CHAPTER One

Number System

زانکۆی سەلاحەددین ـ هەولێر
Salahaddin University-Erbil

Mathematics is the Queen of Sciences and Arithmetic is the Queen of Mathematics

Carl Friedrich Gauss(1777 –1855)

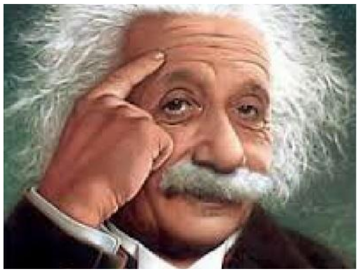
Lecture notes (2024-2025)

Fourth Year Class

by Herish O. Abdullah

& Andam A. Mustafa

Preface: Number Systems



If you can't explain it simply, you don't understand it well enough.

Albert Einstein (1879-1955)

What is Number Theory?

When humans first started using numbers, they probably used the counting or natural numbers, ℕ, first. These are the numbers in the set $\mathbb{N} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \ldots,\}$.

What is $\mathbf{5} - \mathbf{5}$**?** We need a new number, call it zero, to mean nothing. Then we get the whole numbers, $\mathbb{w} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \ldots,\}$. Next, come the integers, which include 0 and the negatives of all the natural numbers. The letter $\boldsymbol{Z}$ stands for the integers, and comes from the German word for number, **zahlen**.

Number theory is the study of the set of natural numbers ℕ. We will especially want to study the relationships between different sorts of numbers. Since ancient times, people have separated the natural numbers into a variety of different types. Here are some familiar and not-so-familiar examples:

Odd	**1, 3, 5, 7, 9, 11, ...**
Even	**2, 4, 6, 8, 10, ...**
Square	**1, 4, 9, 16, 25, 36, ...**
Cube	**1, 8, 27, 64, 125, ...**
Prime	**2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...**
Composite	**4,6,8,9,10,12,14,15,16, ...**
1(modulo 4)	**1,5,9,13,17,21,25, .. .**
3 (modulo 4)	**3,7,11,15,19,23,27, .. .**
Triangular	**1,3,6,10,15,21, ...**

Perfect	**6, 28, 496, ...**
Fibonacci	**1, 1, 2, 3, 5, 8, 13, 21, ...**

Many of these types of numbers are undoubtedly already known to you. Others may not be familiar. The **Fibonacci numbers** are created by starting with **1** and **1**. Then, to get the next number in the list, just add the previous two.

A number is **perfect** if the sum of all its divisors, other than itself, adds back up to the original number. Thus, the numbers dividing **6** are **1**, **2**, and **3**, and

1 + 2 + 3 = 6.

Similarly, the divisors of **28** are **1, 2, 4, 7,** and **14**, and **1 + 2 + 4 + 7 + 14 = 28.**

We will encounter some of these types of numbers in our excursion through the theory of numbers.

Twin Primes In the list of primes it is sometimes true that **consecutive odd numbers** are both prime. We have boxed these twin primes in the following list of primes less than 100:

3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61
67 71 73 79 83 89 97

Are there infinitely many twin primes? That is, are there infinitely many prime numbers $\boldsymbol{p}$ such that $\boldsymbol{p+2}$ is also a prime? At present, no one knows the answer to this question.

Primes of the Form $\mathbf{N^2+1}$ If we list the numbers of the form $\mathbf{N^2+1}$ taking **N** = 1, 2, 3, ... , we find that some of them are prime. Of course, if **N** is odd, then $\mathbf{N^2+1}$ is even, so it won't be prime unless $\mathbf{N=1}$. So it's really only interesting to take even values of **N**. We've highlighted the primes in the following list:

$$2^2 + 1 = 5, \qquad 4^2 + 1 = 17, \qquad 6^2 + 1 = 37, \qquad 8^2 + 1 = 65 = 5.15,$$

$$10^2 + 1 = 101, \qquad 12^2 + 1 = 145 = 5.29\,, \qquad 14^2 + 1 = 197,$$

$$16^2 + 1 = 257, \qquad 18^2 + 1 = 325 = 5^2.13, \qquad 20^2 + 1 = 401.$$

It looks like there are quite a few prime values, but if you take larger values of N you will find that they become much rarer. So we ask whether there are infinitely many primes of the form $\mathbf{N^2 + 1}$. Again, no one presently knows the answer to this question.

Some typical number theoretic questions

<u>Sums of Squares I</u>. Can the sum of two squares be a square? The answer is clearly "**YES**"; for example $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. These are examples of **Pythagorean triples**.

<u>Sums of Squares II</u>. Which numbers are sums of two squares? It often turns out that questions of this sort are easier to answer first for primes, so we ask which (odd) prime numbers is a sum of two squares. For example,

$$3 = No, \qquad 5 = 1^2 + 2^2, \qquad 7 = No, \qquad 11 = No, \qquad 13 = 2^2 + 3^2,$$

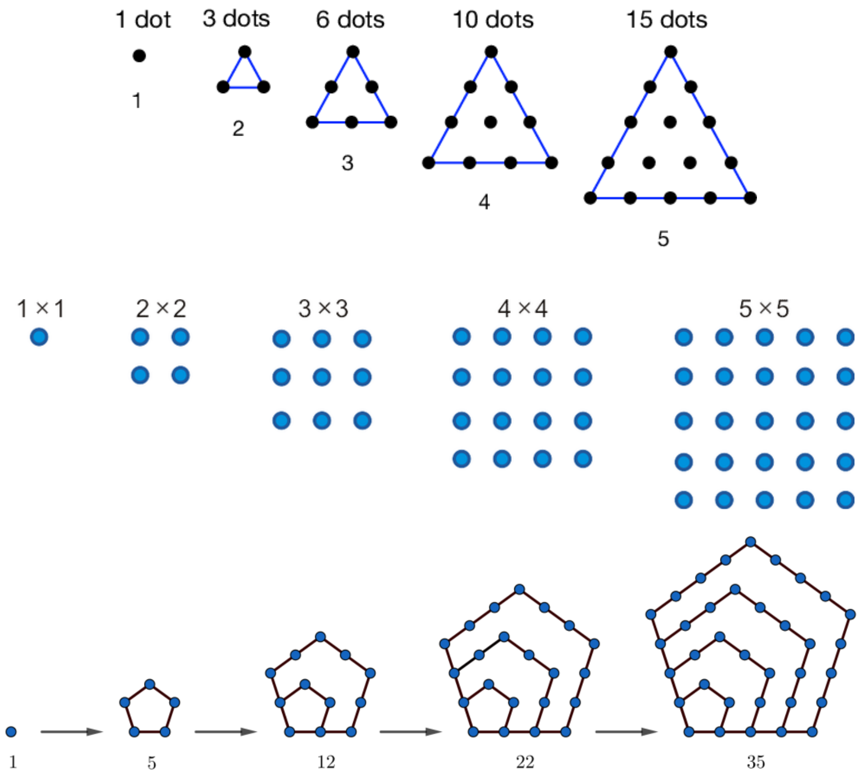
$$17 = 1^2 + 4^2, \qquad 19 = No, \qquad 23 = No, \qquad 29 = 2^2 + 5^2, \qquad 31 = No.$$

Do you see a pattern? Possibly not, since this is only a short list, but a longer list leads to the conjecture that **p** is a sum of two squares if it is congruent to **1 modulo 4**. In other words, **p** is a sum of two squares if it leaves a remainder of **1** when divided by **4**, and it is not a sum of two squares if it leaves a remainder of **3**.

<u>Sums of Higher Powers</u> Can the sum of two cubes be a cube? Can the sum of two fourth powers be a fourth power? In general, can the sum of two nth powers be an nth power? The answer is "**NO**." This famous problem, called **Fermat's Last Theorem**, states that no three positive integers $\boldsymbol{a}$,$\boldsymbol{b}$,$\boldsymbol{c}$ can satisfy the equation $\boldsymbol{a^n + b^n = c^n}$ for any integer value of $n > 2$. This theorem was first **conjectured** by **Pierre de Fermat** in **1637**, but was not completely solved until **1994** by **Andrew Wiles**.

Number Shapes The **square numbers** are the numbers **1, 4, 9, 16, 25, ...** that can be arranged in the shape of a square. The **triangular numbers** are the numbers **1, 3, 6, 10, 15, ...** that can be arranged in the shape of an equilateral triangle, this led the ancient Greeks to call a number triangular if it is the sum of consecutive integers, beginning with 1.

The pentagonal numbers are the numbers **1, 5 = 1+4, 12 = 1+4+7, 22= 1+4 +7 +10, 35= 1+4+7+10+13, ...** that can be arranged in the shape of a pentagon. The first few triangular, square and pentagonal numbers are illustrated in the following figure.



Number Shapes

A natural question to ask is whether there are any triangular numbers that are also square numbers (other than **1**). The answer is "**YES**," the smallest example being

$36 = 6^2 = 1+2+3+4+5+6+7+8.$

We have now seen some of the types of questions that are studied in the Theory of Numbers. How does one attempt to answer these questions?

Exercise

(1) Prove that a number is triangular if and only if it is of the form $\boldsymbol{n(n+1)/2}, \boldsymbol{n \geq 1}$.

(2) The integer $\boldsymbol{n}$ is a triangular number if and only if $\boldsymbol{8n+1}$ is a perfect square.

(3) The sum of any two consecutive triangular numbers is a perfect square.

(4) If $\boldsymbol{P_n}$ denotes the **n**th pentagonal number, where $\boldsymbol{P_1 = 1}$ and $\boldsymbol{P_n = P_{n-1} + (3n-2)}$ for $\boldsymbol{n \geq 2}$, then prove that $\boldsymbol{P_n = \frac{n(3n-1)}{2}}, \boldsymbol{n \geq 1}$.

(5) Find three examples of triangular numbers that are sums of two other triangular numbers.

1.2 Divisibility and the Division Algorithm

The notions of divisibility and factorizations are important tools in number theory. We now discuss the concept of divisibility and its properties.

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 $5 \nmid 26$.

Remarks:

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 $2 \mid n$ 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 $a \nmid b$.

d. If a, b and c are integers such that $a \mid b$ and $b \mid c$, then $a \mid c$. 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 $a \mid c$. 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 1. 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 $c \mid (ma + nb)$.

The above theorem can be generalized to any finite linear combination as follows.

Theorem 2. If $a|b_1, a|b_2, \dots, a \mid b_n$, then $a \mid \sum_{j=1}^{n} k_j b_j$.

Proof. 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.

1.2.1 The Division Algorithm

Well-ordering principle states that, every non-empty set $\boldsymbol{S}$ of nonnegative integers contains a least element; that is, there is some integer a in $\boldsymbol{S}$ such that $\boldsymbol{a \leq b}$, for all $\boldsymbol{b}'$s belonging to $\boldsymbol{S}$.

The following result is called the **Division Algorithm**, and it plays an important role in the theory of numbers.

Theorem 3. (**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 $k < a/b$ we have $a - bk > 0$. 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.

We call $\boldsymbol{a}$ the ***dividend*** and $\boldsymbol{b}$ the ***divisor*** in the above theorem. The integers q and r are called, respectively, the ***quotient*** and ***remainder*** in the division of a by b.

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

Exercises 1

1. Show that $5|25, 19|38$ 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 $a = \pm b$.

1.2.2 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 vice 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 4. Let b be a positive integer with $b > 1$. Then any positive integer m can be written uniquely as

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

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

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 course. We now present examples of how to convert from decimal integer representation to any other base representation and vice versa.

Example 2. 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 $(214)_{10} = (21221)_3$.

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 3.

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.

1.2.3 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 $|a|$ are the same.

Definition 4. 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 4. 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 5. Two integers a and b are relatively prime if $(a, b) = 1$.

Example 5. 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 $(a, b) = (|a|, |b|)$.

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 5. 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

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

Thus, we get that

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

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 6. 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 2, $k \mid (a + cb)$ 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 2 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 6. 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 7. The greatest common divisor of two integers a and b, not both 0 is the least positive integer $\boldsymbol{d}$ 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

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

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 $ma + nb = 1$.

Let $a_1, a_2, \dots, a_n$ 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 $a_1, a_2, \dots, a_n$ is denoted by $(a_1, a_2, \dots, a_n)$.

Definition 7. The integers $a_1, a_2, \dots, a_n$ are said to be mutually relatively prime if $(a_1, a_2, \dots, a_n) = 1$.

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

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

Example 8. The integers $3,14,25$ are pairwise relatively prime. Notice also that these integers are mutually relatively prime.

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

Exercises 4

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 $(\mathrm{m} + \mathrm{n}, \mathrm{m} - \mathrm{n}) = 1$ 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 $a_1, a_2, \dots, a_n$ are integers that are not all 0 and c is a positive integer, then $(ca_1, ca_2, \dots, ca_n) = c(a_1, a_2, \dots a_n)$.

10. Write a program (in Python) to compute the greatest common divisor $\gcd(\boldsymbol{a}, \boldsymbol{b})$ of two integers $\boldsymbol{a}$ and $\boldsymbol{b}$. Your program should work even if one of a orb is zero.

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

Note that by Theorem 6, 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 9. 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 $j = 0,1, \dots, n-2$ and $r_{n+1} = 0,$ then $(a, b) = r_n$.

By applying the division algorithm, we see that

$$\begin{array}{rrr} r_0 = & r_1q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 = & r_2q_2 + r_3 & 0 \leq r_3 < r_2, \\ . & & \\ . & & \\ . & & \\ r_{n-2} = & r_{n-1}q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} = & & r_nq_n. \end{array}$$

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

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

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 7. 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 9. 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 5.

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 $(a, b) = (a/2, b)$.

Exercises 6.

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.

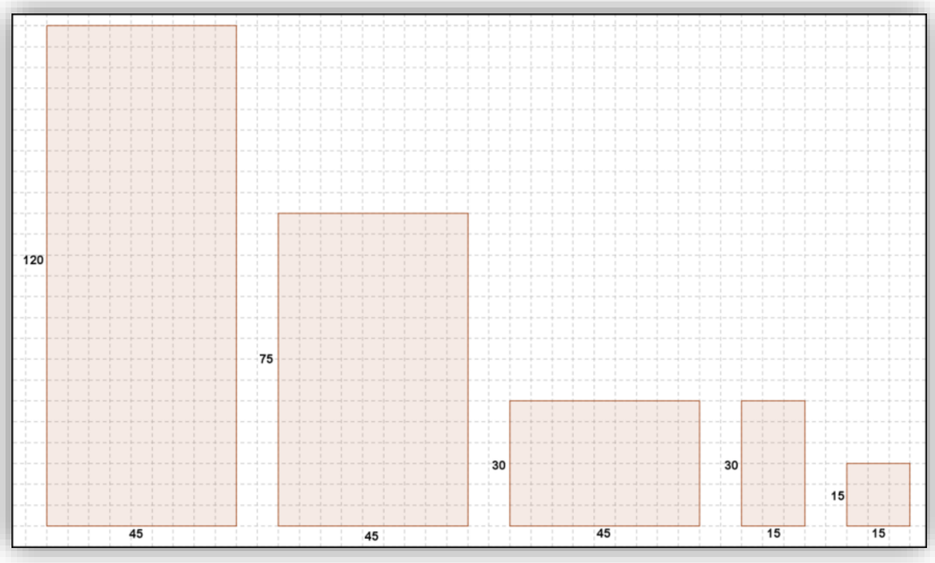
2. Find an upper bound for the number of steps in the Euclidean algorithm that is used to find the greatest common divisor of 15 and 75. Verify your result by using the Euclidean algorithm to find the greatest common divisor of the two integers.

1.2.5 Greatest Common Divisor by Geometry

The **greatest common divisor** of a pair of integers can be found by an interesting geometric method. Suppose the two integers whose ***G.C.D.*** is to be found are ***a*** and ***b***. First, draw a rectangle of length ***a*** and breadth ***b***. From this rectangle mark off the largest possible square. If ***a*** is greater than ***b***, this will be a square of side ***b***. After marking off the square, the portion which remains is a rectangle with sides ***b*** and ***a* – *b***. Again mark off the largest possible square from this rectangle. Continue this process till you obtain a square instead of a rectangle. The measure of the side of this square is equal to the ***G.C.D.*** of the original pair of numbers.

This method is based on the fact that if ***a*** and ***b*** are both divisible by a number, then ***a* – *b*** will also be divisible by the same number. The same principle is applied recursively to obtain the ***G.C.D.***

<u>Example</u> Let $\boldsymbol{a} = \mathbf{120}$ and $\boldsymbol{b} = \mathbf{45}$ and consider the following figure



Therefore, $\boldsymbol{gcd}(\mathbf{120}, \mathbf{45}) = \mathbf{15}$.