form $3m + 2$.

11. Show that if $ac \mid bc$, then $a \mid b$.

12. Show that if $a \mid b$ and $b \mid a$ then $a = \pm b$.

1.4 Representations of Integers in Different Bases

In this section, we show how any positive integer can be written in terms of any positive base integer expansion in a unique way. Normally we use decimal notation to represent integers, we will show how to convert an integer from decimal notation into any other positive base integer notation and vise versa. Using the

decimal notation in daily life is simply better because we have ten fingers which facilitates all the mathematical operations.

Notation An integer a written in base b expansion is denoted by $(a)_b$.

Theorem 6. *Let b be a positive integer with $b > 1$. Then any positive integer m can be written uniquely as*

$$m = a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0,$$

where l is a positive integer, $0 \leq a_j < b$ for $j = 0, 1, ..., l$ and $a_l \neq 0$.

Proof. We start by dividing m by b and we get

$$m = bq_0 + a_0, \quad 0 \leq a_0 < b.$$

If $q_0 \neq 0$ then we continue to divide q_0 by b and we get

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b.$$

We continue this process and hence we get

$$\begin{aligned} q_1 &= bq_2 + a_2, \quad 0 \leq a_2 < b, \\ &\vdots \\ q_{l-2} &= bq_{l-1} + a_{l-1}, \quad 0 \leq a_{l-1} < b, \\ q_{l-1} &= b \cdot 0 + a_l, \quad 0 \leq a_l < b. \end{aligned}$$

Note that the sequence $q_0, q_1, ...$ is a decreasing sequence of positive integers with a last term q_l that must be 0.

Now substituting the equation $q_0 = bq_1 + a_1$ in $m = bq_0 + a_0$, we get

$$m = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0,$$

Successively substituting the equations in m, we get

$$\begin{aligned} m &= b^3 q_2 + a_2 b^2 + a_1 b + a_0, \\ &\cdot \\ &\cdot \\ &\cdot \\ &= b^l q_{l-1} + a_{l-1} b^{l-1} + ... + a_1 b + a_0, \\ &= a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0. \end{aligned}$$

What remains to prove is that the representation is unique. Suppose now that

$$m = a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0 = c_l b^l + c_{l-1} b^{l-1} + ... + c_1 b + c_0$$

where if the number of terms is different in one expansion, we add zero coefficients to make the number of terms agree. Subtracting the two expansions, we get

$$(a_l - c_l) b^l + (a_{l-1} - c_{l-1}) b^{l-1} + ... + (a_1 - c_1) b + (a_0 - c_0) = 0.$$

If the two expansions are different, then there exists $0 \leq j \leq l$ such that $c_j \neq a_j$. As a result, we get

$$b^j ((a_l - c_l) b^{l-j} + ... + (a_{j+1} - c_{j+1}) b + (a_j - c_j)) = 0$$

and since $b \neq 0$, we get

$$(a_l - c_l) b^{l-j} + ... + (a_{j+1} - c_{j+1}) b + (a_j - c_j) = 0.$$

We now get

$$a_j - c_j = (a_l - c_l) b^{l-j} + ... + (a_{j+1} - c_{j+1}) b,$$

and as a result, $b \mid (a_j - c_j)$. Since $0 \leq a_j < b$ and $0 \leq c_j < b$, we get that $a_j = c_j$. This is a contradiction and hence the expansion is unique. $\square$

Note that base 2 representation of integers is called binary representation. Binary representation plays a crucial role in computers. Arithmetic operations can be carried out on integers with any positive integer base but it will not be addressed in this book. We now present examples of how to convert from decimal integer representation to any other base representation and vise versa.

Example 6. *To find the expansion of 214 base 3:*

we do the following

$$\begin{aligned} 214 &= 3 \cdot 71 + 1 \\ 71 &= 3 \cdot 23 + 2 \\ 23 &= 3 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 3 \cdot 0 + 2 \end{aligned}$$

As a result, to obtain a base 3 expansion of 214, we take the remainders of divisions and we get that $(214)_{10} = (21221)_3$.

Example 7. *To find the base 10 expansion, i.e. the decimal expansion, of* $(364)_7$*:*

We do the following: $4 \cdot 7^0 + 6 \cdot 7^1 + 3 \cdot 7^2 = 4 + 42 + 147 = 193$.

In some cases where base $b > 10$ expansion is needed, we add some characters to represent numbers greater than 9. It is known to use the alphabetic letters to denote integers greater than 9 in base b expansion for $b > 10$. For example $(46BC29)_{13}$ where $A = 10, B = 11, C = 12$.

To convert from one base to the other, the simplest way is to go through base 10 and then convert to the other base. There are methods that simplify conversion from one base to the other but it will not be addressed in this book.

Exercises

1. Convert $(7482)_{10}$ to base 6 notation.

2. Convert $(98156)_{10}$ to base 8 notation.

3. Convert $(101011101)_2$ to decimal notation.

4. Convert $(AB6C7D)_{16}$ to decimal notation.

5. Convert $(9A0B)_{16}$ to binary notation.

1.5 The Greatest Common Divisor

In this section we define the greatest common divisor (gcd) of two integers and discuss its properties. We also prove that the greatest common divisor of two integers is a linear combination of these integers.

Two integers a and b, not both 0, can have only finitely many divisors, and thus can have only finitely many common divisors. In this section, we are interested in the greatest common divisor of a and b. Note that the divisors of a and that of $\mid a \mid$ are the same.

Definition 2. *The greatest common divisor of two integers a and b is the greatest integer that divides both a and b.*

We denote the greatest common divisor of two integers a and b by (a, b). We also define $(0, 0) = 0$.

Example 8. *Note that the greatest common divisor of 24 and 18 is 6. In other words* $(24, 18) = 6$.

There are couples of integers (e.g. 3 and 4, etc...) whose greatest common divisor is 1 so we call such integers relatively prime integers.

Definition 3. *Two integers a and b are relatively prime if* $(a, b) = 1$.

Example 9. *The greatest common divisor of 9 and 16 is 1, thus they are relatively prime.*

Note that every integer has positive and negative divisors. If a is a positive divisor of m, then $-a$ is also a divisor of m. Therefore by our definition of the greatest common divisor, we can see that $(a, b) = (\mid a \mid, \mid b \mid)$.

We now present a theorem about the greatest common divisor of two integers. The theorem states that if we divide two integers by their greatest common divisor, then the outcome is a couple of integers that are relatively prime.

Theorem 7. *If* $(a, b) = d$ *then* $(a/d, b/d) = 1$.

Proof. We will show that a/d and b/d have no common positive divisors other than 1. Assume that k is a positive common divisor such that $k \mid a/d$ and $k \mid b/d$. As a result, there are two positive integers m and n such that

$$a/d = km \quad \text{and} \quad b/d = kn$$

Thus we get that

$$a = kmd \quad \text{and} \quad b = knd.$$

Hence kd is a common divisor of both a and b. Also, $kd \geq d$. However, d is the greatest common divisor of a and b. As a result, we get that $k = 1$. □

The next theorem shows that the greatest common divisor of two integers does not change when we add a multiple of one of the two integers to the other.

Theorem 8. *Let* a, b *and* c *be integers. Then* $(a, b) = (a + cb, b)$.

Proof. We will show that every divisor of a and b is also a divisor of $a + cb$ and b and vise versa. Hence they have exactly the same divisors. So we get that the greatest common divisor of a and b will also be the greatest common divisor of $a + cb$ and b. Let k be a common divisor of a and b. By Theorem 4, $k \mid (a + cb)$

and hence k is a divisor of $a+cb$. Now assume that l is a common divisor of $a+cb$ and b. Also by Theorem 4 we have ,

$$l \mid ((a + cb) - cb) = a.$$

As a result, l is a common divisor of a and b and the result follows. □

Example 10. *Notice that* $(4, 14) = (4, 14 - 3 \cdot 4) = (4, 2) = 2$.

We now present a theorem which proves that the greatest common divisor of two integers can be written as a linear combination of the two integers.

Theorem 9. *The greatest common divisor of two integers* a *and* b*, not both* 0 *is the least positive integer such that* $ma + nb = d$ *for some integers* m *and* n*.*

Proof. Assume without loss of generality that a and b are positive integers. Consider the set of all positive integer linear combinations of a and b. This set is non empty since $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$ are both in this set. Thus this set has a least element d by the well-ordering principle. Thus $d = ma + nb$ for some integers m and n. We have to prove that d divides both a and b and that it is the greatest divisor of a and b.

By the division algorithm, we have

$$a = dq + r, \quad 0 \leq r < d.$$

Thus we have

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

We then have that r is a linear combination of a and b. Since $0 \leq r < d$ and d is the least positive integer which is a linear combination of a and b, then $r = 0$ and $a = dq$. Hence $d \mid a$. Similarly $d \mid b$. Now notice that if there is a divisor c that divides both a and b. Then c divides any linear combination of a and b by Theorem 4. Hence $c \mid d$. This proves that any common divisor of a and b divides d. Hence $c \leq d$, and d is the greatest divisor. □

As a result, we conclude that if $(a, b) = 1$ then there exist integers m and n such that $ma + nb = 1$.

Definition 4. *Let $a_1, a_2, ..., a_n$ be integers, not all 0. The greatest common divisor of these integers is the largest integer that divides all of the integers in the set. The greatest common divisor of $a_1, a_2, ..., a_n$ is denoted by $(a_1, a_2, ..., a_n)$.*

Definition 5. *The integers $a_1, a_2, ..., a_n$ are said to be mutually relatively prime if $(a_1, a_2, ..., a_n) = 1$.*

Example 11. *The integers $3, 6, 7$ are mutually relatively prime since $(3, 6, 7) = 1$ although $(3, 6) = 3$.*

Definition 6. *The integers $a_1, a_2, ..., a_n$ are called pairwise prime if for each $i \neq j$, we have $(a_i, a_j) = 1$.*

Example 12. *The integers $3, 14, 25$ are pairwise relatively prime. Notice also that these integers are mutually relatively prime.*

Notice that if $a_1, a_2, ..., a_n$ are pairwise relatively prime then they are mutually relatively prime.

Exercises

1. Find the greatest common divisor of 15 and 35.
2. Find the greatest common divisor of 100 and 104.
3. Find the greatest common divisor of -30 and 95.
4. Let m be a positive integer. Find the greatest common divisor of m and $m + 1$.

5. Let m be a positive integer, find the greatest common divisor of m and $m + 2$.

6. Show that if m and n are integers such that $(m, n) = 1$, then (m+n,m-n)=1 or 2.

7. Show that if m is a positive integer, then $3m + 2$ and $5m + 3$ are relatively prime.

8. Show that if a and b are relatively prime integers, then $(a+2b, 2a+b) = 1$or 3.

9. Show that if $a_1, a_2, ..., a_n$ are integers that are not all 0 and c is a positive integer, then $(ca_1, ca_2, ..., ca_n) = c(a_1, a_2, ...a_n)$.

1.6 The Euclidean Algorithm

In this section we describe a systematic method that determines the greatest common divisor of two integers. This method is called the Euclidean algorithm.

Lemma 1. *If a and b are two integers and $a = bq + r$ where also q and r are integers, then $(a, b) = (r, b)$.*

Proof. Note that by theorem 8, we have $(bq + r, b) = (b, r)$. □

The above lemma will lead to a more general version of it. We now present the Euclidean algorithm in its general form. It states that the greatest common divisor of two integers is the last non zero remainder of the successive division.

Theorem 10. *Let $a = r_0$ and $b = r_1$ be two positive integers where $a \geq b$. If we apply the division algorithm successively to obtain that*

$$r_j = r_{j+1}q_{j+1} + r_{j+2} \text{ where } 0 \leq r_{j+2} < r_{j+1}$$

for all $j = 0, 1, ..., n-2$ *and*

$$r_{n+1} = 0.$$

Then $(a, b) = r_n$.

Proof. By applying the division algorithm, we see that

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Notice that, we will have a remainder of 0 eventually since all the remainders are integers and every remainder in the next step is less than the remainder in the previous one. By Lemma 1, we see that

$$(a, b) = (b, r_2) = (r_2, r_3) = ... = (r_n, 0) = r_n.$$

□

Example 13. *We will find the greatest common divisor of* 4147 *and* 10672*:*

Note that

$$\begin{aligned} 10672 &= 4147 \cdot 2 + 2378, \\ 4147 &= 2378 \cdot 1 + 1769, \\ 2378 &= 1769 \cdot 1 + 609, \\ 1769 &= 609 \cdot 2 + 551, \\ 609 &= 551 \cdot 1 + 58, \\ 551 &= 58 \cdot 9 + 29, \\ 58 &= 29 \cdot 2, \end{aligned}$$

Hence $(4147, 10672) = 29$.

We now use the steps in the Euclidean algorithm to write the greatest common divisor of two integers as a linear combination of the two integers. The following example will actually determine the variables m and n described in Theorem 9. The following algorithm can be described by a general form but for the sake of simplicity of expressions we will present an example that shows the steps for obtaining the greatest common divisor of two integers as a linear combination of the two integers.

Example 14. *Express 29 as a linear combination of* 4147 *and* 10672*:*

$$\begin{aligned}
29 &= 551 - 9 \cdot 58, \\
&= 551 - 9(609 - 551 \cdot 1), \\
&= 10.551 - 9.609, \\
&= 10 \cdot (1769 - 609 \cdot 2) - 9 \cdot 609, \\
&= 10 \cdot 1769 - 29 \cdot 609, \\
&= 10 \cdot 1769 - 29(2378 - 1769 \cdot 1), \\
&= 39 \cdot 1769 - 29 \cdot 2378, \\
&= 39(4147 - 2378 \cdot 1) - 29 \cdot 2378, \\
&= 39 \cdot 4147 - 68 \cdot 2378, \\
&= 39 \cdot 4147 - 68(10672 - 4147 \cdot 2), \\
&= 175 \cdot 4147 - 68 \cdot 10672,
\end{aligned}$$

As a result, we see that $29 = 175 \cdot 4147 - 68 \cdot 10672$.

Exercises

1. Use the Euclidean algorithm to find the greatest common divisor of 412 and 32 and express it in terms of the two integers.

2. Use the Euclidean algorithm to find the greatest common divisor of 780 and 150 and express it in terms of the two integers.

3. Find the greatest common divisor of $70, 98, 108$.

4. Let a and b be two positive even integers. Prove that $(a, b) = 2(a/2, b/2)$.

5. Show that if a and b are positive integers where a is even and b is odd, then $(a, b) = (a/2, b)$.

1.7 Lame's Theorem

In this section, we give an estimate to the number of steps needed to find the greatest common divisor of two integers using the Euclidean algorithm. To do this, we have to introduce the Fibonacci numbers for the sake of proving a lemma that gives an estimate on the growth of Fibonacci numbers in the Fibonacci sequence. The lemma that we prove will be used in the proof of Lame's theorem.

Definition 7. *The Fibonacci sequence is defined recursively by* $f_1 = 1$, $f_2 = 1$, *and*

$$f_n = f_{n-1} + f_{n-2} \textit{for } n \geq 3.$$

The terms in the sequence are called Fibonacci numbers.

In the following lemma, we give a lower bound on the growth of Fibonacci numbers. We will show that Fibonacci numbers grow faster than a geometric series with common ratio $\alpha = (1 + \sqrt{5})/2$.

Lemma 2. *For* $n \geq 3$, *we have* $f_n > \alpha^{n-2}$ *where* $\alpha = (1 + \sqrt{5})/2$.

Proof. We use the second principle of mathematical induction to prove our result. It is easy to see that this is true for $n = 3$ and $n = 4$. Assume that $\alpha^{k-2} < f_k$ for all integers k where $k \leq n$. Now since α is a solution of the polynomial $x^2 - x - 1 = 0$, we have $\alpha^2 = \alpha + 1$. Hence

$$\alpha^{n-1} = \alpha^2.\alpha^{n-3} = (\alpha + 1).\alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}.$$

By the inductive hypothesis, we have

$$\alpha^{n-2} < f_n, \quad \alpha^{n-3} < f_{n-1}.$$

After adding the two inequalities, we get

$$\alpha^{n-1} < f_n + f_{n-1} = f_{n+1}.$$

□

We now present Lame's theorem.

Theorem 11. *using the Euclidean algorithm to find the greatest common divisor of two positive integers has number of divisions less than or equal five times the number of decimal digits in the minimum of the two integers.*

Proof. Let a and b be two positive integers where $a > b$. Applying the Euclidean algorithm to find the greatest common divisor of two integers with $a = r_0$ and $b = r_1$, we get

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Notice that each of the quotients $q_1, q_2, ..., q_{n-1}$ are all greater than 1 and $q_n \geq 2$ and this is because $r_n < r_{n-1}$. Thus we have

$$\begin{aligned}
r_n &\geq 1 = f_2, \\
r_{n-1} &\geq 2r_n \geq 2f_2 = f_3, \\
r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4, \\
r_{n-3} &\geq r_{n-2} + r_{n-1} \geq f_4 + f_3 = f_5, \\
&\vdots \\
r_2 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n, \\
b &= r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.
\end{aligned}$$

Thus notice that $b \geq f_{n+1}$. By Lemma 2, we have $f_{n+1} > \alpha^{n-1}$ for $n > 2$. As a result, we have $b > \alpha^{n-1}$. Now notice since

$$\log_{10} \alpha > \frac{1}{5},$$

we see that

$$log_{10}b > (n-1)/5.$$

Thus we have

$$n - 1 < 5log_{10}b.$$

Now let b has k decimal digits. As a result, we have $b < 10^k$ and thus $log_{10}b < k$. Hence we conclude that $n - 1 < 5k$. Since k is an integer, we conclude that $n \leq 5k$. □

Exercises

1. Find an upper bound for the number of steps in the Euclidean algorithm that is used to find the greatest common divisor of 38472 and 957748838.

2. Find an upper bound for the number of steps in the Euclidean algorithm that is used to find the greatest common divisor of 15 and 75. Verify your result by using the Euclidean algorithm to find the greatest common divisor of the two integers.