Volume-II
RING AND FIELD THEORY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>BLOCK 3</td>
<td>3</td>
</tr>
<tr>
<td>Ring Theory</td>
<td></td>
</tr>
<tr>
<td>BLOCK 4</td>
<td>109</td>
</tr>
<tr>
<td>Field Theory</td>
<td></td>
</tr>
</tbody>
</table>
INTRODUCTION

So far you have studied various aspects of group theory in Blocks 1 and 2 of this course on algebra. This volume comprises two further blocks of the course.

In the first block in this volume, Block 3, the focus is on ring theory. In the next, and last, block, viz., Block 4, you will study different aspects of field theory. In particular, you will study Galois theory.

We hope you will enjoy studying these blocks.
Block 3
RING THEORY

Block Introduction
Notations and Symbols

UNIT 8
Basic Ring Theory – A Review

UNIT 9
Special Integral Domains

UNIT 10
Congruences
Course Design Committee

Prof. Gurmeet Kaur Bakshi  
Deptt. of Mathematics,  
Panjab University

Dr. Anuj Bishnoi  
Deptt. of Mathematics,  
University of Delhi

Prof. K. N. Raghavan  
Deptt. of Mathematics  
Institute of Mathematical Sciences, Chennai

Prof. Ravi Rao  
School of Mathematics  
Tata Institute of Fundamental Research  
Mumbai

Prof. Parvati Shastri  
Centre for Excellence in Basic Sciences  
Mumbai University

Faculty members
School of Sciences, IGNOU
Dr. Deepika  
Prof. Poornima Mital  
Prof. Parvin Sinclair  
Prof. Sujatha Varma  
Dr. S. Venkataraman

* The course design is based on the recommendations of the Expert Committee for the programme M.Sc (Mathematics with Applications in Computer Science).

Block Preparation Team

Prof. B. Sury (Editor)  
Deptt. of Mathematics  
Indian Statistical Institute, Bengaluru

Dr. S. Venkataraman  
School of Sciences  
IGNOU

Prof. Parvin Sinclair  
School of Sciences  
IGNOU

Course Coordinator: Prof. Parvin Sinclair

Acknowledgement: To Sh. S. S. Chauhan for the preparation of the CRC of this block.
So far, in this course, the focus has been on different aspects of group theory. With this block, we move the discussion to rings, a concept you are familiar with from your undergraduate studies.

This block comprises three units. In the first unit, Unit 8, we will help you quickly recall the concepts of rings, subrings, ideals and ring homomorphisms.

In Unit 9, we will first help you revise, and brush up, what you studied earlier about integral domains. We will, then, build on this learning to introduce you to Euclidean domains, principal ideal domains and unique factorisation domains. You will also study units, prime elements and irreducible elements in these domains.

Finally, in Unit 10, we discuss congruences, which is a part of number theory. Here you will study some interesting results about congruences, as well as the quadratic reciprocity law. You will find applications of what you study here in the courses, ‘Coding Theory’ and ‘Cryptography’, which you will study in the next two semesters.

Whatever you study in this block will be of great use to you in the next block, and in other courses of this programme. So please study this block very carefully, doing all the exercises yourself, as you come to them.
(Also see the notation and symbols given in Blocks 1 and 2, which continue here.)

\( (R, +, \cdot) \)  the ring \( R \) w.r.t the operations ‘+’ and ‘\cdot’

\( Ra(aR) \)  the left (right) ideal of \( R \) generated by its element \( a \)

\( < a > \)  the principal ideal generated by \( a \)

\( < a_1, a_2, \ldots, a_n > \)  the ideal generated by \( a_1, \ldots, a_n \)

\( R/I \)  the quotient ring of \( R \) by its ideal \( I \)

\( a \mid b (a \nmid b) \)  \( a \) divides \( b \) ( \( a \) does not divide \( b \) )

\( (a, b) \)  the g.c.d. of elements \( a \) and \( b \)

\( U(R) \)  the group of units of the commutative ring \( R \) with identity

\( R[x] \)  the ring of polynomials in one variable over the ring \( R \)

\( \phi(n) \)  the value of the Euler phi function at the positive integer \( n \)

\( \left( \frac{a}{p} \right) \)  the Legendre symbol, where \( p \) is an odd prime and \( (a, p) = 1, a \in \mathbb{Z} \)
UNIT 8 BASIC RING THEORY – A REVIEW

Structure                                      Page No.
-----------------------------------------------
8.1 Introduction                               7
   Objectives                                  
8.2 Rings                                     7
8.3 Subrings                                   10
8.4 Ideals                                     12
8.5 Quotient Rings                             16
8.6 Ring Homomorphisms                        18
8.7 Summary                                   23
8.8 Solutions / Answers                       24

8.1 INTRODUCTION

In the earlier blocks, the focus was on groups. With this unit, we get you into the study of rings. Here we plan to help you revisit what you studied in your undergraduate studies about rings, and related concepts.

In Sec.8.2, the focus is on recalling the definition of rings, and common examples of commutative and non-commutative rings.

In Sec.8.3 and Sec.8.4, you will revisit the concept, and properties, of a subring and an ideal. This, very naturally, leads you to the focus of Sec.8.5, namely, quotient rings.

Finally, in Sec.8.5, you will relook what a ring homomorphism and isomorphism is. You will also be proving, and applying, the very important Fundamental Theorem of Homomorphism for rings.

Objectives

After reading this unit, you should be able to

- recall the definition, and some basic properties, of a ring, a subring, an ideal and a quotient ring;
- state, prove and apply the Fundamental Theorem of Homomorphism, and the other two isomorphism theorems, for rings.

8.2 RINGS

You are familiar with \( \mathbb{Z} \), the set of integers. You also know that it is a group with respect to addition, but not a group with respect to multiplication.

However, multiplication in \( \mathbb{Z} \) is associative and distributive over addition. As you may recall, these properties of addition and multiplication of integers make the system \( (\mathbb{Z}, +, \cdot) \) a ring, according to the following definition, which you would recall.

**Definition:** A non-empty set \( R \), together with two binary operations, usually called addition (denoted by \(+\)) and multiplication (denoted by \(\cdot\)), is called a **ring** if the following axioms are satisfied:
Ring Theory

**R1** \((\mathbb{R}, +)\) is an abelian group.

**R2** \((\mathbb{R}, \cdot)\) is a semigroup.

**R3** \(a \cdot (b + c) = a \cdot b + a \cdot c\), and \((a + b) \cdot c = a \cdot c + b \cdot c\) for all \(a, b, c\) in \(\mathbb{R}\), i.e., multiplication distributes over addition from the left as well as from the right.

You would also recall that \((\mathbb{Q}, +, \cdot)\) and \((\mathbb{R}, +, \cdot)\) are rings. But, they are also fields, according to the following definition.

**Definition:** A ring \((\mathbb{R}, +, \cdot)\) is a **field** if \((\mathbb{R}^*, \cdot)\) is an abelian group.

(You will study about fields, in detail, in Block 4.)

Let us now recall some examples of rings.

i) \((n\mathbb{Z}, +, \cdot)\), where \(n \in \mathbb{Z}\).

ii) \((\mathbb{Z}_n, +, \cdot)\), where \(\bar{a} + \bar{b} = \bar{a + b}\) and \(\bar{a} \cdot \bar{b} = \bar{ab} \forall \bar{a}, \bar{b} \in \mathbb{Z}_n\).

iii) \((M_n(\mathbb{R}), +, \cdot)\), \(n \in \mathbb{N}\), where \(+\) and \(\cdot\) denote matrix addition and matrix multiplication.

Let us consider two more examples, in detail.

**Example 1:** Let \(X\) be a non-empty finite set, \(\wp(X)\) be the collection of all subsets of \(X\) and \(\Delta\) denote the symmetric difference operation. Show that \((\wp(X), \Delta, \cap)\) is a ring.

**Solution:** For any two subsets \(A\) and \(B\) of \(X\), \(A \Delta B = (A \setminus B) \cup (B \setminus A)\). From Unit 1, recall that \((\wp(X), \Delta)\) is an abelian group. You also know that \(\cap\) is associative. Now let us see if \(\cap\) distributes over \(\Delta\).

Let \(A, B, C \in \wp(X)\). Then, you can check that

\[
A \cap (B \Delta C) = A \cap ([B \setminus C] \cup [C \setminus B]) = [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)] = (A \cap B) \Delta (A \cap C).
\]

So, the left distributive law holds.

Also, \((B \Delta C) \cap A = A \cap (B \Delta C)\), since \(\cap\) is commutative.

\[
= (A \cap B) \Delta (A \cap C) = (B \cap A) \Delta (C \cap A).
\]

Therefore, the right distributive law holds also.

Therefore, \((\wp(X), \Delta, \cap)\) is a ring.

***

**Example 2:** Consider the class of all continuous real valued functions defined on the closed interval \([0, 1]\). Define the binary operations \(+\) and \(\cdot\) on \([0, 1]\) by \((f + g)(x) = f(x) + g(x)\) (i.e., pointwise addition), and \((f \cdot g)(x) = f(x) \cdot g(x)\) (i.e., pointwise multiplication) for every \(f, g \in [0, 1]\) and \(x \in [0, 1]\). Show that \([0, 1]\) is a ring with respect to \(+\) and \(\cdot\).

**Solution:** Since addition in \(\mathbb{R}\) is associative and commutative, so is addition in \([0, 1]\). The additive identity of \([0, 1]\) is the zero function. The additive inverse of \(f \in [0, 1]\) is \((-f)\), where \((-f)(x) = -f(x) \forall x \in [0, 1]\). Thus, \([0, 1], +\) is an abelian group. Again, since multiplication in \(\mathbb{R}\) is associative, so is multiplication in \([0, 1]\).

Finally, the axiom R3 holds because for any \(x \in [0, 1]\),
(f(g + h))(x) = f(x)(g + h)(x) \\
= f(x)(g(x) + h(x)) \\
= f(x)g(x) + f(x)h(x), since \cdot distributes over + in \mathbb{R}. \\
= (f \cdot g)(x) + (f \cdot h)(x) \\
= (f \cdot g + f \cdot h)(x)

Hence, \( f(g + h) = f \cdot g + f \cdot h \).

Since multiplication is commutative in \( C[0,1] \), the other distributive law also holds. Thus, R3 holds for \( C[0,1] \).

Therefore, \((C[0, 1], +, \cdot)\) is a ring. This ring is called the ring of continuous functions on \([0, 1]\).

***

In the examples of rings so far, the multiplication in the ring has been commutative except in \( M_n(\mathbb{R}) \) \((n > 1)\). Related to this remark are the following definitions.

**Definitions:** A ring \((R, +, \cdot)\) is called

i) **commutative** if \( a \cdot b = b \cdot a \ \forall a, b \in R; \)

ii) a **ring with identity** if \( \exists e \in R \) such that \( a \cdot e = e \cdot a = a \ \forall a \in R \). Here \( e \) is called the **multiplicative identity** of \( R \).

Try some exercises now.

---

**E1)** Show that \( \mathbb{Z} + i\mathbb{Z} = \{ m + in \mid m \text{ and } n \text{ are integers} \} \) is a ring with respect to the usual addition and multiplication in \( \mathbb{C} \). (This ring is called the ring of **Gaussian integers**, after the mathematician Carl Friedrich Gauss.)

**E2)** Show that the set \( \mathbb{Q} + \sqrt{2}\mathbb{Q} = \{ p + \sqrt{2} q \mid p, q \in \mathbb{Q} \} \) is a ring with respect to addition and multiplication of real numbers.

**E3)** Let \( S = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \), \( a, b \) are real numbers. Prove that \( S \) is a ring under matrix addition and multiplication.

**E4)** Why is \((\varnothing(X), \cup, \cap)\) not a ring?

**E5)** Give an example, with justification, of a ring which is not a ring with identity.

**E6)** Let \((A, +)\) be an abelian group. Show that the set of all endomorphisms of \( A \), \( \text{End} \ A = \{ f : A \rightarrow A \mid f(a + b) = f(a) + f(b) \ \forall a, b \in A \} \) is a ring w.r.t. + and \( \cdot \), defined by \( (f + g)(a) = f(a) + g(a) \), and \( (f \cdot g)(a) = f \circ g(a) \ \forall a \in A \).

Check whether \( \text{End} \ A \) is commutative or not. Does \( \text{End} \ A \) have identity?

**E7)** Let \((A, +, \cdot)\) and \((B, \oplus, \odot)\) be rings. Show that their Cartesian product, \( A \times B \), is a ring w.r.t. the operations \( \boxplus \) and \( \boxdot \), given by

---
Under what conditions on \( A \) and \( B \) will \( A \times B \) be a commutative ring?

E8) Show that the set of real quaternions,
\[
\mathbb{H} = \{a + ib + jc + kd \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}
\]
is a ring with unity, called the ring of real quaternions.

Let us now consider subsets of rings that are rings in their own right.

### 8.3 SUBRINGS

Analogous to the concept in group theory, of subgroups of a group, is the concept we will now discuss.

**Definition:** Let \((R, +, \cdot)\) be a ring and \(S\) be a non-empty subset of \(R\). \(S\) is called a **subring** of \(R\) if \((S, +, \cdot)\) is itself a ring, i.e., \(S\) is a ring with respect to the operations on \(R\).

For example,

i) \(\mathbb{Z} \cap n\mathbb{Z}, n \in \mathbb{N}\), is a subring of \(\mathbb{Z}\), and \(\mathbb{Z}\) is a subring of \(\mathbb{R}\).

ii) every ring is a subring of itself.

iii) \(\{0\}\) is a subring of every ring, called the **trivial subring**.

As you may recall from your undergraduate studies, the **criteria** for a subset of \((R, +, \cdot)\) to be a subring of \(R\) are as given in the following proposition.

**Proposition 1:** A non-empty subset \(S\) of a ring \((R, +, \cdot)\) is a subring of \(R\) if
\[
\forall x, y \in S, x - y \in S \quad \text{and} \quad xy \in S.
\]

Let us look at some examples. We have already noted that \(\mathbb{Z}\) is a subring of \(\mathbb{R}\). In fact, you can use Proposition 1 to check that \(\mathbb{Z}\) is a subring of \(\mathbb{Q}, \mathbb{C}\), and \(\mathbb{Z} + i\mathbb{Z}\) too. You can also verify that \(\mathbb{Q}\) is a subring of \(\mathbb{R}, \mathbb{C}\) and
\[
\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{\alpha + \sqrt{2}\beta \mid \alpha, \beta \in \mathbb{Q}\}.
\]

Now, let us look at an example of a subring other than sets of numbers.

**Example 3:** Consider the ring \(\wp(X)\), given in Example 1. Check whether or not \(S = \{\emptyset, X\}\) is a subring of \(\wp(X)\).

**Solution:** Note that \(A \Delta A = \emptyset \forall A \in \wp(X)\). \(\therefore -A = A\) in \(\wp(X)\).

Now, to apply the criteria in Proposition 1, we first note that \(S\) is non-empty. Next, \(\emptyset \Delta \emptyset = \emptyset \in S, X \Delta X = \emptyset \in S,\)

Also \(\emptyset \cap \emptyset, \emptyset \cap X, X \cap X\) are in \(S\).

Hence \(S\) is a subring of \(\wp(X)\).

The next example actually gives us an important class of examples.
**Example 4:** Let $R$ be a ring and $a \in R$. Show that the set $aR = \{ax \mid x \in R\}$ is a subring of $R$.

**Solution:** Since $R \neq \emptyset$, $aR \neq \emptyset$.

Next for any two elements $ax$ and $ay$ of $aR$, $ax - ay = a(x - y) \in aR$ and $(ax)(ay) = a(xy) \in aR$.

Hence $aR$ is a subring of $R$.

On the same lines as in Example 4, you can check that $Ra = \{xa \mid x \in R\}$ is a subring of $R$.

Using Example 4, you can immediately see that $\mathbb{m} \mathbb{Z}_n$ is a subring of $\mathbb{Z}_n \forall \mathbb{m} \in \mathbb{Z}_n$. This also shows us a fact that you have already noted: $n\mathbb{Z}$ is a subring of $\mathbb{Z} \forall n \in \mathbb{Z}$.

We would like to make a remark here about rings with identity.

**Remark 1:**

i) If $R$ is a ring with identity, a subring of $R$ may or may not be with identity. For example, the ring $\mathbb{Z}$ has identity 1, but its subring $n\mathbb{Z}(n \geq 2)$ is without identity.

ii) The identity of a subring, if it exists, may not coincide with the identity of the ring. For example, the identity of the ring $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$. But the identity of its subring $\mathbb{Z} \times \{0\}$ is $(1, 0)$.

Try the following exercises now.

---

**E9)**

i) Show that $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\}$ is a subring of $\mathbb{M}_2(\mathbb{Z})$.

ii) Does $S$ have identity? If yes, then is the identity of $S$ the same as that of $\mathbb{M}_2(\mathbb{Z})$? Give reasons for your answers.

**E10)** Show that if $A$ is a subring of $B$, and $B$ is a subring of $C$, then $A$ is a subring of $C$.

**E11)** Is every subset of a ring $R$ a subring of $R$? Why, or why not?

---

Now it is time to recall some properties of subrings.

**Proposition 2:** Let $S_1$ and $S_2$ be subrings of a ring $R$. Then

i) $S_1 \cap S_2$ is also a subring of $R$.

ii) $S_1 \cup S_2$ need not be a subring of $R$.

**Proof:**

i) Since $0 \in S_1$ and $0 \in S_2$, $0 \in S_1 \cap S_2$. $\therefore S_1 \cap S_2 \neq \emptyset$.

Now, let $x, y \in S_1 \cap S_2$. Then $x, y \in S_1$ and $x, y \in S_2$. Thus, $x - y$ and $xy$ are in $S_1$ as well as in $S_2$, i.e., they lie in $S_1 \cap S_2$.

Thus, $S_1 \cap S_2$ is a subring of $R$.
ii) As an example, you know that $2\mathbb{Z}$ and $3\mathbb{Z}$ are subrings of $\mathbb{Z}$. However, their union is not a subring of $\mathbb{Z}$.

To see why, note that 2 and 3 are in $2\mathbb{Z} \cup 3\mathbb{Z}$, but $2+3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. 

On the same lines as the proof above we can prove that **the intersection of any family of subrings of a ring $R$ is a subring of $R$**.

Try some related exercises now.

E12) Let $S_1$ and $S_2$ be subrings of the rings $R_1$ and $R_2$, respectively. Show that $S_1 \times S_2$ is a subring of $R_1 \times R_2$.

E13) Obtain two distinct proper non-trivial subrings of $\mathbb{Z} \times \mathbb{R}$ (i.e., subrings which are neither zero nor the whole ring).

Let us now review an important concept, analogous to that of a normal subgroup of a group.

### 8.4 IDEALS

In Unit 1 you studied normal subgroups and the role that they play in group theory. You saw that the most important reason for the existence of normal subgroups is that they allow us to define quotient groups. In ring theory, we would like to define an analogous concept, a quotient ring. In this section we will discuss a class of subrings that will help us to do so. These subrings are called ideals. While exploring algebraic number theory, the 19th century mathematicians, Dedekind, Kronecker and others, developed the concept of an ideal. In 1920, the ‘mother of algebra’, Emmy Noether took this further, and developed the general concepts that we will now define.

**Definition:** A non-empty subset $I$ of a ring $(R, +, \cdot)$ is called:

i) **a left ideal** of $R$ if $a - b \in I$ and $ra \in I \forall a, b \in I, r \in R$.

ii) **a right ideal** of $R$ if $a - b \in I$ and $ar \in I \forall a, b \in I, r \in R$.

iii) **an ideal** of $R$ if it is both a left ideal and a right ideal of $R$, that is, if $a - b \in I, ar \in I, ra \in I \forall a, b \in I, r \in R$.

For instance, $n\mathbb{Z}$ is an ideal of $\mathbb{Z} \forall n \in \mathbb{Z}$. In fact, every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, for some $n \in \mathbb{Z}$.

Here, we need to make some important comments.

**Remark 2:** A subring $I$ of a ring $R$ is an ideal of $R$ iff $ra \in I$ and $ar \in I \forall r \in R$ and $a \in I$.

**Remark 3:** If $R$ is commutative, then every left ideal of $R$ is a right ideal, and hence, an ideal of $R$.

**Remark 4:** Recall that every ring is an ideal of itself. If an ideal $I$ of a ring $R$
is such that \( I \neq R \), then \( I \) is called a **proper ideal** of \( R \). Also, \( \{0\} \) is an ideal of \( R \), called the **trivial ideal** of \( R \).

Try some exercises now.

**E14**) Show that \( \{0, 3\} \) and \( \{0, 2, 4\} \) are proper ideals of \( \mathbb{Z}_6 \).

**E15**) Give an example of a subring of a ring \( R \) which is not an ideal of \( R \).

Now let us consider some more examples of ideals.

**Example 5:** Let \( X \) be an infinite set. Consider \( I \), the set of all finite subsets of \( X \). Show that \( I \) is an ideal of \( \wp(X) \).

**Solution:** \( I = \{A \mid A \) is a finite subset of \( X\} \). Note that

i) \( \emptyset \in I \), i.e., the zero element of \( \wp(X) \) is in \( I \).

ii) \( A-B = A \triangle B = A \triangle B \) as \( B = B \) in \( \wp(X) \).

If \( A, B \in I \), then \( A-B \) is again a finite subset of \( X \), and hence \( A-B \in I \).

iii) Whenever \( A \) is a finite subset of \( X \) and \( B \) is any subset of \( X \), \( A \cap B \) is a finite subset of \( X \). Thus, \( A \in I \) and \( B \in \wp(X) \Rightarrow AB \in I \) and \( BA \in I \). Hence, \( I \) is an ideal of \( \wp(X) \).

***

**Example 6:** Consider the ring \( \mathbb{C}[0,1] \) given in Example 2. Let \( M = \{f \in \mathbb{C}[0,1] \mid f(1/2) = 0\} \). Show that \( M \) is an ideal of \( \mathbb{C}[0,1] \).

**Solution:** The zero element, \( 0 \), is defined by \( 0(x) = 0 \) for all \( x \in [0,1] \). Since \( 0(1/2) = 0 \), \( 0 \in M \).

Also, if \( f, g \in M \), then \( (f-g)(1/2) = f(1/2) - g(1/2) = 0 - 0 = 0 \).

So, \( f-g \in M \).

Next, if \( f \in M \) and \( g \in \mathbb{C}[0,1] \), then \( (fg)(1/2) = f(1/2)g(1/2) = 0g(1/2) = 0 \), so \( fg \in M \).

Since \( \mathbb{C}[0,1] \) is commutative, this shows that \( M \) is an ideal of \( \mathbb{C}[0,1] \).

***

Now you can try an exercise that is a generalisation of Example 6, and another exercise.

**E16**) For \( a \in [0,1] \), check whether or not the sets

\[
I_a = \{f \in \mathbb{C}[0,1] \mid f(a) = 0\} \quad \text{and} \quad J_a = \{f \in \mathbb{C}[0,1] \mid f(a) = 1\}
\]

are ideals of \( \mathbb{C}[0,1] \).

**E17**) Let \( R \) be a ring and \( a \in R \). Show that \( Ra \) and \( aR \) are left and right ideals, respectively, of \( R \).

**E17** can be generalised, as in the next example.
**Example 7:** For any ring $R$ and $a_1, \ldots, a_n \in R$, show that

$$S = Ra_1 + Ra_2 + \cdots + Ra_n = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_1, x_2, \ldots, x_n \in R\}$$

is a left ideal of $R$.

**Solution:** Firstly, $0 = 0a_1 + 0a_2 + \cdots + 0a_n \in S$.

Next, \((x_i - y_i)a_i + (x_2 - y_2)a_2 + \cdots + (x_n - y_n)a_n \in Ra_1 + Ra_2 + \cdots + Ra_n\)

$$\forall x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in R.$$  

Finally, for $r \in R$ and $x_1a_1 + x_2a_2 + \cdots + x_na_n \in S$,

$$r(x_1a_1 + x_2a_2 + \cdots + x_na_n) = rx_1a_1 + rx_2a_2 + \cdots + rx_na_n \in S,$$  

since $rx_i \in R \forall i = 1, \ldots, n$.

Thus, $S$ is a left ideal of $R$.

***

This method of obtaining left ideals can be applied to give right ideals, and ideals, of a ring. Such ideals crop up again and again in ring theory. We give them a special name.

**Definition:** Let $A$ be a non-empty subset of a ring $R$ with identity. Then the **ideal generated by the set $A$** is the smallest ideal of $R$ containing $A$, and is

$$RAR = \{r_1a_1r_1' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{N}\},$$  

denoted by $\langle a_1, a_2, \ldots, a_n \rangle$.

If $A = \{a\}$, then

$$RAR = \left\{ \sum_{i=1}^n r_i a_i r_i' \mid r_i, r_i' \in R, n \in \mathbb{N} \right\}$$

is called the **principal ideal** generated by $a$. This is also denoted by $\langle a \rangle$.

**Remark 5:** Note that if $R$ is commutative, then $RAR = RA = AR$, where $A \subseteq R$.

Now some exercises on principal, and other, ideals.

---

**E18)** Find the principal ideal of $M_2(\mathbb{Z})$ generated by $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Show that it is not the same as the left ideal $M_2(\mathbb{Z}) \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

**E19)** Find the principal ideals of $\mathbb{Z}_{10}$ generated by $3$, and by $\overline{3}$.

**E20)** An element of a ring $R$ is called **nilpotent** if there exists a positive integer $n$ such that $a^n = 0$. Show that

i) $\overline{3}$ is nilpotent in $\mathbb{Z}_9$;  

ii) the set of nilpotent elements of a commutative ring $R$ is an ideal of $R$, called the **nil radical** of $R$.

**E21)** Find the nil radicals of $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_8$ and $\wp(X)$.
By now you must be familiar with the concept of ideals. Let us now obtain an important property of ideals.

**Theorem 1:** Let $R$ be a ring with identity $1$. If $I$ is a left ideal of $R$ and $1 \in I$, then $I = R$.

**Proof:** We know that $I \subseteq R$. We want to prove that $R \subseteq I$. Let $r \in R$. Since $1 \in I$ and $I$ is a left ideal of $R$, $r = r \cdot 1 \in I$. So, $R \subseteq I$. Hence $I = R$.

Theorem 1 stays valid if ‘left ideal’ is replaced by ‘right ideal’ or ‘ideal’.

Using this result we can immediately say that $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. Does this also tell us whether $\mathbb{Q}$ is an ideal of $\mathbb{R}$ or not? Certainly. Since $1 \in \mathbb{Q}$ and $\mathbb{Q} \neq \mathbb{R}$, $\mathbb{Q}$ can’t be an ideal of $\mathbb{R}$.

Now let us shift our attention to the algebra of ideals.

**Theorem 2:** If $I$ and $J$ are ideals of a ring $R$, then the following are ideals of $R$:

i) $I \cap J$,

ii) $I + J = \{a + b | a \in I \text{ and } b \in J\}$, and

iii) $IJ = \{x \in R | x \text{ is a finite sum } a_1b_1 + \cdots + a_nb_n, \text{ where } a_i \in I \text{ and } b_i \in J\}$.

**Proof:** You know that $I \cap J$, $I + J$ and $IJ$ are subrings of $R$. Next, to show that these subrings are ideals, consider the following:

i) If $a \in I \cap J$, then $a \in I$ and $a \in J$. Therefore, $ax \in I$ and $ax \in J$ for all $x$ in $R$. So $ax \in I \cap J$ for all $a \in I \cap J$ and $x \in R$. Similarly, $xa \in I \cap J \forall a \in I \cap J$ and $x \in R$. Thus, $I \cap J$ is an ideal of $R$.

ii) Let $x \in I + J$ and $r \in R$. Then $x = a + b$ for some $a \in I$ and $b \in J$. Now $xr = (a + b)r = ar + br \in I + J$, since $ar \in I$ and $br \in J$ for all $r \in R$. Similarly, $rx \in I + J \forall r \in R$ and $x \in I + J$.

Thus, $I + J$ is an ideal of $R$.

iii) Let $x \in IJ$, say $x = a_1b_1 + \cdots + a_nb_n$, with $a_i \in I$ and $b_i \in J$. Then, for any $r \in R$, $xr = (a_1b_1 + \cdots + a_nb_n)r = a_1(b_1r) + \cdots + a_n(b_nr)$, which is a finite sum of elements of the form $ab$ with $a \in I$ and $b \in J$.

(Note that $b_i \in J \Rightarrow b_i r \in J$ for all $r$ in $R$.)

Hence $xr \in IJ$ for $x \in IJ$ and $r \in R$.

Similarly, for $r \in R$ and $x \in IJ$, $rx \in IJ$.

Thus, $IJ$ is an ideal of $R$.

Note how we have defined $IJ$. Here is a comment about this.

**Remark 6:** If we were to define $IJ = \{ab | a \in I, b \in J\}$, then $IJ$ need not even be a subring, leave alone being an ideal. For example, consider the ideals $I = <2, x>$ and $J = <5, x>$ in $\mathbb{Z}[x]$. Then $IJ = <10, x>$. So $x \in IJ$. But $x$ can’t be written as a product of two elements of the form $2p(x) + xp(x)$ and
5p_1(x) + xp_3(x), where p_1(x) ∈ Z[x]. So we reach a contradiction. Therefore, IJ is defined as in Theorem 2.

Here is an exercise about the relationship between the ideals obtained in Theorem 2. In fact, these inclusions are true for any I and J (see E22). We show the relationship in Fig. 2.

E22) If I and J are ideals of a ring R, then show that:

i) \( IJ \subseteq I \cap J \subseteq I \subseteq I+J \) and \( IJ \subseteq I \cap J \subseteq J \subseteq I+J \) (see Fig.2).

ii) \( I+J \) is the smallest ideal containing both the ideals I and J, i.e., if A is an ideal of R containing both I and J, then A must contain \( I+J \);

iii) \( I \cap J \) is the largest ideal that is contained in both I and J;

iv) If \( 1 \in R \) and \( I+J = R \), then \( IJ = I \cap J \), i.e., if the top two of Fig.2 are equal, then so are the lowest two.

Fig. 2: The ideal hierarchy!

Let us now go back to what we said at the beginning of this section – why ideals matter.

8.5 QUOTIENT RINGS

In Unit 1 you reviewed your understanding of quotient groups. You know that given a normal subgroup N of a group G, the set of all cosets of N is a group, called the quotient group associated with the normal subgroup N. You
also know that this set is a group only if \( N \) is normal. Using ideals, we will now define a similar concept for rings.

If \((R, +, \cdot)\) is a ring and \( I \) is a subring of \( R \), then \((I, +) \leq (R, +)\). Since \((R, +)\) is an abelian group, \( I \triangleleft R \). Hence, \( R/I \) is a quotient group. Now, the question is when is \( R/I \) a ring, where \( \cdot \) is defined by

\[
(x + I) \cdot (y + I) = xy + I \quad \forall \ x + I, \ y + I \in R/I.
\]

To answer this, we need to check under what conditions on \( I \) the multiplication is well-defined.

Now, if \( a + I = a' + I, \ b + I = b' + I \) in \( R/I \), then \( \cdot \) is well-defined if

\[
ab + I = a'b' + I.
\]

Since \( a + I = a' + I, \ a - a' \in I \). Let \( a - a' = x \).

Similarly, \( b - b' \in I \), say \( b - b' = y \).

Then \( ab = (a' + x)(b' + y) = a'b' + (xb' + a'y + xy) \).

So, \( ab - a'b' \in I \) only if \( xb' + a'y + xy \in I \). This need not happen if \( I \) is only a subring, or only a left ideal, or only a right ideal of \( R \). It will happen if \( I \) is an ideal of \( R \).

Thus, \( \cdot \) is well-defined on \( R/I \) if \( I \) is an ideal of \( R \).

So, we are now ready to prove the following result.

**Theorem 3:** Let \( R \) be a ring and \( I \) be an ideal of \( R \). Then \( R/I \) is a ring with respect to addition and multiplication defined by

\[
(x + I) + (y + I) = (x + y) + I, \quad \text{and} \quad (x + I) \cdot (y + I) = xy + I \quad \forall \ x, y \in R.
\]

**Proof:** As we have noted earlier, \( (R/I, +) \) is an abelian group. So, to prove that \( R/I \) is a ring we only need to check that \( \cdot \) is associative and distributive over + . Now,

i) \textbf{ is associative}: \( \forall a, b, c \in R \),

\[
((a + I) \cdot (b + I)) \cdot (c + I) = (ab + I) \cdot (c + I) = (ab)c + I = a(bc) + I = (a + I) \cdot ((b + I) \cdot (c + I))
\]

ii) \textbf{Distributive law}: Let \( a + I, b + I, c + I \in R/I \). Then

\[
(a + I) \cdot ((b + I) + (c + I)) = (a + I)[(b + c) + I] = a(b + c) + I = (ab + ac) + I = (ab + I) + (ac + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I)
\]

Thus, \( R/I \) is a ring.

The ring \( R/I \) is called the \textbf{quotient ring of} \( R \) \textbf{by the ideal} \( I \). Let us look at some examples. We start with an example that gave rise to the terminology ‘\( R \) mod \( I \)’.

**Example 8:** Let \( R = \mathbb{Z} \) and \( I = n\mathbb{Z} \). What are all the elements of \( R/I \)?
Ring Theory

**Solution:** You have seen that \( n \mathbb{Z} \) is an ideal of \( \mathbb{Z} \). You also know that

\[
\mathbb{Z} / n \mathbb{Z} = \{n \mathbb{Z}, 1 + n \mathbb{Z}, \ldots, (n-1) + n \mathbb{Z}\}.
\]

\[= \{\bar{0}, \bar{1}, \ldots, \bar{n-1}\}, \text{ the same as the set of equivalence classes modulo } n.\]

So, \( \mathbb{R} / I \) is the ring \( \mathbb{Z}_n \).

***

Now let us look at an ideal of \( \mathbb{Z}_n \), where \( n = 8 \).

**Example 9:** Let \( R = \mathbb{Z}_8 \). Check whether or not \( I = \{\bar{0}, \bar{4}\} \) is an ideal of \( R \).

**Solution:** \( I = 4R \), and hence is a principal ideal of \( R \). From group theory, you know that the number of elements in \( R / I = o(R/I) = o(R) = \frac{8}{2} = 4 \).

You can see that these 4 elements are the cosets

\[0 + I = \{\bar{0}, \bar{4}\}, 1 + I = \{\bar{1}, \bar{5}\}, 2 + I = \{\bar{2}, \bar{6}\}, 3 + I = \{\bar{3}, \bar{7}\}.
\]

***

**Example 10:** Consider Example 5. Find two distinct elements of \( \mathbb{Z}/I \).

**Solution:** One element is \( \bar{0} \), and another is \( 2\mathbb{Z} + I \). Note that \( \bar{0} \neq 2\mathbb{Z} \) since \( 2\mathbb{Z} \Delta \{0\} \notin I \).

***

Try these exercises now.

---

E23) Show that if \( R \) is a ring with identity, then \( R/I \) is a ring with identity.

E24) If \( R \) is a ring with identity \( I \) and \( I \) is an ideal of \( R \) containing \( 1 \), what is \( R/I \)?

E25) Let \( N \) be the nil radical of a commutative ring \( R \). Show that \( R/N \) has no non-zero nilpotent elements.

---

As you may recall, the utility and importance of quotient rings shows up in the context of homomorphisms, which we discuss in the next section.

### 8.6 RING HOMOMORPHISMS

Let us begin by considering \( f : \mathbb{Z} \to \mathbb{Z}_5 : f(n) = \bar{n} \). You know that \( f \) is a group homomorphism. Also, \( f(n \cdot m) = \bar{n} \cdot \bar{m} = \bar{n} \cdot \bar{m} = f(n)f(m) \). As you may recall, these properties of \( f \) make it a ring homomorphism, a map that preserves the ring structure of its domain. Let us define this formally.
Definitions: Let \((R_1, +, \cdot)\) and \((R_2, \oplus, \odot)\) be two rings and \(f : R_1 \to R_2\) be a map.

i) \(f\) is called an **ring homomorphism** if
\[
f(a + b) = f(a) \oplus f(b), \quad \text{and} \quad f(a \cdot b) = f(a) \odot f(b)
\]
for all \(a, b\) in \(R_1\). Then the **image** of \(f\) is the set \(\text{Im } f = \{f(x) \mid x \in R_1\}\), which is a subring of \(R_2\), and the **kernel** of \(f\) is the set \(\text{Ker } f = \{x \in R_1 \mid f(x) = 0\}\), which is an ideal of \(R_1\).

ii) If \(f\) is a ring homomorphism which is surjective, then \(f\) is called an **epimorphism**, and \(R_2\) is called the **homomorphic image** of \(R_1\).

iii) If \(f\) is an injective homomorphism, then it is called a **monomorphism**.

iv) If \(f\) is a bijective homomorphism, then \(f\) is called an **isomorphism**, and \(R_1\) is said to be isomorphic to \(R_2\), denoted by \(R_1 \cong R_2\).

As you may recall, for any ring \(R\), the identity map \(I_R\) is a ring homomorphism, with kernel \(\{0\}\) and image \(R\). You have also seen that
\[
f : \mathbb{Z} \to \mathbb{Z}_n : f(m) = \overline{m} \text{ is a ring homomorphism. Here Ker } f = \langle n \rangle \text{ and } \text{Im } f = \mathbb{Z}_n.
\]

Consider the following remark here.

Remark 7: A ring homomorphism from \(R_1\) to \(R_2\) is a group homomorphism from \((R_1, +)\) to \((R_2, +)\). However, not every group homomorphism from \((R_1, +)\) to \((R_2, +)\) is a ring homomorphism from \(R_1\) to \(R_2\) (see E27).

Let us now look at some more examples of a ring homomorphism.

Example 11: Consider the map \(f : \mathbb{Z}_6 \to \mathbb{Z}_3 : f(n \pmod{6}) = n \pmod{3}\). Show that \(f\) is a ring homomorphism. What is \(\text{Ker } f\)? What is \(\text{Im } f\)?

Solution: Firstly, is \(f\) well-defined? To check this, note that
\[
n \pmod{6} = m \pmod{6}
\]
\[
\Rightarrow 6 \mid (n - m)
\]
\[
\Rightarrow 3 \mid (n - m)
\]
\[
\Rightarrow n \pmod{3} = m \pmod{3}, \text{ that is, } f(\overline{n}) = f(\overline{m}).
\]
Thus, \(f\) is well-defined.

Next, for any \(n, m \in \mathbb{Z}\),
\[
f(n \pmod{6} + m \pmod{6}) = f((n + m) \pmod{6}) = (n + m) \pmod{3}
\]
\[
= n \pmod{3} + m \pmod{3}
\]
\[
= f(n \pmod{6}) + f(m \pmod{6})
\]
You can similarly check that
\[
f(n \pmod{6}, m \pmod{6}) = f(n \pmod{6}), f(m \pmod{6})
\]
Thus, \(f\) is a ring homomorphism.
Ker \( f = \{ n \equiv 0 \pmod{6} \mid n \equiv 0 \pmod{3} \} = \{ n \equiv 0 \pmod{6} \mid n \in \mathbb{Z} \} = \{ 0, 3 \} \), bar denoting ‘mod’.

Also check that \( \text{Im } f = \mathbb{Z}_3 \).

***

**Example 12:** Consider the ring \( \mathbb{C}[0, 1] \). Define \( \phi : \mathbb{C}[0, 1] \to \mathbb{R} : \phi(f) = f(1/2) \).

Show that \( \phi \) is a homomorphism.

Is \( \phi \) an epimorphism? Is \( \phi \) a monomorphism? Give reasons for your answers.

**Solution:** Let \( f \) and \( g \in \mathbb{C}[0, 1] \). You already know that \( \phi \) is a group homomorphism. Also

\[
\phi(fg) = (fg)(1/2) = f \left( \frac{1}{2} \right) g \left( \frac{1}{2} \right) = \phi(f)\phi(g).
\]

Thus, \( \phi \) is a ring homomorphism.

For any \( r \in \mathbb{R} \), define \( f : [0, 1] \to [0, 1] : f(x) = r \). Then \( f \in \mathbb{C}[0, 1] \), and

\[
\phi(f) = f \left( \frac{1}{2} \right) = r. \text{ Hence } \phi \text{ is an epimorphism.}
\]

However, \( \phi \) is not 1-1, since the zero function and \( f : [0, 1] \to [0, 1] : f(x) = x - \frac{1}{2} \) are two distinct elements of \( \mathbb{C}[0, 1] \) in \( \text{Ker } \phi \).

***

**Example 13:** Check whether or not the map \( f : \mathbb{Z} \to M_2(\mathbb{Z}) : f(n) = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} \) is a ring homomorphism.

**Solution:** Note that \( f(n) = nI \), where \( I \) is the identity matrix of order 2. Now you can check that \( f(n + m) = f(n) + f(m) \) and \( f(nm) = f(n)f(m) \) for all \( n, m \in \mathbb{Z} \).

Thus, \( f \) is a homomorphism.

***

**Example 14:** Consider the ring \( \wp(X) \), and let \( Y \) be a non-empty subset of \( X \).

Define \( f : \wp(X) \to \wp(Y) \) by \( f(A) = A \cap Y \) for all \( A \in \wp(X) \). (Note that \( f \) is just the ‘multiplication’ by \( Y \).) Show that \( f \) is a ring homomorphism. Does \( Y^c \in \text{Ker } f \)? What is \( \text{Im } f \)?

**Solution:** For any \( A \) and \( B \) in \( \wp(X) \),

i) \( f(A \Delta B) = f((A \setminus B) \cup (B \setminus A)) = (f(A \setminus B) \cup (B \setminus A)) \cap Y = (f(A) \setminus f(B)) \cup (f(B) \setminus f(A)) \cap Y = f(A) \Delta f(B) \).

ii) \( f(A \cap B) = (A \cap Y) \cap (B \cap Y) = f(A \cap f(B)). \)

So, \( f \) is a ring homomorphism from \( \wp(X) \) into \( \wp(Y) \).

Now, the zero element of \( \wp(Y) \) is \( \emptyset \). Therefore,
Ker $f = \{ A \in \mathcal{P}(X) | A \cap Y = \emptyset \}$. Hence $Y^c \in \text{Ker } f$.

Finally, we will show that $f$ is surjective. For this, take any $B \in \mathcal{P}(Y)$.
Then, $B \in \mathcal{P}(X)$ and $f(B) = B \cap Y = B$. Thus, $B \in \text{Im } f$.
Therefore, $\text{Im } f = \mathcal{P}(Y)$, and $f$ is an onto homomorphism.

***

Now, for some exercises to help you check how well you have recalled the concept you have just studied.

---

E26) If $S$ is a subring of a ring $R$, then show that the inclusion map $i : S \rightarrow R : i(x) = x$ is a ring homomorphism. What are $\text{Ker } i$ and $\text{Im } i$?

E27) Give an example, with justification, of a group homomorphism between two rings, which is not a ring homomorphism.

E28) Let $R_1$ and $R_2$ be two rings. Define $f : R_1 \rightarrow R_2 : f(x) = 0$. Show that $f$ is a homomorphism. Also obtain $\text{Ker } f$ and $\text{Im } f$. (This function is called the trivial homomorphism.)

E29) Is $f : \mathbb{Z} \rightarrow M_2(\mathbb{Z}) : f(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ a ring isomorphism? Why, or why not?

E30) Let $A$ and $B$ be two rings. Check whether or not the projection map $\pi : A \times B \rightarrow A : \pi(x, y) = x$ is a homomorphism. If $\pi$ is a homomorphism, find $\text{Ker } \pi$ and $\text{Im } \pi$. If $\pi$ is not a homomorphism, then give a non-trivial ideal of $A \times B$.

E31) Show that the map $\phi : C[0, 1] \rightarrow \mathbb{R} \times \mathbb{R} : \phi(f) = (f(0), f(1))$ is a homomorphism. Is it an isomorphism? Why, or why not?

---

Having discussed many examples, let us now review some basic results about ring homomorphisms.

**Proposition 3:** Let $f : R_1 \rightarrow R_2$ be a homomorphism from a ring $R_1$ into a ring $R_2$. Then

i) $f(0) = 0$,

ii) $f(-x) = -f(x) \forall x \in R_1$, and

iii) $f(x - y) = f(x) - f(y) \forall x, y \in R_1$.

We will not prove this here, but you would have realised that these properties follow from the fact that $f$ is a group homomorphism from $(R_1, +)$ to $(R_2, +)$.

We will now list some more properties as exercises, for you to prove.
E32) Show that if \( f : R_1 \to R_2 \) is a ring epimorphism and \( R_1 \) is with identity \( 1 \), then \( R_2 \) is with identity \( f(1) \).

E33) Let \( f : R_1 \to R_2 \) be a ring homomorphism. Then show that

i) if \( S \) is a subring of \( R_1 \), \( f(S) \) is a subring of \( R_2 \);

ii) if \( T \) is a subring of \( R_2 \), \( f^{-1}(T) \) is a subring of \( R_1 \).

E34) Show that the homomorphic image of an ideal need not be an ideal.

E35) Let \( f : R_1 \to R_2 \) be a ring homomorphism. Show that

i) if \( f \) is surjective and \( I \) is an ideal of \( R_1 \), then \( f(I) \) is an ideal of \( R_2 \).

ii) if \( I \) is an ideal of \( R_2 \), then \( f^{-1}(I) \) is an ideal of \( R_1 \), and \( \text{Ker } f \subseteq f^{-1}(I) \).

Now let us see what the ring analogue of the isomorphism theorems is. Over here we would like to make the following remark.

**Remark 8:** Two rings are isomorphic if and only if they are algebraically identical. That is, isomorphic rings must have exactly the same algebraic properties. Thus, if \( R_1 \) is a ring with identity, then it cannot be isomorphic to a ring without identity.

Similarly, if the only ideals of \( R_1 \) are \( \{0\} \) and itself, then any ring isomorphic to \( R_1 \) must have this property too.

Let us now look at the analogue of Theorem 7 of Unit 1. Its proof, as you would recall, is along the same lines as that of the FTH for group homomorphisms.

**Theorem 4 (The Fundamental Theorem of Homomorphism):** Let \( R \) and \( S \) be two rings and \( f : R \to S \) be a ring homomorphism. Then \( R/\text{Ker } f \cong \text{Im } f \). □

Applying FTH to \( f : \mathbb{Z} \to \mathbb{Z}_m : f(n) = \bar{n} \), for \( m \geq 1 \), tells us that \( \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m \).

As another application of FTH, consider the following example.

**Example 15:** Consider \( p : R_1 \times R_2 \to R_1 : p(a,b) = a \), where \( R_1 \) and \( R_2 \) are rings. Then use the Fundamental Theorem of Homomorphism to show that \( (R_1 \times R_2)/R_2 \cong R_1 \).

**Solution:** You can see that \( p \) is onto and its kernel is \( (0,0) \mid b \in R_2 \), which is isomorphic to \( R_2 \) under the map \( (0,b) \mapsto b \).

Therefore, \( (R_1 \times R_2)/R_2 \cong R_1 \).
Example 16: Prove that the only non-trivial ring homomorphism from \( \mathbb{Z} \) into itself is \( I_\mathbb{Z} \). Further, if \( f \) and \( g \) are two isomorphisms from a ring \( R \) to \( \mathbb{Z} \), then \( f = g \).

Solution: Let \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) be a non-trivial ring homomorphism. Let \( n \) be an integer. Then \( n = 1+1+\ldots+1 \) (\( n \) times).

Therefore, \( f(n) = f(1) + f(1) + \ldots + f(1) \) (\( n \) times) = \( nf(1) \).

Next, if \( n \) is a negative integer, then \( -n \) is a positive integer. Therefore, \( f(-n) = (-n)f(1) \), i.e., \( -f(n) = -nf(1) \), since \( f \) is a homomorphism.

Thus, \( f(n) = nf(1) \) in this case too.

Also \( f(0) = 0 = 0f(1) \).

Thus, \( f(n) = nf(1) \) \( \forall n \in \mathbb{Z} \).

Now, since \( f \) is a non-trivial homomorphism, \( f(m) \neq 0 \) for some \( m \in \mathbb{Z} \).

Then, \( f(m) = f(m1) = f(m)f(1) \).

Cancelling \( f(m) \) on both sides we get \( f(1) = 1 \).

Therefore, from (1) we see that \( f(n) = n \) \( \forall n \in \mathbb{Z} \), i.e., \( f = I_\mathbb{Z} \).

For the second statement, note that the composition is an isomorphism from \( \mathbb{Z} \) onto itself.

There, \( f \circ g^{-1} = I_\mathbb{Z} \), i.e., \( f = g \).

E36) What does the Fundamental Theorem of Homomorphism say in Examples 11-14?

E37) Apply the Fundamental Theorem of Homomorphism for rings to prove that \( \mathbb{C}^5/\mathbb{C}^1 \cong \mathbb{C}^2 \).

E38) (Second isomorphism theorem) Let \( S \) be a subring, and \( I \) be an ideal of a ring \( R \). Show that \( (S + I)/I \cong S/(S \cap I) \).

E39) (Third isomorphism theorem) Let \( I \) and \( J \) be ideals of a ring \( R \) such that \( J \subseteq I \). Show that \( I/J \) is an ideal of the ring \( R/J \) and that \( (R/J)/(I/J) \cong R/I \).

We halt this recall of basic ring theory here. In the next unit we shall look at a particular class of commutative rings. For now, we briefly summarise what we have done in this unit.

8.7 SUMMARY

In this unit, we have helped you revisit the following points.

1) The definition, and examples, of a ring.

2) Some properties of a ring.
The definition, and examples, of a commutative ring and a ring with identity.

The definition, and examples, of a subring.

The intersection of subrings is a subring of the ring.

The Cartesian product of subrings is a subring of the Cartesian product of the corresponding rings.

The definition, and examples, of an ideal.

The definition, and examples, of a quotient ring.

If $I$ is a left ideal, or a right ideal, or an ideal of a ring $R$ with identity, and $1 \in I$, then $I = R$.

If $I$ and $J$ are ideals of a ring $R$, then $I \cap J, I + J$ and $IJ$ are also ideals of $R$.

The definition, and examples, of a quotient ring.

The definition of a ring homomorphism, its kernel and its image, along with several examples.

The direct or inverse image of a subring under a homomorphism is a subring.

If $f : R \to S$ is a homomorphism, then
i) $\text{Im } f$ is a subring of $S$,
ii) $\text{Ker } f$ is an ideal of $R$,
iii) $f^{-1}(I)$ is an ideal of $R$ for every ideal $I$ of $S$,
iv) if $f$ is surjective, then $f(I)$ is an ideal of $S$.

The definition, and examples, of a ring isomorphism.

Applications of the Fundamental Theorem of Homomorphism for rings, which says that if $f : R \to S$ is a ring homomorphism, then $(R/\text{Ker } f) \cong \text{Im } f$.

<table>
<thead>
<tr>
<th>SOLUTIONS/ANSWERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E1</strong></td>
</tr>
</tbody>
</table>
Finally, you should check that the right and left distributive laws hold, i.e., R3 is satisfied. Thus, \((\mathbb{Z} + i\mathbb{Z}, +, \cdot)\) is a ring.

E2) We define addition and multiplication in \(\mathbb{Q} + \sqrt{2} \mathbb{Q}\) by
\[
(a + \sqrt{2} b) + (c + \sqrt{2} d) = (a + c) + \sqrt{2} (b + d),
\]
and
\[
(a + \sqrt{2} b). (c + \sqrt{2} d) = (ac + 2bd) + \sqrt{2}(ad + bc) \quad \forall a, b, c, d \in \mathbb{Q}.
\]
Since + is associative and commutative in \(\mathbb{R}\), the same holds for + in \(\mathbb{Q} + \sqrt{2} \mathbb{Q}\).
\[0 = 0 + \sqrt{2} 0\]
is the additive identity, and \((-a) + \sqrt{2} (-b)\) is the additive inverse of \(a + \sqrt{2} b\). Since multiplication in \(\mathbb{R}\) is associative, R2 holds also. Since multiplication distributes over addition in \(\mathbb{R}\), it does so in \(\mathbb{Q} + \sqrt{2} \mathbb{Q}\) as well, that is, R3 holds. Thus, \((\mathbb{Q} + \sqrt{2} \mathbb{Q}, +, \cdot)\) is a ring.

E3) \(S\) is a subset of \(M_2(\mathbb{R})\). So, the operations on \(S\) are those on \(M_2(\mathbb{R})\).
\[
\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a + c & 0 \\ b + d & 0 \end{bmatrix} \in S \quad \text{and} \quad \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} = \begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \in S.
\]
Thus, + and \(\cdot\) are closed on \(S\).
You can check that \((S, +) \leq (M_2(\mathbb{R}), +)\). Hence, R1 is satisfied. Since \(\cdot\) is associative in \(M_2(\mathbb{R})\), it is associative in \(S\). Hence, R2 is satisfied. Since \(\cdot\) distributes over + in \(M_2(\mathbb{R})\), R3 is satisfied by \((S, +, \cdot)\). Hence, \((S, +, \cdot)\) is a ring.

E4) \(\cup\) and \(\cap\) are well-defined binary operations on \(\wp(X)\).
Note that \((\wp(X), \cup)\) is not a group, since for any \(A \subseteq X\), \(A \neq \emptyset\), there is no \(B \subseteq X\) such that \(A \cup B = \emptyset\), the identity w.r.t. \(\cup\). Hence, \((\wp(X), \cup, \cap)\) is not a ring.

E5) The ring in E3 is a ring without identity since the identity, \(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\) \(\notin S\).

E6) Let us first check that + and \(\cdot\), as defined, are binary operations on \(\text{End} A\). For all \(a, b \in A\),
\[
(f + g)(a + b) = f(a + b) + g(a + b)
\]
\[
= (f(a) + f(b)) + (g(a) + g(b))
\]
\[
= (f(a) + g(a)) + (f(b) + g(b))
\]
\[
= (f + g)(a) + (f + g)(b), \quad \text{and}
\]
\[
(f \cdot g)(a + b) = f(g(a + b))
\]
\[
= f(g(a) + g(b))
\]
\[
= f(g(a)) + f(g(b))
\]
\[
= (f \cdot g)(a) + (f \cdot g)(b)
\]
Thus, \( f + g \) and \( f \cdot g \in \text{End} A \).

Now let us see if \((\text{End} A, +, \cdot)\) satisfies R1-R3.

Since \(+\) in the abelian group \( A \) is associative and commutative, so is \(+\) in \( \text{End} A \). The zero homomorphism on \( A \) is the zero element in \( \text{End} A \). \((-f)\) is the additive inverse of \( f \in \text{End} A \). Thus, \((\text{End} A, +)\) is an abelian group.

You also know that the composition of functions is an associative operation in \( \text{End} A \).

Finally, to check R3 we look at \( f \cdot (g + h) \) for any \( f, g, h \in \text{End} A \). Now for any \( a \in A \),

\[
[f \cdot (g + h)](a) = f((g + h)(a)) \\
= f(g(a) + h(a)) \\
= f(g(a)) + f(h(a)) \\
= (f \cdot g)(a) + (f \cdot h)(a) \\
= (f \cdot g + f \cdot h)(a)
\]

\[\therefore f \cdot (g + h) = f \cdot g + f \cdot h.\]

We can similarly prove that \((f + g) \cdot h = f \cdot h + g \cdot h\).

Thus, R1-R3 are satisfied for \( \text{End} A \).

Hence, \((\text{End} A, +, \cdot)\) is a ring.

Note that \( \cdot \) is not commutative since \( f \circ g \) need not be equal to \( g \circ f \) for \( f, g \in \text{End} A \).

I : \( A \rightarrow A : I(a) = a \) is an endomorphism of \( A \), with \( I \circ f = f \circ I \) \( \forall f \in \text{End} A \). Hence \( \text{End} A \) is a ring with identity.

E7) The addition and multiplication in \( A \times B \) are defined componentwise. The zero element of \( A \times B \) is \((0,0)\). The additive inverse of \((a,b)\) is \((-a, \ominus b)\), where \( \ominus b \) denotes the inverse of \( b \) with respect to \( \oplus \).

Since the multiplications in \( A \) and \( B \) are associative, \( \square \) is associative in \( A \times B \). Again, using the fact that R3 holds for \( A \) and \( B \), you can show that R3 holds for \( A \times B \). Thus, \((A \times B, \boxplus, \boxtimes)\) is a ring.

Now, for \((a, b), (c, d) \in A \times B \), \((a, b) \boxtimes (c, d) = (c, d) \boxtimes (a, b) \) iff \( ac = ca \) and \( b \circ d = d \circ b \). Thus, \( A \times B \) is commutative iff both \( A \) and \( B \) are commutative.

E8) Here \( + \) and \( \cdot \) are defined as follows.

\[
(a_1 + ib_1 + jc_1 + kd_1) + (a_2 + ib_2 + jc_2 + kd_2) \\
= (a_1 + a_2) + i(b_1 + b_2) + j(c_1 + c_2) + k(d_1 + d_2),
\]

\[
(a_1 + ib_1 +jc_1 + kd_1) \cdot (a_2 + ib_2 + jc_2 + kd_2) \\
= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + i(b_1a_2 + a_1b_2 + c_1d_2 - c_2d_1) \\
+ j(a_2c_1 + a_1c_2 + b_1b_2 - d_2b_1) + k(d_1a_2 + a_1d_2 + b_1c_2 - b_2c_1).
\]

Thus, \( + \) and \( \cdot \) are closed on \( \mathbb{H} \).

You can check that \((\mathbb{H}, +)\) is an abelian group, with additive identity \( 0 \).
Again, check that \( \cdot \) satisfies associativity on \( \mathbb{H} \), and 1 is the identity w.r.t. \( \cdot \).

Finally, check that \( \cdot \) distributes over + in \( \mathbb{H} \).

E9) i) \( S \neq \emptyset \), since \( 0 \in S \).
    Also check that for \( A, B \in S \), \( A - B \in S \) and \( AB \in S \).
    Hence, \( S \) is a subring of \( M_2(\mathbb{Z}) \).

    ii) \[
    \begin{bmatrix}
    1 & 0 \\
    0 & 1 \\
    \end{bmatrix}
    \in S.
    \] Hence \( S \) has identity, which is the same as that of \( M_2(\mathbb{Z}) \).

E10) Since \( A \) is a subring of \( B \), \( A \neq \emptyset \) and \( \forall x, y \in A \), \( x - y \in A \) and \( xy \in A \).

Here the addition and multiplication are those defined on \( B \). But these are the same as those defined on \( C \) since \( B \) is a subring of \( C \).

Thus, \( A \) is a subring of \( C \).

E11) No, there are several counterexamples. For instance, take \( R = \mathbb{Z} \), and the subset \( \{1\} \). This is not a subring, since \( \{1\} \), + is not a group. In fact, any finite subset of \( \mathbb{Z} \), apart from \( \{0\} \), will not be a subring of \( \mathbb{Z} \).

E12) \( S_1 \) and \( S_2 \) are subrings of \( R_1 \) and \( R_2 \), so that \( S_1 \neq \emptyset \) and \( S_2 \neq \emptyset \).
\[\therefore S_1 \times S_2 \neq \emptyset.\]

Now, let \((a, b) \) and \((a', b') \) \( \in S_1 \times S_2 \). Then \( a, a' \in S_1 \) and \( b, b' \in S_2 \).
As \( S_1 \) and \( S_2 \) are subrings, \( a - a', a - a' \in S_1 \) and \( b - b', b - b' \in S_2 \).
(We are using + and \( \cdot \) for both \( R_1 \) and \( R_2 \) here, for convenience.)

Hence, \((a, b) - (a', b') = (a - a', b - b') \in S_1 \times S_2 \), and \((a, b) \cdot (a', b') = (a a', b b') \in S_1 \times S_2 \).
Thus, \( S_1 \times S_2 \) is a subring of \( R_1 \times R_2 \).

E13) \( 2\mathbb{Z} \times \mathbb{R} \), \( 3\mathbb{Z} \times \{0\} \) are two among infinitely many examples.

E14) Note that the two sets are \( 3\mathbb{Z}_6 \) and \( 2\mathbb{Z}_6 \). You know that they are subrings of \( \mathbb{Z}_6 \). Now, by elementwise multiplication you can check that \( r x \in 3\mathbb{Z}_6 \forall r \in 3\mathbb{Z}_6 \) and \( x \in 3\mathbb{Z}_6 \).

(For instance, \( 3 \cdot 3 = 15 = 3 \in 3\mathbb{Z}_6 \).)

You can similarly see that \( r x \in 2\mathbb{Z}_6 \forall r \in 2\mathbb{Z}_6 \), \( x \in 2\mathbb{Z}_6 \).

Thus, \( 3\mathbb{Z}_6 \) and \( 2\mathbb{Z}_6 \) are ideals of \( \mathbb{Z}_6 \).

E15) For example, \( S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \in \mathbb{Z} \right\} \) is a subring of \( M_2(\mathbb{Z}) \). However, it is not an ideal of \( M_2(\mathbb{Z}) \) since, for example, \( \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin S \).

E16) \( I_a \neq \emptyset \), since \( 0 \in I_a \).
Ring Theory

\( f, g \in I_a \Rightarrow (f - g)(a) = f(a) - g(a) = 0 \Rightarrow f - g \in I_g. \)

\( f \in I_a, \ g \in C[0, 1] \Rightarrow (fg)(a) = f(a)g(a) = 0 \Rightarrow fg \in I_a. \)

\( \therefore I_a \) is an ideal of \( C[0, 1]. \)

You can check that if \( f \in J_a \), then \(-f \notin J_a\). Hence \( J_a \) is not even a subring of \( C[0, 1] \), and hence certainly not an ideal of \( C[0, 1]. \)

E17) \( Ra \) is a subring of \( R \) (see Example 4).

Also, for \( r \in R \) and \( xa \in Ra \),

\( r(xa) = (rx)a \in Ra. \)

\( \therefore Ra \) is a left ideal of \( R. \)

You can similarly show that \( aR \) is a right ideal of \( R. \)

E18) You can check that any element of the ideal generated by \( \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \) is of the form

\( \sum_{i=1}^{n} \begin{bmatrix} a_i \delta_i & \delta_i \\ c_i r_i & c_i \delta_i \end{bmatrix}, a_i, c_i, r_i, \delta_i \in \mathbb{Z}. \)

However, any element of \( M_2(\mathbb{Z}) \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \) is of the form \( \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix} \), for \( a, c \in \mathbb{Z}. \)

So, for example, \( \begin{bmatrix} 6 & 10 \\ -3 & -5 \end{bmatrix} \) is in the ideal, but not in the left ideal, generated by \( \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \)

Thus, the two sets are not equal.

E19) \( \overline{3} \mathbb{Z}_{10} = \{ \overline{3}x \mid x \in \mathbb{Z}_{10} \} = \{ \overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27} \} = \{ \overline{0}, \overline{3}, \overline{6}, 9, \overline{2}, \overline{5}, \overline{8}, \overline{1}, \overline{4}, \overline{7} \} = \mathbb{Z}_{10}. \)

\( \overline{5} \mathbb{Z}_{10} = \{ \overline{0}, \overline{5} \}. \)

E20) i) Since \( \overline{6}^2 = \overline{36} = \overline{0} \) in \( \mathbb{Z}_9 \), \( \overline{6} \) is nilpotent in \( \mathbb{Z}_9. \)

ii) Let \( N = \{ a \in R \mid a^n = 0 \text{ for some positive integer } n \} \). Then \( 0 \in N. \)

Also, if \( a, b \in N \), then \( a^n = 0 \) and \( b^m = 0 \) for some positive integers \( m \) and \( n. \)

Now, \( (a - b)^{m+n} = \sum_{r=0}^{m+n} \binom{m+n}{r} a^r (-b)^{m+n-r} \) (since \( R \) is commutative).

For each \( r = 0, 1, \ldots, m+n \), either \( r \geq n \) or \( m+n-r \geq m \), and hence, either \( a^r = 0 \) or \( b^{m+n-r} = 0. \) Thus, each term \( a^r b^{m+n-r} = 0. \) So \( (a - b)^{m+n} = 0. \)

Thus, \( a - b \in N \) whenever \( a, b \in N. \)

Finally, if \( a \in N, a^n = 0 \) for some positive integer \( n \), and hence, for any \( r \in R, (ar)^n = a^n r^n = 0, \) i.e., \( ar \in N. \)
So, \( N \) is an ideal of \( R \).

E21) \( \forall x \in \mathbb{Z}, x^n = 0 \Rightarrow x = 0 \). Hence, the nil radical of \( \mathbb{Z} = \{0\} \). Similarly, the nil radical of \( \mathbb{R} \) is \( \{0\} \).

Let the nil radical of \( \mathbb{Z}_q \) be \( N \). Then \( \overline{0} \in N \).

\( \overline{1} \in N \) since \( \overline{1}^n = \overline{1} \neq \overline{0} \) for all \( n \).

\( \overline{2}^3 = \overline{0} \Rightarrow \overline{2} \in N \).

\( \overline{3}^n \neq \overline{0} \forall n \). \( \therefore \overline{3} \notin N \).

Similarly, you can check that \( \overline{4}, \overline{6} \in N \) and \( \overline{5}, \overline{7} \notin N \).

\( \therefore N = \{ \overline{0}, \overline{2}, \overline{4}, \overline{6} \} = \langle \overline{2} \rangle \).

For any \( A \in \mathcal{P}(X) \), \( A^n = A \cap A \cap \ldots \cap A = A \forall n \).

Thus, \( A^n = \emptyset \) iff \( A = \emptyset \). Thus, the nil radical of \( \mathcal{P}(X) \) is \( \{ \emptyset \} \).

E22) i) For any \( a \in I \) and \( b \in J \), \( ab \in I \) and \( ab \in J \).

Thus, \( ab \in I \cap J \). Since \( I \cap J \) is an ideal, any finite sum of such elements will also be in \( I \cap J \). Thus, \( IJ \subseteq I \cap J \).

Next, by definition \( I \cap J \subseteq I \) and \( I \cap J \subseteq J \).

Also, \( I \subseteq I + J \), \( J \subseteq I + J \).

ii) Let \( A \) be an ideal of \( R \) containing \( I \) as well as \( J \). Then certainly \( I + J \subseteq A \). Thus, (ii) is proved.

iii) Let \( B \) be an ideal of \( R \) such that \( B \subseteq I \) and \( B \subseteq J \). Then certainly, \( B \subseteq I \cap J \). Thus, (iii) is proved.

iv) We want to show that \( I \cap J \subseteq IJ \).

Let \( x \in I \cap J \). Then \( x \in I \) and \( x \in J \).

Since \( 1 \in R = I + J \), \( 1 = i + j \), for some \( i \in I \) and \( j \in J \).

\( \therefore x = x.1 = xi + xj = ix + xj \in IJ \).

Thus, \( I \cap J \subseteq IJ \).

E23) Check that \( 1 + I \) is the identity of \( R/I \), where \( 1 \) is the identity of \( R \).

E24) Since \( 1 \in I \), you know that \( I = R \).

\( \therefore R/I = \{0\} \).

E25) Let \( x + N \in R/N \) be a nilpotent element.

Then \( (x + N)^n = N \) for some positive integer \( n \).

\( \Rightarrow x^n \in N \) for some positive integer \( n \).

\( \Rightarrow (x^n)^m = 0 \) for some positive integer \( m \).

\( \Rightarrow x^{nm} = 0 \) for some positive integer \( nm \).

\( \Rightarrow x \in N \).

\( \Rightarrow x + N = 0 + N \), the zero element of \( R/N \).

Thus, \( R/N \) has no non-zero nilpotent elements.

E26) For \( x, y \in S \),
Ring Theory

\[ i(x + y) = x + y = i(x) + i(y), \text{ and} \]
\[ i(xy) = xy = i(x)i(y) \]

\[ \therefore i \text{ is a homomorphism.} \]

\[ \text{Ker } i = \{ x \in S \mid i(x) = 0 \} = \{0\}. \]
\[ \text{Im } i = \{ i(x) \mid x \in S \} = S. \]

E27) \( f : \mathbb{Z} \to 2\mathbb{Z} : f(x) = 2x \) is a group homomorphism.

However, \( f(2.3) = f(6) = 12, \) and \( f(2).f(3) = 4.6 = 24. \)

Thus, \( f(2.3) \neq f(2)f(3). \)

\[ \therefore f \text{ is not a ring homomorphism.} \]

E28) For any \( x, y \in \mathbb{R}_1, f(x + y) = 0 = 0 + 0 = f(x) + f(y), \) and
\[ f(xy) = 0 = 0 = f(x).f(y). \]

\[ \therefore f \text{ is a homomorphism.} \]

\[ \text{Ker } f = \{ x \in \mathbb{R}_1 \mid f(x) = 0 \} = \mathbb{R}_1. \]
\[ \text{Im } f = \{0\}. \]

E29) Since \( \text{Im } f \neq M_2(\mathbb{Z}) \) (e.g., \( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \not\in \text{Im } f), f \) is not surjective, and hence not an isomorphism.

E30) For any \((a, b), (c, d) \in A \times B, \)
\[ \pi((a, b) + (c, d)) = \pi(a + c, b + d) = a + c = \pi(a, b) + \pi(c, d), \]
\[ \pi((a, b)(c, d)) = \pi(ac, bd) = ac = \pi(a, b)\pi(c, d). \]

Thus, \( \pi \) is a ring homomorphism.

\[ \text{Ker } \pi = \{ (a, b) \in A \times B \mid a = 0 \} = \{0\} \times B. \]
\[ \text{Im } \pi = \{ \pi(a, b) \mid (a, b) \in A \times B \} = \{a \mid (a, b) \in A \times B \} = A. \]

E31) For \( f, g \in C[0, 1], \)
\[ \phi(f + g) = ((f + g)(0), (f + g)(1)) \]
\[ = (f(0), f(1)) + (g(0), g(1)) \]
\[ = \phi(f) + \phi(g), \] and
\[ \phi(fg) = (fg(0), fg(1)) = (f(0), g(0))(f(1), g(1)) \]
\[ = \phi(f)\phi(g). \]

\[ \therefore \phi \text{ is a homomorphism.} \]

\( \phi \) is not an isomorphism, because, for example,
\[ f : [0, 1] \to \mathbb{R} : f(x) = \sqrt{\frac{1}{4} - \left(x - \frac{1}{2}\right)^2} \text{ is in Ker } \phi \text{ and } f \neq 0. \]

E32) For any \( r \in \mathbb{R}_2 \exists s \in \mathbb{R}_1 \) such that \( r = f(s). \)

Thus, \( r = f(s) = f(scdot l) = f(s)f(l) = rf(l). \)
Similarly, \( r = f(l)r \ \forall r \in \mathbb{R}_2. \)

Hence \( f(l) \) is the identity of \( \mathbb{R}_2. \)

E33) We will prove (ii). The proof of (i) is similar.

Firstly, since \( T \neq \emptyset, f^{-1}(T) \neq \emptyset. \)

Next, \( a, b \in f^{-1}(T). \)
\[ \Rightarrow f(a), f(b) \in T \]
\[ \Rightarrow f(a) - f(b) \in T \text{ and } f(a)f(b) \in T \]
\[ \Rightarrow f(a - b) \in T \text{ and } f(ab) \in T \]
\[ \Rightarrow a - b \in f^{-1}(T) \text{ and } ab \in f^{-1}(T) \]
\[ \Rightarrow f^{-1}(T) \text{ is a subring of } R_i. \]

E34) Consider the inclusion \( i : \mathbb{Z} \to \mathbb{R} : i(x) = x. \) You know that \( 2\mathbb{Z} \) is an ideal of \( \mathbb{Z}. \) But is \( i(2\mathbb{Z}) \) (i.e., \( 2\mathbb{Z} \)) an ideal of \( \mathbb{R}? \) No. For example,
\[ 2 \in 2\mathbb{Z}, \quad \frac{1}{4} \in \mathbb{R}, \text{ but } (2) \left( \frac{1}{4} \right) = \frac{1}{2} \notin 2\mathbb{Z}. \]

E35) Here we will prove (i), and leave (ii) to you.
Firstly, since \( I \) is a subring of \( R_1, f(I) \) is a subring of \( R_2. \)
Secondly, take any \( f(x) \in f(I) \) and \( r \in R_2. \) Since \( f \) is surjective, \( \exists s \in R_1 \) such that \( f(s) = r. \)
Then \( rf(x) = f(s)f(x) = f(sx) \in f(I), \) since \( sx \in I. \)
Similarly, \( f(x)r \in f(I). \)
Thus, \( f(I) \) is an ideal of \( R_2. \)

E36) Example 11: \( \mathbb{Z}_6/\langle 0, 3 \rangle \simeq \mathbb{Z}_3, \) that is, \( \mathbb{Z}_6/\langle 3 \rangle \simeq \mathbb{Z}_3. \)

Example 12: \( \text{Ker } \phi = \{ f \in C[0,1] \left| f \left( \frac{1}{2} \right) = 0 \right. \}. \) Also, \( \text{Im } \phi = \mathbb{R}. \)

So \( C[0,1]/\text{Ker } \phi \simeq \mathbb{R}. \)

Example 13: \( \text{Ker } f = \{ 0 \}, \text{Im } f = \{ n \mid n \in \mathbb{Z} \}. \) So, FTH says that \( \mathbb{Z} \simeq \{ n \mid n \in \mathbb{Z} \}. \)

Example 14: \( \phi(X)/\text{Ker } f \simeq \phi(Y). \)

E37) Define \( \pi : \mathbb{C}^5 \to \mathbb{C}^2 : \pi(z_1, z_2, z_3, z_4, z_5) = (z_1, z_2). \)
Then \( \pi \) is well-defined.
Also \( \pi[(z_1, z_2, z_3, z_4, z_5) + (w_1, w_2, w_3, w_4, w_5)] \]
\[ = \pi(z_1 + w_1, z_2 + w_2, z_3 + w_3, z_4 + w_4, z_5 + w_5) \]
\[ = (z_1 + w_1, z_2 + w_2) = (z_1, z_2) + (w_1, w_2) \]
\[ = \pi(z_1, z_2, z_3, z_4, z_5) + \pi(w_1, w_2, w_3, w_4, w_5). \]
Similarly, check that \( \pi(z, w) = \pi(z).\pi(w), \) where \( z, w \in \mathbb{C}^5. \)

For any \( (z_1, z_2) \in \mathbb{C}^2, \) \( \pi(z_1, z_2, 0, 0, 0) = (z_1, z_2). \) Hence \( \text{Im } \pi = \mathbb{C}^2. \)

Ker \( \pi = \{ (z_1, z_2, z_3, z_4, z_5) \in \mathbb{C}^5 \left| z_1 = 0 = z_2 \right. \} = \{ (0, 0, z_3, z_4, z_5) \in \mathbb{C}^5 \}. \)

So, by FTH, \( \mathbb{C}^5/\text{Ker } \pi \simeq \mathbb{C}^2 \ldots (1) \)
Now define \( f : \text{Ker } \pi \to \mathbb{C}^3 : f(0, 0, z_3, z_4, z_5) = (z_3, z_4, z_5). \)
Then \( f \) is an isomorphism. Hence \( \text{Ker } \pi \simeq \mathbb{C}^3, \) \ldots (2)
Thus, by (1) and (2) we get \( \mathbb{C}^5/\mathbb{C}^3 \simeq \mathbb{C}^2. \)

E38) Since \( I \) is an ideal of \( R \) and \( I \subseteq S + I, \) it is an ideal of \( S + I. \)
Thus, \((S+I)/I\) is a well-defined ring.
Define \(f : S \to (S+I)/I : f(x) = x + I\).
Then, you can check that \(f\) is well-defined, \(f(x + y) = f(x) + f(y)\), and \(f(xy) = f(x)f(y)\) for all \(x, y \in S\).
Further, check that \(f\) is surjective and \(\ker f = S \cap I\).
Thus, the FTH tells us that \(S/(S \cap I) = (S+I)/I\).

E39) Define \(f : R/J \to R/I : f(r + J) = r + I\).
You should check that \(f\) is well-defined, \(f\) is a ring homomorphism, \(f\) is surjective and \(\ker f = I/J\).
Thus, \(I/J\) is an ideal of \(R/J\), and by the FTH, we see that \((R/J)/(I/J) = R/I\).
9.1 INTRODUCTION

In the previous unit, you revisited basic concepts of ring theory. In this unit, we shall focus on integral domains. To start with, in Sec.9.2, we help you recall some basic properties of an integral domain. Here we also take a quick review of two particular types of ideals of a commutative ring, prime ideals and maximal ideals.

Then, in the rest of the unit, we focus on three special kinds of integral domains. These domains were mainly studied with a view to develop number theory. Let us say a few introductory sentences about them.

You would recall that the division algorithm holds for $\mathbb{Z}$ and $F[x]$, where $F$ is a field. Actually, there are lots of other domains for which this algorithm is true. Such integral domains are called Euclidean domains. We shall discuss their properties in Sec.9.3.

In the next section, Sec.9.4, we shall look at some domains which are algebraically very similar to $\mathbb{Z}$. These are the principal ideal domains, so called because every ideal in them is principal.

Finally, in Sec.9.5, we shall discuss domains in which every non-zero non-invertible element can be uniquely factorised in a particular way. Such domains are appropriately called unique factorisation domains. While discussing them, we shall also introduce you to the concept of an irreducible element of a domain.

While going through the unit, you will also see the relationship between Euclidean domains, principal ideal domains and unique factorisation domains.

In this unit any ring we consider, unless specified otherwise, is a commutative ring with unity.

Objectives

After studying this unit, you should be able to

- define, and give examples of, an integral domain;
- check whether a function is a Euclidean valuation or not;
• define, and give examples of, a principal ideal domain;
• define, and give examples of, a unique factorisation domain;
• obtain the g.c.d of any pair of elements in a unique factorisation domain;
• prove, and use, the relationship between Euclidean domains, principal ideal domains and unique factorisation domains.

### 9.2 INTEGRAL DOMAINS

You know that the product of two non-zero integers is a non-zero integer, i.e. if \( m, n \in \mathbb{Z} \) such that \( m \neq 0, n \neq 0 \), then \( mn \neq 0 \). On the other hand, you know, that in the ring \( \mathbb{Z}_6 \), \( 2 \neq 0 \) and \( 3 \neq 0 \), yet \( 2 \cdot 3 = 0 \). This example leads us to the following definitions.

**Definitions:**

1) A non-zero element \( r \) in a ring \( R \) is called a **zero divisor** in \( R \) if there exists a non-zero element \( s \) in \( R \) such that \( rs = 0 \). (Note that here \( s \) will be a zero divisor too.)

2) A commutative ring \( R \) with identity is called an **integral domain** if it has no zero divisors.

So, as mentioned earlier, \( \mathbb{Z} \) is an integral domain, while \( \mathbb{Z}_6 \) is not. Let us look at some more examples.

**Example 1:** Show that \( \mathbb{C}[0, 1] \) is not an integral domain.

**Solution:**
Firstly, \( \mathbb{C}[0, 1] \) is commutative, and with identity, which is the constant function 1.

Next, consider the functions \( f \) and \( g \in \mathbb{C}[0, 1] \), given by
\[
f(x) = \begin{cases} 
 x - \frac{1}{2}, & 0 \leq x \leq 1/2 \\
 0, & 1/2 \leq x \leq 1 
\end{cases} \quad \text{and} \quad g(x) = \begin{cases} 
 0, & 0 \leq x \leq 1/2 \\
 x - 1/2, & 1/2 \leq x \leq 1 
\end{cases}.
\]

Then \( f \neq 0, g \neq 0 \) and \( (fg)(x) = 0 \) \( \forall x \in [0, 1] \). Thus, \( fg \) is the zero function.

Hence, \( f \) is a zero divisor in \( \mathbb{C}[0, 1] \).

Hence \( \mathbb{C}[0,1] \) is not a domain.

***

**Example 2:** Check whether or not \( \mathbb{R}[x] \), the ring of polynomials over \( \mathbb{R} \), is an integral domain.

**Solution:**
You know that \( \mathbb{R}[x] \) is a commutative ring with unity. Now, let
\[
f(x) = \sum_{i=0}^{m} a_i x^i \quad \text{and} \quad g(x) = \sum_{j=0}^{n} b_j x^j \quad \text{be in} \quad \mathbb{R}[x] \quad \text{such that} \quad f(x) \cdot g(x) = 0.
\]

Then \( a_0 b_0 = 0 \), and \( a_i = 0 = b_j \ \forall \ i \geq 1, \ j \geq 1 \).

\[\Rightarrow a_0 = 0 \ \text{or} \ b_0 = 0\]

\[\Rightarrow f(x) = 0 \ \text{or} \ g(x) = 0.
\]

Thus, \( \mathbb{R}[x] \) has no zero divisors.

***

**Example 3:** Show that even if \( A \) and \( B \) are integral domains, \( A \times B \) is not an integral domain.
**Solution:** For every $a \neq 0$ in $A$, $(a, 0)$ is a zero divisor in $A \times B$ because, for any $b \neq 0$ in $B$, $(a, 0)(0, b) = (0, 0)$. Hence the result.

***

Try some exercises now.

---

**E1)** Let $n \in \mathbb{N}$ and $m|n$, $1 < m < n$. Then show that $\overline{m}$ is a zero divisor in $\mathbb{Z}_n$. Is the converse true? Give reasons for your answer.

**E2)** Show that if $p$ is a prime, then $\mathbb{Z}_p$ is an integral domain.

**E3)** Is the ring $\wp(X)$, where $X$ is a set with at least two elements, an integral domain? Why, or why not?

**E4)** Which of the following rings have zero divisors? Give reasons for your answers.

$\mathbb{Z}_4$, $\mathbb{Z}_5$, $2\mathbb{Z}$, $\mathbb{Z} + i\mathbb{Z}$, $\mathbb{R} \times \mathbb{R}$.

**E5)** In a domain, show that the only solutions of the equation $x^2 = x$ are $x = 0$ and $x = 1$.

**E6)** If $A$ and $B$ are rings such that $A \subseteq B$ and $A$ is an integral domain, then $B$ must be an integral domain. True or false? Why, or why not?

---

Let us now recall how the concepts of divisibility, and related concepts, are suitably generalised to any commutative ring.

**Definition:** In a commutative ring $R$, we say that an element $a$ divides an element $b$ (and denote it by $a | b$) if $b = ra$ for some $r \in R$. In this case we also say that $a$ is a factor of $b$, or $a$ is a divisor of $b$.

Thus, for example, $\overline{3}$ divides $\overline{6}$ in $\mathbb{Z}_7$, since $\overline{3} \cdot \overline{2} = \overline{6}$. Similarly, $2 | (-4)$ in $\mathbb{Z}$, since $(-4) = 2(-2)$.

Related to this is the concept of a unit, which we will now discuss.

**Definition:** Let $R$ be a commutative ring with identity $1$. An element $a \in R$ is called a unit (or an invertible element) in $R$, if $a | 1$. In other words, $a$ is a unit in $R$ if $ab = 1$ for some $b \in R$, i.e., if $a$ has a multiplicative inverse in $R$.

For example, both $1$ and $-1$ are units in $\mathbb{Z}$ since $1 \cdot 1 = 1$ and $( -1)(-1) = 1$.

**Caution:** Note the difference between a unit in $R$ and the unity in $R$. The unity is the identity with respect to multiplication, and is certainly a unit. But a ring can have other units too, as you have just seen in the case of $\mathbb{Z}$.

Now, can we obtain all the units in a commutative ring $R$ with identity? Call this set $U(R)$. You know that every non-zero element in a field $F$ is
invertible. Thus, \( U(F) = F' = F \setminus \{0\} \). Let us look at some other cases also.

**Example 4:** Obtain \( U(C[x]) \).

**Solution:** Let \( f(x) \in C[x] \) be a unit. Then \( \exists g(x) \in C[x] \) such that \( f(x)g(x) = 1 \). Therefore,
\[
\deg(f(x)g(x)) = \deg(1) = 0, \text{ i.e.,} \quad \deg(f(x)) + \deg(g(x)) = 0.
\]
Since \( \deg(f(x)) \) and \( \deg(g(x)) \) are non-negative integers, this equation can hold only if \( \deg(f(x)) = 0 = \deg(g(x)) \). Thus, \( f(x) \) must be a non-zero constant, i.e., an element of \( \mathbb{C} \setminus \{0\} \). Thus, the units of \( \mathbb{C}[x] \) are the non-zero elements of \( \mathbb{C} \).
That is, the units of \( C \) and \( C[x] \) coincide.

***

**Example 5:** Find all the units in \( R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \).

**Solution:** Let \( a + b\sqrt{-5} \) be a unit in \( R \). Then there exists \( c + d\sqrt{-5} \in R \) such that \( (a + b\sqrt{-5})(c + d\sqrt{-5}) = 1 \)
\[
\Rightarrow (ac - 5bd) + (bc + ad)\sqrt{-5} = 1
\]
\[
\Rightarrow ac - 5bd = 1 \quad \text{and} \quad bc + ad = 0
\]
\[
\Rightarrow abc - 5b^2d = b \quad \text{and} \quad bc + ad = 0
\]
\[
\Rightarrow a(-ad) - 5b^2d = b, \text{ substituting } bc = -ad.
\]
So, if \( b \neq 0 \), then \( (a^2 + 5b^2) \mid b \), which is not possible since \( a, b \in \mathbb{Z} \).
\[
\therefore \ b = 0.
\]
Thus, the only units of \( R \) are the invertible elements of \( \mathbb{Z} \), i.e., \( U(R) = \{\pm 1\} \).

***

We have asked you to find \( U(R) \) for other rings \( R \) in the following exercises.

---

**E7** Find all the units in

- i) \( \mathbb{Z}_6 \),
- ii) \( \mathbb{Z}/5\mathbb{Z} \),
- iii) \( \mathbb{Q} + i\mathbb{Q} \).

**E8** Let \( R \) be a commutative ring with unity. Prove that \( u \in R \) is a unit iff \( Ru = R \).

**E9** Let \( R \) be an integral domain. Show that

- i) \( u \) is a unit in \( R \) iff \( u \mid 1 \).
- ii) for \( a, b \in R \), \( a \mid b \) and \( b \mid a \) iff \( a \) and \( b \) are associates in \( R \).

**E10** If \( R \) is a commutative ring with identity, show that \( (U(R), \cdot) \) is a group. Further, if \( \phi: R \rightarrow R' \) is a ring homomorphism between commutative rings with unity, show that \( \phi \) induces a group homomorphism \( \psi: U(R) \rightarrow U(R') \).

---

Let us, now, go back to school mathematics for a moment, where you studied about the gcd, i.e., the HCF of any two integers. We shall generalise this concept to any commutative ring.
**Definitions:** Given two elements $a$ and $b$ in a commutative ring $R$, one of which at least is non-zero, we say that $c \in R$ is a

1) **common divisor** of $a$ and $b$ if $c \mid a$ and $c \mid b$.

2) **greatest common divisor** (g.c.d, in short) of $a, b \in R$ if
   i) $c$ is a common divisor, and
   ii) for any common divisor $d$ of $a$ and $b$, $d \mid c$.

This definition can be generalised to define the g.c.d of $n$ elements in $R$, as follows.

**Definition:** The **greatest common divisor** of $a_1, \ldots, a_n$ in a commutative ring $R$ is $c \in R$ if $c \mid a_i \quad \forall i = 1, \ldots, n$, and for any common divisor $d \in R$ of $a_1, \ldots, a_n$, $d \mid c$. [Here at least one $a_i \neq 0$.]

For example, a g.c.d of $5$ and $(-15)$ in $\mathbb{Z}$ is $5$, and a g.c.d of $5$, $6$ and $7$ in $\mathbb{Z}$ is $1$.

Before considering any more examples, you need to see the relationship between any two g.c.d.s of two elements in a domain.

**Proposition 1:** Let $R$ be an integral domain and $a, b \in R$. If a g.c.d. of $a$ and $b$ exists, then it is unique up to multiplication by a unit.

**Proof:** So, let $d$ and $d'$ be two g.c.d.s of $a$ and $b$. Since $d$ is a common divisor and $d'$ is a g.c.d, we get $d \mid d'$. Similarly, we get $d' \mid d$. Thus, by E9 we see that $d$ and $d'$ are associates in $R$. Thus, the g.c.d of $a$ and $b$ is unique up to units.

This result allows us to say the g.c.d instead of a g.c.d. We denote the g.c.d of $a$ and $b$ by $(a, b)$. (This notation is also used for elements of $R \times R$. But there should be no cause for confusion. The context will clarify what we are using the notation for.)

Now, how do we obtain the g.c.d of two elements in practice? How did we do it in $\mathbb{Z}$? We looked at the common factors of the two elements and their product turned out to be the required g.c.d. We will use the same method in the following example.

**Example 6:** Find the g.c.d of $p(x) = x^2 + 3x - 10$ and $q(x) = 6x^2 - 10x - 4$ in $\mathbb{Q}[x]$.

**Solution:** By factorising them, we get $p(x) = (x - 2)(x + 5)$ and $q(x) = 2(x - 2)(3x + 1)$. The g.c.d of $p(x)$ and $q(x)$ is the product of the common factors of $p(x)$ and $q(x)$, which is $(x - 2)$.

[Note that $\alpha(x - 2)$ is also the g.c.d $\forall \alpha \in \mathbb{Q}'$, since any such $\alpha$ is a unit in $\mathbb{Q}[x]$.]
Try an exercise now.

E11) Find the g.c.d of:

i) \( \overline{2} \) and \( \overline{6} \) in \( \mathbb{Z}/\langle 8 \rangle \), and in \( \mathbb{Z}/\langle 7 \rangle \).

ii) \( x^2 + 8x + 15 \) and \( x^2 + 12x + 35 \) in \( \mathbb{Z}[x] \).

iii) \( x^3 - 2x^2 + 6x - 5,5x^3 + x^2 - 3x - \frac{3}{5} \) and \( x^2 - 2x + 1 \) in \( \mathbb{Q}[x] \).

Let us now look at the defining property of a prime number. In \( \mathbb{Z} \), you know that if \( p \) is a prime number and \( p \mid ab \), where \( a, b \in \mathbb{Z} \), then either \( p \) divides \( a \) or \( p \) divides \( b \). In other words, if \( ab \in p\mathbb{Z} \), then either \( a \in p\mathbb{Z} \) or \( b \in p\mathbb{Z} \). Because of this property, we say that \( p\mathbb{Z} \) is a prime ideal, as you may recall from your undergraduate studies.

**Definition:** A proper ideal \( P \) of a ring \( R \) is called a **prime ideal** of \( R \) if whenever \( P \mid ab \) for \( a, b \in R \), then either \( a \in P \) or \( b \in P \).

The following are examples of prime ideals.

i) \( \{0\} \) is a prime ideal of any integral domain.

ii) \( \langle m \rangle \) is a prime ideal in \( \mathbb{Z} \) iff \( m \) is a prime number or \( m = 0 \).

iii) If \( R \) is an integral domain, then \( I = \{(0, x) \mid x \in R\} \) is a prime ideal of \( R \times R \).

Try the following exercises now. They will help you engage more with the concept of ‘prime ideal’. Note that E13 actually gives the defining property of a prime ideal.

E12) Check whether or not the set \( I = \{f \in C[0, 1] \mid f(0) = 0\} \) is a prime ideal of \( C[0, 1] \).

E13) Show that an ideal \( P \) of a commutative ring \( R \) with identity is a prime ideal of \( R \) if and only if the quotient ring \( R/P \) is an integral domain.

Intimately related to the concept of a prime ideal is the following concept.

**Definition:** A non-zero element \( p \) of an integral domain \( R \) is called a **prime element** if

i) \( p \) is not a unit, and

ii) whenever \( a, b \in R \) and \( p \mid ab \), then \( p \mid a \) or \( p \mid b \).

You would also recall, from your undergraduate studies, that a **non-zero element** \( p \) of an integral domain \( R \) is a prime element if and only if \( Rp \) is a prime ideal of \( R \).
This criterion is very useful for checking whether an element is a prime element or not, or for finding out when a principal ideal is a prime ideal.

Prime ideals have several useful properties. In the following exercises we ask you to prove some of them.

**E14)** Let $R$ and $S$ be commutative rings and $f : R \to S$ be a ring epimorphism with kernel $N$. Show that

i) if $J$ is a prime ideal in $S$, then $f^{-1}(J)$ is a prime ideal in $R$.

ii) if $I$ is a prime ideal in $R$ containing $N$, then $f(I)$ is a prime ideal in $S$.

iii) the map $\phi$ between the set of prime ideals of $R$ that contain $N$ and the set of all prime ideals of $S$, given by $\phi(I) = f(I)$, is a bijection.

**E15)** i) Let $p_1, p_2 \in \mathbb{Z}$ be distinct primes. Then $< p_1 > \cap < p_2 >$ is not a prime ideal in $\mathbb{Z}$.

ii) If $I_1$ and $I_2$ are ideals of a commutative ring such that neither $I_1$ nor $I_2$ contains the other, then show that the ideal $I_1 \cap I_2$ is not prime.

Now consider the ideal $2\mathbb{Z}$ in $\mathbb{Z}$. Suppose the ideal $n\mathbb{Z}$ in $\mathbb{Z}$ is such that $2\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$. Then $n \mid 2$. $\therefore n = \pm 1$ or $n = \pm 2$. $\therefore n\mathbb{Z} = \mathbb{Z}$ or $n\mathbb{Z} = 2\mathbb{Z}$.

This shows that $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, as you can see from the following definition.

**Definition:** A proper ideal $M$ of a ring $R$ is called a **maximal ideal** if whenever $I$ is an ideal of $R$ such that $M \subseteq I \subseteq R$, then either $I = M$ or $I = R$.

Thus, a proper ideal $M$ is a maximal ideal if there is no proper ideal of $R$ which properly contains it.

A defining property of maximal ideals is what we shall now state.

**Theorem 1:** An ideal $M$ in a ring $R$ is maximal if and only if $R/M$ is a field.

(You will study about fields in detail in the next block.)

This theorem throws up a lot of examples of maximal ideals. For example, $\{0\}$ is a maximal ideal in $\mathbb{Q}$ since $\mathbb{Q}/\{0\} \cong \mathbb{Q}$, a field.

Similarly, $\mathbb{R}$ and $\mathbb{C}$ have $\{0\}$ as a maximal ideal.

Here is an important comment, relating maximal and prime ideals.

**Remark 1:** Since every field is an integral domain, **every maximal ideal of a commutative ring with identity is a prime ideal**, by E13. But the converse need not be true. For instance, $\{0\}$ is a prime ideal of $\mathbb{Z}$, but not a maximal ideal. Why? Think about this while doing E16.
E16) Show that $p\mathbb{Z}$ is maximal in $\mathbb{Z}$, where $p$ is a prime. Hence decide whether $\{0\}$ is maximal in $\mathbb{Z}$.

E17) Give an example, with justification, of an ideal of a commutative ring which is neither maximal nor prime.

Now that you have regained familiarity with domains, we shall discuss some domains with special properties.

### 9.3 EUCLIDEAN DOMAINS

You know that $\mathbb{Z}$ satisfies a division algorithm. There are many other domains that have this property. In this section we will introduce you to them and discuss some of their properties. Let us start with a definition.

**Definition:** Let $R$ be an integral domain. A function $d : R \backslash \{0\} \to \mathbb{N} \cup \{0\}$ is a **Euclidean valuation** of $R$ if the following conditions are satisfied:

i) $d(a) \leq d(ab)$ for all $a, b \in R \backslash \{0\}$, and

ii) for any $a, b \in R$, $b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

An integral domain with a Euclidean valuation is called a **Euclidean domain**.

Euclidean domains are so called because of the essential property of the division algorithm. This is the basis for the Euclidean algorithm for finding the g.c.d of any two non-zero elements in the domain. Now let us consider an example of such a domain.

**Example 7:** Show that $\mathbb{Z}$ is a Euclidean domain.

**Solution:** Define $d : \mathbb{Z} \to \mathbb{N} \cup \{0\} : d(n) = |n|$.

Then, for any $a, b \in \mathbb{Z} \backslash \{0\}$,

$$d(ab) = |ab| = |a||b|$$

$$\geq |a| \quad \text{(since $|b| \geq 1$ for $b \neq 0$)}$$

$$= d(a),$$

i.e., $d(a) \leq d(ab)$.

Further, the division algorithm in $\mathbb{Z}$ says that if $a, b \in \mathbb{Z}$, $b \neq 0$, then

$\exists q, r \in \mathbb{Z}$ such that

$$a = bq + r,$$

where $r = 0$ or $0 < |r| < |b|$.

i.e., $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Hence, $d$ is a Euclidean valuation on $\mathbb{Z}$, making $\mathbb{Z}$ a Euclidean domain.

***

For other examples try the following exercises.

E18) Show that $\mathbb{C}$, with the Euclidean valuation $d$ defined by

$$d(a) = 1 \quad \forall \ a \in \mathbb{C} \backslash \{0\},$$

is a Euclidean domain.
E19) Define the function \( d : \mathbb{R}[x] \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\} : d(f(x)) = \deg f(x) \).

Show that \( d \) is a Euclidean valuation on \( \mathbb{R}[x] \), and hence, \( \mathbb{R}[x] \) is a Euclidean domain.

Is \( d \), restricted to \( \mathbb{Z}[x] \setminus \{0\} \), a Euclidean valuation? Why, or why not?

Now we are in a position to discuss some basic properties of a Euclidean domain.

**Proposition 2:** Let \( R \) be a Euclidean domain with Euclidean valuation \( d \). Then, for any \( a \in R \setminus \{0\} \), \( d(a) = d(1) \) iff \( a \) is a unit in \( R \).

**Proof:** Let us first assume that \( a \in R \setminus \{0\} \) with \( d(a) = d(1) \).

By the division algorithm in \( R \), \( \exists q, r \in R \) such that

\[
1 = aq + r, \quad \text{where } r = 0 \quad \text{or} \quad d(r) < d(a) = d(1).
\]

Now, if \( r \neq 0 \), \( d(r) = d(r.1) \geq d(1) \). Thus, \( d(r) < d(1) \) can’t happen.

Thus, the only possibility for \( r \) is \( r = 0 \).

Therefore, \( 1 = aq \), so that \( a \) is a unit.

Conversely, assume that \( a \) is a unit in \( R \). Let \( b \in R \) such that \( ab = 1 \). Then \( d(a) \leq d(ab) = d(1) \). But we know that \( d(a) = d(a.1) \geq d(1) \). So, we must have \( d(a) = d(1) \).

Using the result above, we can immediately solve Example 4, since \( f(x) \) is a unit in \( \mathbb{C}[x] \) iff \( \deg f(x) = \deg(1) = 0 \).

Similarly, Proposition 2 tells us that \( n \in \mathbb{Z} \) is a unit in \( \mathbb{Z} \) iff \( |n| = |1| = 1 \). Thus, the only units in \( \mathbb{Z} \) are 1 and (-1).

Now let us look at the ideals of a Euclidean domain.

**Theorem 2:** Let \( R \) be a Euclidean domain, with Euclidean valuation \( d \). Then every ideal \( I \) of \( R \) is a principal ideal, i.e., \( I = Ra \) for some \( a \in R \).

**Proof:** If \( I = \{0\} \), then \( I = Ra \), where \( a = 0 \). So let us assume that \( I \neq \{0\} \).

Then \( I \setminus \{0\} \) is non-empty. Consider the set \( \{d(a)|a \in I \setminus \{0\}\} \). It has a minimal element, \( d(b) \), where \( b \in I \setminus \{0\} \). We will show that \( I = Rb \).

Since \( b \in I \) and \( I \) is an ideal of \( R \),

\[
Rb \subseteq I. \quad \text{ ...(1)}
\]

Now take any \( a \in I \). Since \( I \subseteq R \) and \( R \) is a Euclidean domain, we can find \( q, r \in R \) such that \( a = bq + r \), where \( r = 0 \) or \( d(r) < d(b) \).

Now, \( b \in I \Rightarrow bq \in I \). Also, \( a \in I \). Therefore, \( r = a - bq \in I \).

The way we have chosen \( d(b), d(r) < d(b) \) is not possible. Therefore, \( r = 0 \), and hence, \( a = bq \in Rb \).

Thus, \( I \subseteq Rb \). \quad \text{ ...(2) }

From (1) and (2), we get \( I = Rb \).

Thus, every ideal \( I \) of a Euclidean domain \( R \) with Euclidean valuation \( d \) is principal, and is generated by \( a \in I \), where \( d(a) \) is a minimal element of the set \( \{d(x)|x \in I \setminus \{0\}\} \).

**Theorem 2** tells us, for example, that every ideal of \( \mathbb{Z} \) is principal, a fact that you have already noted in Unit 8.
Now try the following exercises involving the ideals of a Euclidean domain.

E20) Show that every ideal of \( \mathbb{R}[x] \) is principal.

E21) Using \( \mathbb{Z} \) as an example, show that the set
\[ S = \{ a \in \mathbb{R} \setminus \{0\} \mid d(a) > d(l) \} \cup \{0\} \]
\[ \] is not an ideal of the Euclidean domain \( \mathbb{R} \) with Euclidean valuation \( d \).

Theorem 2 leads us to a concept that we shall discuss now.

### 9.4 PRINCIPAL IDEAL DOMAINS (PID)

In the previous section we have noted that every ideal of \( \mathbb{F}[x] \) is principal, where \( \mathbb{F} \) is a field. There are several other integral domains, apart from Euclidean domains, which have this property. Such rings have a very appropriate name.

**Definition:** An integral domain \( \mathbb{R} \) is called a principal ideal domain (PID, in short) if every ideal in \( \mathbb{R} \) is a principal ideal.

Thus, \( \mathbb{Z} \) is a PID. Can you think of another example of a PID? What about \( \mathbb{Q} \) and \( \mathbb{Q}[x] \)? In fact, by Theorem 2 all Euclidean domains are PIDs. But, the converse is not true. That is, every principal ideal domain need not be a Euclidean domain.

For example, the ring of all complex numbers of the form \( a + \frac{b}{2}(1+i\sqrt{19}) \), where \( a, b \in \mathbb{Z} \), is a principal ideal domain, but not a Euclidean domain. The proof of this is too technical for this course, so you can take our word for it for the present!

Now let us look at an example of an integral domain that is not a PID.

**Example 8:** Show that \( \mathbb{Z}[x] \) is not a PID.

**Solution:** You know that \( \mathbb{Z}[x] \) is a domain. We will show that not all its ideals are principal. Consider the ideal of \( \mathbb{Z}[x] \) generated by 2 and \( x \), i.e., \( <2, x> \). We will show that \( <2, x> \neq <f(x)> \) for any \( f(x) \in \mathbb{Z}[x] \), using the method of proof by contradiction.

So, suppose \( \exists f(x) \in \mathbb{Z}[x] \) such that \( <2, x> = <f(x)> \). Clearly, \( f(x) \neq 0 \).

Also, since 2 and \( x \) are in \( <f(x)> \), \( \exists g(x), h(x) \in \mathbb{Z}[x] \) such that
\[ 2 = f(x)g(x) \quad \text{and} \quad x = f(x)h(x). \]

Thus, \( \deg f(x) + \deg g(x) = \deg 2 = 0 \), \( \quad \quad \quad \quad \quad \quad \quad \quad \Quad(3) \)
and \( \deg f(x) + \deg h(x) = \deg x = 1 \). \( \quad \quad \quad \quad \quad \quad \quad \quad \Quad(4) \)

(3) shows that \( \deg f(x) = 0 \), i.e., \( f(x) \in \mathbb{Z} \), say \( f(x) = n \).

Then (4) shows that \( \deg h(x) = 1 \). Let \( h(x) = ax + b \), with \( a, b \in \mathbb{Z} \).

Then \( x = f(x)h(x) = n(ax + b) \).

Comparing the coefficients on either side of this equation, we see that \( na = 1 \) and \( nb = 0 \).
Thus, \( n \) is a unit in \( \mathbb{Z} \), that is, \( n = \pm 1 \), i.e., \( f(x) = \pm 1 \). Therefore, \(<1> = <x, 2>\). Thus, we can write
\[ l = x(a_0 + a_1 x + \cdots + a_r x^r) + 2(b_0 + b_1 x + \cdots + b_s x^s), \]
where \( a_i, b_j \in \mathbb{Z} \) \( \forall i = 0, 1, \ldots, r \) and \( j = 0, 1, \ldots, s \).

Now, on comparing the constant term on either side, we see that \( l = 2b_0 \). This can’t be true, since \( 2 \) is not invertible in \( \mathbb{Z} \). So we reach a contradiction. Thus, \(<x, 2>\) is not a principal ideal. Thus, \( \mathbb{Z}[x] \) is not a PID.

***

Now, try the following related exercises.

---

**E22**) Show that a subring of a PID need not be a PID.

**E23**) Will any quotient ring of a PID be a PID? Why, or why not?

---

We will now discuss some properties of divisibility in PIDs. Let us first consider some properties of the g.c.d of elements in a PID.

**Theorem 3:** Let \( R \) be a PID and \( a, b \in R \). Then \( (a, b) \) exists and is of the form \( ax + by \) for some \( x, y \in R \).

**Proof:** Consider the ideal \(<a, b>\). Since \( R \) is a PID, this ideal must be principal also. Let \( d \in R \) such that \(<a, b> = <d>\). We will show that the g.c.d of \( a \) and \( b \) is \( d \).

Since \( a \in <d> \), \( d \mid a \). Similarly, \( d \mid b \).

Now suppose \( c \in R \) such that \( c \mid a \) and \( c \mid b \).

Since \( d \in <a, b> \), \( \exists x, y \in R \) such that \( d = ax + by \).

Since \( c \mid a \) and \( c \mid b \), \( c \mid (ax + by) \), i.e., \( c \mid d \).

Thus, we have shown that \( d = (a, b) \), and \( d = ax + by \) for some \( x, y \in R \).

As we have noted earlier, \( \mathbb{F}[x] \) is a PID, for any field \( \mathbb{F} \). This leads us to the following corollary to Theorem 3.

**Corollary 1:** Let \( \mathbb{F} \) be a field. Then any two polynomials \( f(x) \) and \( g(x) \) in \( \mathbb{F}[x] \) have a g.c.d which is of the form \( a(x)f(x) + b(x)g(x) \) for some \( a(x), b(x) \in \mathbb{F}[x] \).

For example, in E11(iii), \( (x - 1) = \frac{1}{5}(x^3 - 2x^2 + 6x - 5) + \frac{(-x)}{5}(x^2 - 2x + 1) \).

Now you can use Theorem 3 to do the following exercise.

---

**E24**) Let \( R \) be a PID and \( a, b, c \in R \) such that \( a \mid bc \). Show that if \( (a, b) = 1 \), then \( a \mid c \).

---

\( a, b \in R \) are called **relatively prime** if \( (a, b) = 1 \).
Let us now discuss a concept related to that of a prime element of a domain.

**Definition:** Let \( R \) be an integral domain. We say that a non-zero element \( x \in R \) is **irreducible** if

i) \( x \) is not a unit, and

ii) if \( x = ab \) with \( a, b \in R \), then \( a \) is a unit or \( b \) is a unit.

Thus, an element is irreducible if it cannot be factored in a non-trivial way, i.e., its only factors are its associates and the units in the ring.

So, for example, the irreducible elements of \( \mathbb{Z} \) are the prime numbers and their associates. This means that an element in \( \mathbb{Z} \) is prime iff it is irreducible.

Let us look at the irreducible elements in \( \mathbb{R}[x] \) and \( \mathbb{C}[x] \), i.e., the irreducible polynomials over \( \mathbb{R} \) and \( \mathbb{C} \).

Recall the following important theorems about polynomials in \( \mathbb{C}[x] \) and \( \mathbb{R}[x] \).

**Theorem 4 (Fundamental Theorem of Algebra):** Any non-constant polynomial in \( \mathbb{C}[x] \) has a root in \( \mathbb{C} \). (In fact, it has all its roots in \( \mathbb{C} \).)

Does this tell us anything about the irreducible polynomials over \( \mathbb{C} \)? Yes. In fact, it tells us that any polynomial over \( \mathbb{C} \) can be written as a product of linear polynomials over \( \mathbb{C} \). So, Theorem 4 can also be written as follows.

**Theorem 4':** A polynomial is irreducible in \( \mathbb{C}[x] \) iff it is linear.

A corollary to this result is

**Theorem 5:** Any irreducible polynomial in \( \mathbb{R}[x] \) has degree 1 or degree 2.

We will use these results often when discussing polynomials over \( \mathbb{C} \) or \( \mathbb{R} \). Try the following exercises now.

---

**E25** Which of the following polynomials are irreducible? Give reasons for your choice.

i) \( x^2 - 2x + 1 \in \mathbb{R}[x] \)

ii) \( x^2 + x + 1 \in \mathbb{C}[x] \)

iii) \( x - i \in \mathbb{C}[x] \)

iv) \( x^3 - 3x^2 + 2x + 5 \in \mathbb{R}[x] \).

**E26** Let \( R \) be a domain and \( p \in R \) be a prime element. Show that \( p \) is irreducible.

In E26, you have seen that every prime element is irreducible in an integral domain. The converse is not necessarily true. However, it is true for a PID.

**Theorem 6:** In a PID, an element is prime iff it is irreducible.

**Proof:** Let \( R \) be a PID. From E26 you know that every prime element of \( R \) is irreducible. Now, let us prove the converse. Let \( x \in R \) be irreducible, and let
Suppose \( \gcd(x, a) = 1 \), since the only factor of \( x \) is itself, up to units. Thus, by E24, \( x \mid b \). Thus, \( x \) is prime.

Now, for a moment let us recall that an element \( p \in R \) is prime iff \( \langle p \rangle \) is a prime ideal of \( R \). If \( R \) is a PID, we shall use Theorem 6 to make a stronger statement.

**Theorem 7:** Let \( R \) be a PID. An ideal \( \langle r \rangle \) is a maximal ideal of \( R \) iff \( r \) is a prime element of \( R \).

**Proof:** If \( \langle r \rangle \) is a maximal ideal of \( R \), then it is a prime ideal of \( R \).
Therefore, \( r \) is a prime element of \( R \).
Conversely, let \( r \) be prime, and \( I \) be an ideal of \( R \) such that \( \langle r \rangle \nsubseteq I \). Since \( R \) is a PID, \( I = \langle s \rangle \) for some \( s \in R \). We will show that \( s \) is a unit in \( R \); and hence, by E8, \( \langle s \rangle = R \), i.e., \( I = R \).
Now, \( \langle r \rangle \nsubseteq \langle s \rangle \Rightarrow r = st \) for some \( t \in R \). Since \( r \) is irreducible, either \( s \) is an associate of \( r \) or \( s \) is a unit in \( R \). If \( s \) is an associate of \( r \), then \( \langle s \rangle = \langle r \rangle \), a contradiction. Therefore, \( s \) must be a unit in \( R \). Therefore, \( I = R \).
Thus, \( \langle r \rangle \) is a maximal ideal of \( R \).

What Theorem 7 says is that the non-zero prime ideals and maximal ideals coincide in a PID.

Try the following exercise now.

---

**E27** Which of the following ideals are maximal? Give reasons for your choice.

i) \( \langle 5 \rangle \) in \( \mathbb{Z} \),

ii) \( \langle x^2 - 1 \rangle \) in \( \mathbb{Q}[x] \),

iii) \( \langle x^2 + x + 1 \rangle \) in \( \mathbb{R}[x] \),

iv) \( \langle x \rangle \) in \( \mathbb{Z}[x] \).

---

Now, why do you think we have said that Theorem 6 is true for a PID only? You will get an answer to this question in Sec.9.6. Just now we will look at some applications of Theorem 6. This theorem allows us to give a lot of examples of prime elements of \( \mathbb{R}[x] \). For example, any linear polynomial over \( \mathbb{R} \) is irreducible, and hence prime. What about elements of \( \mathbb{Q}[x] \)? In the next section, we will particularly consider irreducibility, and hence primeness, over \( \mathbb{Q}[x] \).

**9.5 IRREDUCIBILITY IN \( \mathbb{Q}[X] \)**

In the previous section, we introduced you to irreducible polynomials in \( F[x] \), where \( F \) is a field. We also stated the Fundamental Theorem of Algebra,
which said that a polynomial over \( \mathbb{C} \) is irreducible iff it is linear. You also learnt that if a polynomial over \( \mathbb{R} \) is irreducible, it must have degree 1 or degree 2. Thus, any polynomial over \( \mathbb{R} \) of degree more than 2 is reducible. And, using the quadratic formula, we know which quadratic polynomials over \( \mathbb{R} \) are irreducible.

Now let us look at polynomials over \( \mathbb{Q} \). Again, as for any field, a linear polynomial over \( \mathbb{Q} \) is irreducible (since it is of least positive degree). Also, by using the quadratic formula we can explicitly obtain the roots of any quadratic polynomial over \( \mathbb{Q} \), and hence figure out whether it is irreducible or not. But, can you tell whether \( x^4 - 4 \) is irreducible over \( \mathbb{Q} \) or not? Though it has no roots in \( \mathbb{Q} \), it is reducible since \( x^4 - 4 = (x^2 - 2)(x^2 + 2) \), with both factors in \( \mathbb{Q}[x] \). Similarly, how would you decide if \( 2x^2 + 3x^2 + 6 \) is irreducible or not over \( \mathbb{Q} \)? In two seconds we can tell you that it is irreducible, by using the **Eisenstein criterion**. This criterion was discovered by the nineteenth century mathematician Ferdinand Gotthold Max Eisenstein. In this section, we will build up the theory for proving this useful criterion.

Let us start with some definitions.

**Definition:** Let \( R \) be a PID and \( f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x] \). The content of \( f[x] \) is defined to be the g.c.d of \( a_0, a_1, \ldots, a_n \).

Further, \( f(x) \) is called a **primitive polynomial** if the content of \( f(x) \) is 1.

For example, the content of \( 3x^2 + 6x + 12 \) in \( \mathbb{Z}[x] \) is the g.c.d of 3, 6 and 12, i.e., 3. Thus, this polynomial is not primitive. But \( 7x^5 + 3x^2 + 4x - 5 \) is primitive, since the g.c.d of \( 7, 0, 0, 3, 4, -5 \) is 1.

We will now prove that the product of primitive polynomials is a primitive polynomial.

**Theorem 8 (Gauss’s Lemma):** Let \( f(x) \) and \( g(x) \) be primitive polynomials in \( \mathbb{Z}[x] \). Then \( f(x)g(x) \) is also a primitive polynomial.

**Proof:** Let \( f(x) = a_0 + a_1x + \cdots + a_nx^n \) and \( g(x) = b_0 + b_1x + \cdots + b_mx^m \) be in \( \mathbb{Z}[x] \), where the g.c.d of \( a_0, a_1, \ldots, a_n \) is 1 and the g.c.d of \( b_0, b_1, \ldots, b_m \) is 1. Now \( f(x)g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n} \), where

\[
c_k = a_0b_k + a_1b_{k-1} + \cdots + a_nb_0.
\]

We shall prove the result by contradiction. So, suppose that \( f(x)g(x) \) is not primitive. Then the g.c.d of \( c_0, c_1, \ldots, c_{m+n} \) is greater than 1, and hence some prime \( p \) must divide it. Thus, \( p | c_i \forall i = 0, 1, \ldots, m+n \).

Since \( f(x) \) is primitive, \( p \) does not divide some \( a_i \). Let \( r \) be the least integer such that \( p \nmid a_r \). Similarly, let \( s \) be the least integer such that \( p \nmid b_s \).

Now consider

\[
c_{rs} = a_rb_{rs} + a_{r-1}b_{rs-1} + \cdots + a_1b_{rs-1} + a_0b_{rs}.
\]

Gauss’s Lemma remains valid if \( \mathbb{Z} \) is replaced by any PID.
By our choice of \( r \) and \( s \), \( p | a_0, p | a_1, \ldots, p | a_{r-1} \) and \( p | b_0, p | b_1, \ldots, p | b_{s-1} \).

Also \( p | c_{r,s} \).

Therefore, \( p \mid [c_{r,s} - (a_0b_{r,s} + \cdots + a_{r-1}b_{s-1} + a_{r-1}b_1 + \cdots + a_s b_0)] \),

i.e., \( p | a_i \) or \( p | b_s \), since \( p \) is a prime.

But the way we have defined \( a_i \) and \( b_s \), \( p \mid a_i \) and \( p \mid b_s \).

So we reach a contradiction. Therefore, our assumption is false. That is, our theorem is true.

You may like to try the following exercises now.

---

**E28)** What are the contents of the following polynomials over \( \mathbb{Z} \)?

i) \( 1 + x + x^2 + x^3 + x^4 \), \( 7x^4 - 7 \), \( 5(2x^2 -1)(x + 2) \).

**E29)** Prove that any polynomial \( f(x) \in \mathbb{Z}[x] \) can be written as \( \alpha g(x) \), where \( \alpha \) is the content of \( f(x) \) and \( g(x) \) is a primitive polynomial.

**E30)** Prove that the content of \( f(x)g(x) \) is the product of the content of \( f(x) \) and the content of \( g(x) \), where \( f(x), g(x) \in \mathbb{Z}[x] \).

---

We now use Gauss’s Lemma to begin our discussion on irreducibility in \( \mathbb{Q}[x] \).

Consider any polynomial over \( \mathbb{Q} \), say \( f(x) = \frac{3}{2}x^3 + \frac{1}{3}x^2 + 3x + \frac{1}{3} \).

Thus, we can multiply any \( f(x) \in \mathbb{Q}[x] \) by a suitable integer \( m \) so that \( mf(x) \in \mathbb{Z}[x] \).

Theorem 9: If \( f(x) \in \mathbb{Z}[x] \) is irreducible in \( \mathbb{Z}[x] \), then it is irreducible in \( \mathbb{Q}[x] \).

**Proof:** Let us suppose that \( f(x) \) is not irreducible over \( \mathbb{Q}[x] \). Then we should reach a contradiction. So let \( f(x) = g(x)h(x) \) in \( \mathbb{Q}[x] \), where neither \( g(x) \) nor \( h(x) \) is a unit, i.e., \( \deg g(x) > 0 \), \( \deg h(x) > 0 \).

Since \( g(x) \in \mathbb{Q}[x], \exists m \in \mathbb{Z} \) such that \( mg(x) \in \mathbb{Z}[x] \). Similarly, \( \exists n \in \mathbb{Z} \) such that \( nh(x) \in \mathbb{Z}[x] \). Then,

\[
\text{m}f(x) = (mg(x))(nh(x)) \quad \text{...(5)}
\]

Now, by E30, \( f(x) = rf_i(x), mg(x) = sg_i(x), nh(x) = th_i(x) \), where \( r, s \) and \( t \) are the contents of \( f(x), mg(x) \) and \( nh(x) \), and \( f_i(x), g_i(x), h_i(x) \) are primitive polynomials of positive degree.

Thus, (5) gives us

\[
\text{m}f_i(x) = stg_i(x)h_i(x). \quad \text{...(6)}
\]

Since \( g_i(x) \) and \( h_i(x) \) are primitive, Gauss’s Lemma says that \( g_i(x)h_i(x) \) is primitive. Thus, the content of the right hand side polynomial in (6) is \( st \). But
the content of the left hand side polynomial in (6) is $mnr$. Thus, (6) says that $mnr = st$.

Hence, (6) gives us $f_1(x) = g_1(x)h_1(x)$.

Therefore, $f(x) = r_1f_1(x) = (rg_1(x))h_1(x)$ is in $\mathbb{Z}[x]$, where neither $rg_1(x)$ nor $h_1(x)$ is a unit. This contradicts the fact that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Thus, our supposition is false. Hence, $f(x)$ must be irreducible in $\mathbb{Q}[x]$. ■

Regarding Theorem 9, consider the following remark.

**Remark 2:** Is the converse of Theorem 9 true? That is, if $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}[x]$, will it be irreducible over $\mathbb{Z}[x]$? The answer is ‘no’.

For example, consider $2x$. This is irreducible in $\mathbb{Q}[x]$, since $2$ is a unit in $\mathbb{Q}$. However, $2x$ is not irreducible in $\mathbb{Z}[x]$, since $2$ is not a unit in $\mathbb{Z}$. However, if $f \in \mathbb{Z}[x]$ is monic and irreducible in $\mathbb{Q}[x]$, then it is irreducible over $\mathbb{Z}[x]$, which can be proved using E30.

Let us now look at Theorem 9 again. It says that to check the irreducibility of a polynomial in $\mathbb{Q}[x]$, it is enough to check the irreducibility of polynomials in $\mathbb{Z}[x]$. And, for checking the irreducibility of some polynomials in $\mathbb{Z}[x]$, we have Eisenstein’s criterion, that we mentioned at the beginning of this section.

**Theorem 10 (Eisenstein’s Criterion):** Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $n \geq 1$. Suppose that for some prime number $p$,

i) $p \nmid a_n$,

ii) $p \mid a_0$, $p \mid a_1$, ..., $p \mid a_{n-1}$, and

iii) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$).

**Proof:** Can you guess our method of proof? By contradiction, once again! Suppose $f(x)$ is reducible in $\mathbb{Z}[x]$.

Let $f(x) = g(x)h(x)$,

where $g(x) = b_0 + b_1 + \cdots + b_mx^m$, $m > 0$ and $h(x) = c_0 + c_1x + \cdots + c_rx^r$, $r > 0$.

Then $n = \deg f = \deg g + \deg h = m + r$, and

$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0 \quad \forall \ k = 0, 1, ..., n$.

Now $a_0 = b_0c_0$. We know that $p \mid a_0$. Thus, $p \mid b_0c_0$. \(\vdots\) $p \mid b_0$ or $p \mid c_0$.

Since $p^2 \nmid a_0$, $p$ cannot divide both $b_0$ and $c_0$. Let us suppose that $p \mid b_0$ and $p \nmid c_0$.

Now let us look at $a_n = b_m c_r$. Since $p \nmid a_n$, we see that $p \nmid b_m$ and $p \nmid c_r$.

Thus, we see that for some $i$, $p \nmid b_i$. Let $k$ be the least integer such that $p \nmid b_k$. Note that $0 < k \leq m < n$, so that $p \mid a_k$.

Now, $a_k = (b_0c_k + \cdots + b_{k-1}c_i) + b_kc_0$.

Since $p \mid a_k$ and $p \mid b_0$, $p \mid b_1$, ..., $p \mid b_{k-1}$, we see that
\[ p | [a_k - (b_0c_k + \cdots + b_{k-1}c_0)], \text{ i.e., } p | b_k \text{ and } p | c_0. \] So we reach a contradiction. (By a similar argument, you would reach a contradiction if you had assumed \( p | b_0 \) and \( p | c_0 \) earlier.)

Thus, \( f(x) \) must be irreducible in \( \mathbb{Z}[x] \).

Let us illustrate the use of this criterion.

**Example 9:** Is \( 2x^7 + 3x^5 - 6x + 3x^3 + 12 \) irreducible in \( \mathbb{Q}[x] \)? Why, or why not?

**Solution:** By looking at the coefficients we see that the prime number 3 satisfies the conditions given in Eisenstein’s criterion. That is, 3 divides each of 12, 0, 0, 3, -6, 3; \( 3^3 \) \( 12; 3 \) 2. Therefore, the given polynomial is irreducible in \( \mathbb{Q}[x] \).

***

**Example 10:** Let \( p \) be a prime number. Is \( \mathbb{Q}[x]/<x^3 - p> \) a field? Why, or why not?

**Solution:** Since \( \mathbb{Q}[x] \) is a PID, you know that if \( f(x) \) is irreducible in \( \mathbb{Q}[x] \), then \(<f(x)>\) is a maximal ideal of \( \mathbb{Q}[x] \).

Now, by Eisenstein’s criterion, \( x^3 - p \) is irreducible since \( p \) satisfies the required conditions. Therefore, \(<x^3 - p>\) is a maximal ideal of \( \mathbb{Q}[x] \).

Thus, from Theorem 1 and Theorem 7, we conclude that \( \mathbb{Q}[x]/<x^3 - p> \) is a field.

***

In this example we have brought out an important fact which we ask you to prove in the following exercise.

E31) For any \( n \in \mathbb{N} \) and prime number \( p \), show that \( x^n - p \) is irreducible over \( \mathbb{Q}[x] \). Note that this shows us that we can obtain irreducible polynomials of any degree over \( \mathbb{Q}[x] \).

Now let us look at another example of an irreducible polynomial. While solving this we will show you how Eisenstein’s criterion can be used indirectly.

**Example 11:** Let \( p \) be a prime number. Show that \( \phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \) is irreducible in \( \mathbb{Z}[x] \). (\( \phi_p(x) \) is called the pth cyclotomic polynomial.)

**Solution:** To start with, note that \( f(x) = g(x)h(x) \) in \( \mathbb{Z}[x] \) iff \( f(x+1) = g(x+1)h(x+1) \) in \( \mathbb{Z}[x] \). Thus, \( f(x) \) is irreducible in \( \mathbb{Z}[x] \) iff \( f(x+1) \) is irreducible in \( \mathbb{Z}[x] \).

Now, \( \phi_p(x) = \frac{x^p - 1}{x - 1} \).
Take \( f(x) = \phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} \)

\[
= \frac{1}{x}(x^p + px^{p-1}C_1x^{p-2} + \cdots + px + 1 - 1), \text{ by the binomial theorem}
\]

\[
= x^{p-1} + px^{p-2} + px^{p-3} + \cdots + px + p.
\]

Now apply Eisenstein’s criterion to \( f(x) \) taking \( p \) as the prime. Since \( p \mid C_r \)
for \( r = 1, \ldots, p-1 \), we find that \( f(x) \) is irreducible. Therefore, \( \phi_p(x+1) \) is irreducible.

Now, if \( \phi_p(x) = g(x)h(x) \), with \( \deg g > 0, \deg h > 0 \), then

\( f(x) = \phi_p(x+1) = g(x+1)h(x+1) \) would be reducible, which is a contradiction. Hence \( \phi_p(x) \) is irreducible in \( \mathbb{Z}[x] \), and in \( \mathbb{Q}[x] \).

***

Before going further, here is an important comment.

**Remark 3:** Note that Eisenstein’s criterion is sufficient, but not necessary, for
irreducibility over \( \mathbb{Z}[x] \). Thus, if a polynomial in \( \mathbb{Z}[x] \) does not satisfy the
criterion, it can still be irreducible. For instance, \( x^2 + 4 \) is irreducible over
\( \mathbb{Z}[x] \), but there is no \( p \in \mathbb{Z} \) for which this polynomial satisfies Eisenstein’s
criterion.

You can try these exercises now.

---

**E32)** Which of the following elements of \( \mathbb{Z}[x] \) are irreducible in \( \mathbb{Q}[x] \), and
why?

i) \( x^2 - 12 \), ii) \( 8x^3 + 6x^2 - 9x + 24 \), iii) \( 5x + 1 \).

**E33)** Let \( p \) be a prime integer. Let \( a \) be a non-zero non-unit square-free
integer, i.e., \( b^2 \not\mid a \) for any \( b \in \mathbb{Z} \). Show that \( \mathbb{Z}[x]/<x^p + a> \) is an
integral domain.

**E34)** Show that \( x^p + \bar{a} \in \mathbb{Z}_p[x] \) is not irreducible for any \( \bar{a} \in \mathbb{Z}_p \).

---

So far we have used the fact that if \( f(x) \in \mathbb{Z}[x] \) is irreducible over \( \mathbb{Z} \), then it is
also irreducible over \( \mathbb{Q} \). Do you think we can have a similar relationship
between irreducibility in \( \mathbb{Q}[x] \) and \( \mathbb{R}[x] \)? To answer this, consider

\( f(x) = x^2 - 2 \). This is irreducible in \( \mathbb{Q}[x] \), but \( f(x) = (x - \sqrt{2})(x + \sqrt{2}) \) in
\( \mathbb{R}[x] \). Thus, we cannot extend irreducibility over \( \mathbb{Q} \) to irreducibility over \( \mathbb{R} \).

However, there is another property that \( \mathbb{Q}[x] \) and \( \mathbb{R}[x] \) have in common with
\( \mathbb{Z} \), which we discuss in the next section.
9.6 UNIQUE FACTORISATION DOMAINS (UFD)

Recall, from your earlier study of mathematics, that every element of \( \mathbb{Z} \), other than 0, 1 and \(-1\), can be uniquely written as a product of primes in \( \mathbb{Z} \), i.e., a product of irreducible elements in \( \mathbb{Z} \). In this section, we shall look at a class of domains that satisfies a generalised form of this property. Let us begin with defining such a domain.

**Definition:** An integral domain \( R \) is called a **unique factorisation domain** (UFD, in short) if every non-zero element of \( R \), which is not a unit in \( R \), can be uniquely expressed (up to units) as a product of a finite number of irreducible elements of \( R \).

Thus, if \( R \) is a UFD and \( a \in R \), with \( a \neq 0 \) and \( a \) being non-invertible, then

i) \( a \) can be written as a product of a finite number of irreducible elements, and

ii) if \( a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m \) be two factorisations into irreducibles, then \( n = m \) and each \( p_i \) is an associate of some \( q_j \), where \( 1 \leq i \leq n, 1 \leq j \leq m \).

Can you think of an example of a UFD? As noted above, \( \mathbb{Z} \) is a UFD. Consider another example.

**Example 12:** Show that a field is a UFD.

**Solution:** Let \( F \) be a field and \( a \in F, a \neq 0 \). Then \( a \) is invertible. So there is no non-zero non-unit in \( F \). Hence, \( F \) is trivially a UFD.

***

To get many other examples, let us go back to PIDs for a bit. You will see that every PID is a UFD. For this, we will first show a very interesting property of the ideals of a PID. This property, called the **ascending chain condition**, says that any increasing chain of ideals in a PID must stop after a finite number of steps.

**Theorem 11:** Let \( R \) be a PID and \( I_1, I_2, \ldots \) be an infinite sequence of ideals of \( R \) satisfying \( I_1 \subseteq I_2 \subseteq \cdots \). Then \( \exists m \in \mathbb{N} \) such that \( I_m = I_{m+1} = I_{m+2} = \cdots \).

**Proof:** Consider the set \( I = I_1 \cup I_2 \cup \ldots = \bigcup_{n=1}^{\infty} I_n \). We will prove that \( I \) is an ideal of \( R \).

Firstly, \( I \neq \emptyset \) since \( I_1 \neq \emptyset \) and \( I_1 \subseteq I \).

Secondly, if \( a, b \in I \), then \( a \in I_r \) and \( b \in I_s \) for some \( r, s \in \mathbb{N} \).

Assume \( r \geq s \). Then \( I_r \subseteq I_s \). Therefore, \( a, b \in I_s \). Since \( I_s \) is an ideal of \( R \), \( a - b \in I_s \subseteq I \). Thus, \( a - b \in I \) for some \( r \in \mathbb{N} \).

Finally, let \( x \in R \) and \( a \in I \). Then \( a \in I_r \) for some \( r \in \mathbb{N} \).
\[ xa \in I_r \subseteq I \] Thus, whenever \( x \in R \) and \( a \in I \), \( xa \in I \).

Thus, \( I \) is an ideal of \( R \).
Next, since $R$ is a PID, $I = <a>$ for some $a \in R$. Since $a \in I$, $a \in I_m$ for some $m \in \mathbb{N}$. Then $I \subseteq I_m$. But $I_m \subseteq I$. So we see that $I = I_m$.

Now, $I_m \subseteq I_{m+1} \subseteq I = I_n$. Therefore, $I_m = I_{m+1}$. Similarly, $I_m = I_{m+2}$, and so on. Thus, $I_m = I_{m+1} = I_{m+2} = \cdots$.

Now, let us consider another property of PIDs. Take any integer $n$. Then we know that $n = 0$, or $n = \pm 1$, or $n$ has a prime factor. This property of integers is true for the elements of any PID, as you will see now.

**Theorem 12:** Let $R$ be a PID and $a$ be a non-zero non-invertible element of $R$. Then there is some prime element $p$ in $R$ such that $p|a$.

**Proof:** If $a$ is prime, take $p = a$. If $a$ is not a prime, we can write $a = a_1b_1$, where neither $a_1$ nor $b_1$ is an associate of $a$. Then $<a > \nsubseteq <a_1 >$. If $a_1$ is prime, take $p = a_1$. Otherwise, we can write $a_1 = a_2b_2$, where neither $a_2$ nor $b_2$ is an associate of $a_1$. Then $<a_1 > \nsubseteq <a_2 >$. Continuing in this way we get an increasing chain of ideals $<a > \nsubseteq <a_1 > \nsubseteq <a_2 > \nsubseteq \cdots$.

By Theorem 11, this chain stops with some $<a_n >$. This will happen only when $a_n$ won’t have any non-trivial factors. Thus, $a_n$ will be prime. Take $p = a_n$, and the theorem is proved.

And now we are in a position to prove that any non-zero non-invertible element of a PID can be written as a finite product of prime elements, which is the same as irreducible elements in a PID.

**Theorem 13:** Let $R$ be a PID. Let $a \in R$ such that $a \neq 0$ and $a$ is not a unit. Then $a = p_1p_2 \cdots p_m$, where $p_1$, $p_2$, ..., $p_m$ are prime elements of $R$.

**Proof:** If $a$ is a prime element, there is nothing to prove. If not, then $p|a$ for some prime $p$ in $R$, by Theorem 12. Let $a = p_1a_1$. If $a_1$ is a prime, we are through. Otherwise $p|a_1$ for some prime $p_2$ in $R$. Let $a_1 = p_2a_2$. Then $a = p_1p_2a_2$. If $a_2$ is a prime, we are through. Otherwise we continue the process. Note that since $a_1$ is a non-trivial factor of $a$, $<a>_R \nsubseteq <a_1 >$. Similarly, $<a_1 > \nsubseteq <a_2 >$. So, as the process continues we get an increasing chain of ideals $<a>_R \nsubseteq <a_1 > \nsubseteq <a_2 > \nsubseteq \cdots$ in the PID $R$.

Just as in the proof of Theorem 12, this chain ends at $<a_m >$ for some $m \in \mathbb{N}$, and $a_m$ is irreducible.

Hence, the process stops after $m$ steps, i.e., we can write $a = p_1p_2 \cdots p_m$, where $p_i$ is a prime element of $R \forall i = 1, \ldots, m$.

So, you have seen why, and how, any non-zero non-invertible element in a PID can be factorised into a product of primes. What is interesting about this factorisation is that it is unique, which we shall prove next. But before going into the proof of this result, we ask you to prove a property of prime elements that you will need in the proof.
Special Integral Domains

E35) Use induction on $n$ to prove that if $p$ is a prime element in an integral domain $R$ and if \( p \mid a_1a_2\ldots a_n \) (where $a_1, a_2, \ldots, a_n \in R$), then $p \mid a_i$ for some $i = 1, 2, \ldots, n$.

Now, assuming the result in E35, let us state the result we have been aiming for.

**Theorem 14:** Every PID is a UFD, that is, if $R$ is a PID, $a \neq 0$ is non-invertible in $R$ and $a = p_1p_2\ldots p_n = q_1q_2\ldots q_m$, where $p_i$ and $q_j$ are irreducible elements of $R$, then $n = m$ and each $p_i$ is an associate of some $q_j$ for $1 \leq i \leq n, 1 \leq j \leq m$.

**Proof:** Since $p_1p_2\ldots p_n = q_1q_2\ldots q_m$, $p_1 \mid q_j$ for some $j = 1, \ldots, m$. By changing the order of the $q_j$, if necessary, we can assume that $j = 1$, i.e., $p_1 \mid q_1$. Let $q_1 = p_1u_1$. Since $q_1$ is irreducible, $u_1$ must be a unit in $R$. So $p_1$ and $q_1$ are associates. Now we have $p_1p_2\ldots p_n = (p_1u_1)q_2\ldots q_m$.

Cancelling $p_1$ from both sides, we get $p_2p_3\ldots p_n = u_1q_2\ldots q_m$.

Now, suppose $m > n$. Then we can apply the same process to $p_2, p_3$, and so on, to get each $p_j$ as an associate of some $q_j$, and $1 = u_1u_2\ldots u_nq_{n+1}\ldots q_m$.

This shows that $q_{n+1}$ is a unit, which contradicts the fact that $q_{n+1}$ is irreducible.

Thus, $m \leq n$.

Interchanging the roles of the $p_i$s and $q_j$s, and by using a similar argument, we get $n \leq m$.

Thus, $n = m$.

In this process, you have also seen that each $p_i$ is an associate of some $q_j$, and vice versa.

Using Theorem 14, we know, for example, that $x^2 - 1 \in \mathbb{R}[x]$ can be written as $(x - 1)(x + 1)$, or $(x + 1)(x - 1)$, or $\left[ \frac{1}{2}(x + 1) \right][2(x - 1)]$ in $\mathbb{R}[x]$, i.e., the only factorisation possible for $x^2 - 1$ is $(x - 1)(x + 1)$, up to units and order.

Now try the following exercises.

E36) Give the prime factorisation of $3x^5 - 2x^2 + 4x - 6$ in $\mathbb{Q}[x]$ and in $\mathbb{Z}_2[x]$.

E37) Directly prove that $F[x]$ is a UFD, for any field $F$.  

Every Euclidean domain is a UFD.
Ring Theory

(Hint: Suppose you want to factorise $f(x)$. Then use induction on $\deg f(x)$.)

So far you have seen several examples of UFDs. Now consider an example of a domain which is not a UFD (and hence, neither a PID nor a Euclidean domain).

Example 13: Show that $\mathbb{Z}[^{\sqrt{-5}}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is not a UFD.

Solution: Let us define a function

$$N : \mathbb{Z}[^{\sqrt{-5}}] \rightarrow \mathbb{N} \cup \{0\} : N(a + b\sqrt{-5}) = a^2 + 5b^2.$$  

This function is called the norm function. You can check that $N(\alpha \beta) = N(\alpha)N(\beta) \quad \forall \alpha, \beta \in \mathbb{Z}[^{\sqrt{-5}}].$

Now, 9 has two factorisations in $\mathbb{Z}[^{\sqrt{-5}}]$, namely, $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$

From Example 5, you also know that the only units of $\mathbb{Z}[^{\sqrt{-5}}]$ are 1 and $-1$. Thus, no two of $3, 2 + \sqrt{-5},$ and $2 - \sqrt{-5}$ are associates of each other.

We now show that each of them is irreducible. Suppose not, that is, suppose any one of them, say $2 + \sqrt{-5}$, is reducible.

Then $2 + \sqrt{-5} = \alpha \beta$ for some non-invertible $\alpha, \beta \in \mathbb{Z}[^{\sqrt{-5}}].$

Applying the function $N$, we see that $N(2 + \sqrt{-5}) = N(\alpha)N(\beta)$, i.e., $9 = N(\alpha)N(\beta)$.

Since $N(\alpha), N(\beta) \in \mathbb{N}$, and $\alpha, \beta$ are not units, the only possibilities are $N(\alpha) = 3 = N(\beta)$.

So, if $\alpha = a + b\sqrt{-5}$, then $a^2 + 5b^2 = 3$.

But, if $b \neq 0$, then $a^2 + 5b^2 \geq 5$; and if $b = 0$, then $a^2 = 3$. Neither of these situations are possible in $\mathbb{Z}$. So we reach a contradiction. Therefore, our assumption that $2 + \sqrt{-5}$ is reducible is wrong. That is, $2 + \sqrt{-5}$ is irreducible.

Similarly, you can show that $3$ and $2 - \sqrt{-5}$ are irreducible. Thus, the factorisation of 9 as a product of irreducible elements is not unique. Therefore, $\mathbb{Z}[^{\sqrt{-5}}]$ is not a UFD.

***

From this example you can also see that an irreducible element need not be a prime element. For example, $2 + \sqrt{-5}$ is irreducible and $(2 + \sqrt{-5}) \mid 3, 3$, but $(2 + \sqrt{-5}) \nmid 3$. Thus, $2 + \sqrt{-5}$ is not a prime element.

Now for an exercise.

E38) Give two different factorisations of 6 as a product of irreducible elements in $\mathbb{Z}[^{\sqrt{-5}}]$.

E39) Show that $\mathbb{Z}[^{\sqrt{-3}}]$ is not a UFD.
Now let us discuss some properties of a UFD. The first property says that any two elements of a UFD have a g.c.d. and their g.c.d is the product of all their common factors. Here we will use the fact that any element a in a UFD R can be written as $a = p_1^{r_1}p_2^{r_2}...p_n^{r_n}$, where the $p_i$s are distinct irreducible elements of R and $r_i \in \mathbb{N}$ $\forall$ $i = 1, ..., n$. For example, in $\mathbb{Z}[x]$ we have $x^3 - x^2 - x + 1 = (x - 1)(x + 1)(x - l) = (x - l)^2(x + 1)$.

So, let us prove the following result, which generalises the process you used in Example 6 and E11.

**Theorem 15:** Any two elements of a UFD have a g.c.d.

**Proof:** Let $R$ be a UFD and $a, b \in R$.
Let $a = p_1^{r_1}p_2^{r_2}...p_n^{r_n}$ and $b = p_1^{s_1}p_2^{s_2}...p_n^{s_n}$, where $p_i, p_2, ..., p_n$ are distinct irreducible elements of $R$, and $r_i$ and $s_i$ are non-negative integers $\forall$ $i = 1, 2, ..., n$. (If some $p_i$ does not occur in the factorisation of $a$, then the corresponding $r_i = 0$. Similarly, if some $p_i$ is not a factor of $b$, then the corresponding $s_i = 0$.

For example, take 20 and 15 in $\mathbb{Z}$. Then $20 = 2^2 \times 3^0 \times 5^1$ and $15 = 2^0 \times 3^1 \times 5^1$.

Now, let $t_i = \min (r_i, s_i)$ $\forall$ $i = 1, 2, ..., n$.
Then $d = p_1^{t_1}p_2^{t_2}...p_n^{t_n}$ divides $a$ as well as $b$, since $t_i \leq r_i$ and $t_i \leq s_i$ $\forall$ $i = 1, 2, ..., n$.

Now, let $c \mid a$ and $c \mid b$. Then every irreducible factor of $c$ must be an irreducible factor of $a$ and of $b$, because of the unique factorisation property.

Thus, $c = p_1^{m_1}p_2^{m_2}...p_n^{m_n}$, where $m_i \leq r_i$ and $m_i \leq s_i$ $\forall$ $i = 1, 2, ..., n$. Thus, $m_i \leq t_i$ $\forall$ $i = 1, 2, ..., n$.

Therefore, $c \mid d$.

Hence, $d = (a, b)$.

Now, let us go back to Example 13 for a moment. Over there we found a non-UFD in which an irreducible element need not be a prime element. The following result says that this difference between irreducible and prime elements can only occur in a domain that is not a UFD.

**Theorem 16:** Let $R$ be a UFD. An element of $R$ is prime iff it is irreducible.

**Proof:** By E26, you know that every prime in $R$ is irreducible. So let us prove the converse.
Let $a \in R$ be irreducible and let $a \mid bc$, where $b, c \in R$.
Let $bc = ad$, where $d \in R$.

Consider $(a, b)$. Since $a$ is irreducible, $(a, b) = 1$ or $(a, b) = a$.

If $(a, b) = a$, then $a \mid b$.

If $(a, b) = 1$, then $a \not\mid b$. Let $b = p_1^{q_1}p_2^{q_2}...p_m^{q_m}$ and $c = q_1^{r_1}q_2^{r_2}...q_n^{r_n}$, be irreducible factorisations of $b$ and $c$.
Since $bc = ad$ and $a$ is irreducible, $a$ must be one of the $p_i$s or one of the $q_j$s. Since $a \not\mid b$, $a \neq p_i$ for any $i$. Therefore, $a = q_j$ for some $j$. That is, $a \mid c$. 

\[55\]
Thus, if \((a, b) = 1\), then \(a \mid c\).

So, we have shown that \(a \mid bc \Rightarrow a \mid b\) or \(a \mid c\).

Hence, \(a\) is prime.

For the final property of UFDs that we are going to state, recall that \(\mathbb{Z}\) is a PID but \(\mathbb{Z}[x]\) is not a PID. You may ask what happens to \(R[x]\) if \(R\) is a UFD. We state the following result.

**Theorem 17:** Let \(R\) be a UFD. Then \(R[x]\) is a UFD.

We will not prove this result here, even though it is very useful for mathematicians. But let us apply it. You can use it to solve the following exercises.

---

E40) Give an example, with justification, of a UFD which is not a PID.

E41) Which of the following statements are true? Give reasons for your answers.
   
i) If \(x\) is an irreducible element of a UFD \(R\), then \(\overline{x}\) is irreducible in every quotient ring of \(R\).
   
ii) Any quotient ring of a UFD retains the property of unique factorisation.
   
iii) A subring of a UFD is a UFD.
   
iv) If \(R\) is a ring such that \(R[x]\) is a UFD, then \(R\) is a UFD.

---

Let us wind up this unit now, with a brief description of what we have covered in it.

**9.7 SUMMARY**

In this unit, we have discussed the following points.

1) A recall of the definition, and some properties, of an integral domain.

2) A recall of the definition, and some properties, of a prime ideal and a maximal ideal of a ring.

3) The definition, and examples, of a Euclidean domain.

4) The definitions, and examples, of units, associates, factors, the g.c.d of \(n\) elements, prime elements and irreducible elements in an integral domain.

5) The definition, and examples, of a principal ideal domain (PID).

6) Every Euclidean domain is a PID, but the converse is not true. Thus, \(\mathbb{Z}, F\) and \(F[x]\) are PIDs, for any field \(F\).

7) The g.c.d of any two elements \(a\) and \(b\) in a PID \(R\) exists, and is of the form \(ax + by\) for some \(x, y \in R\).
8) The Fundamental Theorem of Algebra: Any non-constant polynomial over \( \mathbb{C} \) has all its roots in \( \mathbb{C} \).

9) In a PID, every prime ideal is a maximal ideal.

10) Eisenstein’s criterion for irreducibility in \( \mathbb{Q}[x] \).

11) The definition, and examples, of a unique factorisation domain (UFD).

12) Every PID is a UFD, but the converse is not true. Thus, \( \mathbb{Z}, \mathbb{F}, \text{and } \mathbb{F}[x] \) are UFDs, for any field \( \mathbb{F} \).

13) In a UFD (and hence, in a PID) an element is prime iff it is irreducible.

14) Any two elements in a UFD have a g.c.d.

15) If \( R \) is a UFD, then so is \( R[x] \). However, this statement is not true if ‘UFD’ is replaced by ‘Euclidean domain’ or ‘PID’.

9.8 SOLUTIONS / ANSWERS

E1) Let \( n = mr \), where \( r \in \mathbb{N} \).
Then \( \bar{m}\bar{r} = \bar{n} = \overline{0} \) in \( \mathbb{Z}_n \).
Since \( 1 < m < n \), \( \bar{m} \neq \overline{0} \). Similarly, \( \bar{r} \neq \overline{0} \).
Thus \( \bar{m} \in \mathbb{Z}_n \) is a zero divisor.

The converse is not true. For example, \( \overline{4} \) is a zero divisor in \( \mathbb{Z}_6 \), but \( 4 \not| \overline{6} \).

E2) You know that \( \mathbb{Z}_p \) is a non-zero commutative ring with identity.
Now, suppose \( \bar{a}, \bar{b} \in \mathbb{Z}_p \) satisfy \( \bar{a}\bar{b} = \overline{0} \). Then \( ab = 0 \), i.e., \( p|ab \).
Since \( p \) is a prime number, \( p|a \) or \( p|b \). Thus, \( \overline{a} = \overline{0} \) or \( \overline{b} = \overline{0} \).
Thus, \( \mathbb{Z}_p \) is without zero divisors, and hence, is a domain.

E3) Each non-empty proper subset \( A \) of \( X \) is a zero divisor because \( \phi(A) = A \cap (X \setminus A) = \emptyset \), the zero element of \( \phi(X) \). Hence \( \phi(X) \) is not a domain.

E4) \( \mathbb{Z}_4 \), since \( \overline{2} \) is a zero divisor; and \( \mathbb{R} \times \mathbb{R} \), since \( (1, 0) \) is a zero divisor.
\( \mathbb{Z}_5 \) has no zero divisors, since \( 5 \) is a prime.
\( 2\mathbb{Z} \subseteq \mathbb{Z} \), and \( \mathbb{Z} \) has no zero divisors.

For any non-zero \( a + ib \in \mathbb{Z} + i\mathbb{Z} \),
\( (a + ib)(c + id) = 0 \Rightarrow [(ac - bd) + i(ad + bc)] = 0 \Rightarrow ac - bd = 0 = ad + bc \Rightarrow b(c^2 + d^2) = 0 .
If \( b = 0 \), then \( ac - bd = 0 \) gives \( a = 0 \) or \( c = 0 \). But \( a \neq 0 \) since \( a + ib \neq 0 \). \( \therefore c = 0 \). Then \( ad + bc = 0 \) gives \( d = 0 \), i.e., \( c + id = 0 \).
Again, if \( b \neq 0 \), then \( c^2 + d^2 = 0 \Rightarrow c = 0 = d \). Thus, in either case, 
\((a + ib)\) is not a zero divisor.

E5) \( x^2 = x \Rightarrow x(x - 1) = 0 \Rightarrow x = 0 \) or \( x = 1 \).

E6) False. For example, \( \mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z} \), and \( \mathbb{Z} \times \{0\} \) is a domain, while \( \mathbb{Z} \times \mathbb{Z} \) is not.

E7) i) Let \( \bar{m} \in \mathbb{Z}_6 \) be a unit. Then \( \exists \bar{n} \in \mathbb{Z}_6 \) such that \( \bar{m} \bar{n} = \bar{1} \).
\[ \therefore \exists r \in \mathbb{Z} \text{ s.t. } mn + 6r = 1, \text{ that is, the g.c.d of } m \text{ and } 6 \text{ is } 1. \]
\[ \therefore \bar{m} = \bar{1} \text{ or } \bar{3}. \]

ii) Since \( \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5 \), the argument in (i) above tells us that the units are all the non-zero elements of \( \mathbb{Z}/5\mathbb{Z} \).

iii) Let \( a + ib \in \mathbb{Q} + i\mathbb{Q} \) be a unit. Then both \( a \) and \( b \) can’t be zero, that is, \( a^2 + b^2 \neq 0 \). Also, \( \exists c + id \in \mathbb{Q} + i\mathbb{Q} \) such that \( (a + ib)(c + id) = 1 \). In fact, \( c + id = \frac{(a - ib)}{a^2 + b^2} \). Thus, \( a + ib \) is a unit \( \forall a + ib \in (\mathbb{Q} + i\mathbb{Q}) \setminus \{0\} \).

E8) Let \( u \in \mathbb{R} \) be a unit. Then \( \exists v \in \mathbb{R} \) such that \( vu = 1 \). Thus, for any \( r \in \mathbb{R} \), \( r = r.1 = r(vu) = (rv)u \in Ru \).
Thus, \( \mathbb{R} \subseteq Ru \). Also \( Ru \subseteq \mathbb{R} \). \( \therefore R = Ru \).
Conversely, let \( Ru = R \). Since \( 1 \in R = Ru \), \( \exists v \in R \) such that \( 1 = vu \).
Thus, \( u \) is a unit in \( R \).

E9) i) \( u \) is a unit iff \( uv = 1 \) for some \( v \in \mathbb{R} \) iff \( u \mid 1 \).

ii) \( a \mid b \) and \( b \mid a \)
\[ \Rightarrow b = ac \text{ and } a = bd \text{ for some } c, d \in \mathbb{R}. \]
\[ \Rightarrow b = bdc \]
\[ \Rightarrow b = 0 \text{ or } dc = 1. \]
If \( b = 0 \), then \( a = 0 \), and then \( a \) and \( b \) are associates.
If \( b \neq 0 \), then \( dc = 1 \). Thus, \( c \) is a unit and \( b = ac \).
Therefore, again, \( a \) and \( b \) are associates.
Conversely, let \( a \) and \( b \) be associates in \( \mathbb{R} \), say \( a = bu \), where \( u \) is a unit in \( R \). Then \( b \mid a \). Also, let \( v \in \mathbb{R} \) such that \( uv = 1 \). Then \( av = buv = b \). Thus, \( a \mid b \).

E10) \( U(\mathbb{R}) = \{ x \in \mathbb{R} \mid \exists y \in \mathbb{R} \text{ with } xy = 1 \} \)
\( U(\mathbb{R}) \neq \emptyset \) since \( 1 \in U(\mathbb{R}) \).
Since \( (\mathbb{R}, \cdot) \) is commutative, you should check that
\( xy \in U(\mathbb{R}) \forall x \in U(\mathbb{R}), y \in U(\mathbb{R}). \)
Hence \( (U(\mathbb{R}), \cdot) \) is a semigroup.
Also, \(1 \in U(R)\) is the identity w.r.t. \(\cdot\).

Finally, for \(x \in U(R), \exists y \in U(R)\) s.t. \(xy = 1\), i.e., \(y = x^{-1}\), so that \(x^{-1} \in U(R)\).

Hence \((U(R), \cdot)\) is a group.

Let \(\phi : R \rightarrow R'\) be a ring homomorphism.

Consider \(\psi : U(R) \rightarrow U(R') : \psi(x) = \phi(x)\).

Then \(\psi\) is well-defined since \(\phi\) is well-defined.

Also \(\psi(x, x_2) = \phi(x, x_2) = \phi(x_1)\phi(x_2) = \psi(x_1)\psi(x_2)\).

Hence \(\psi\) is a group homomorphism.

E11) i) \(\overline{2}\) in \(\mathbb{Z}_8\), and \(\overline{1}\) in \(\mathbb{Z}_7\) (both \(\overline{2}\) and \(\overline{6}\) are units in \(\mathbb{Z}_7\)).

ii) \(x^2 + 8x + 15 = (x + 3)(x + 5), x^2 + 12x + 35 = (x + 5)(x + 7)\).

Thus, their g.c.d is \(x + 5\).

iii) \(x^3 - 2x^2 + 6x - 5 = (x - 1)(x^2 - x + 5), 5x^3 + x^2 - 3x - \frac{3}{5} = 5(x + 1)\left(x^2 - \frac{3}{5}\right), x^2 - 2x + 1 = (x - 1)^2\).

Thus, their g.c.d is \(1\).

E12) Firstly, \(I\) is an ideal of \(C[0, 1]\) (because \(f, g \in I \Rightarrow f - g \in I\), and for \(h \in C[0, 1], f \in I, hf \in I\).)

Secondly, since any non-zero constant function over \([0, 1]\) is in \(C[0, 1] \setminus I\), \(I\) is a proper ideal.

Finally, let \(fg \in I\). Then \(f(0)g(0) = 0\) in \(R\). Since \(R\) is a domain, we must have \(f(0) = 0\) or \(g(0) = 0\), i.e., \(f \in I\) or \(g \in I\).

Thus, \(I\) is a prime ideal of \(C[0, 1]\).

E13) Let us first assume that \(P\) is a prime ideal of \(R\). Since \(R\) has identity, so has \(R/P\). Now, let \(a + P\) and \(b + P\) be in \(R/P\) such that \((a + P)(b + P) = P\), the zero element of \(R/P\).

Then \(ab + P = P\), i.e., \(ab \in P\).

As \(P\) is a prime ideal of \(R\), either \(a \in P\) or \(b \in P\), i.e., either \(a + P = P\) or \(b + P = P\).

Thus, \(R/P\) has no zero divisors. Hence, \(R/P\) is an integral domain.

Conversely, assume that \(R/P\) is an integral domain. Let \(a, b \in R\) such that \(ab \in P\). Then \(ab + P = P\) in \(R/P\), i.e., \((a + P)(b + P) = P\) in \(R/P\).

As \(R/P\) is an integral domain, either \(a + P = P\) or \(b + P = P\), i.e., either \(a \in P\) or \(b \in P\).

This shows that \(P\) is a prime ideal of \(R\).

E14) i) From E35 of Unit 8, you know that \(f^{-1}(J)\) is an ideal of \(R\). Since \(f\) is surjective and \(J \neq S, f^{-1}(J) \neq R\).

Now, let \(a, b \in R\) such that \(ab \in f^{-1}(J)\).
Ring Theory

\[ \Rightarrow f(ab) \in J \]
\[ \Rightarrow f(a)f(b) \in J \]
\[ \Rightarrow f(a) \in J \text{ or } f(b) \in J, \text{ since } J \text{ is a prime ideal.} \]
\[ \Rightarrow a \in f^{-1}(J) \text{ or } b \in f^{-1}(J). \]

Thus, \( f^{-1}(J) \) is a prime ideal in \( R \).

ii) Since \( f \) is onto, you know that \( f(I) \) is an ideal of \( S \). Since \( I \neq R, 1 \notin I \). Also \( f^{-1}(f(I)) = I \), since \( N \subseteq I \). So \( f(I) \notin f(I) \). Thus, \( f(I) \neq S \).

Next, let \( x, y \in S \) such that \( xy \in f(I) \).

Since \( S = \text{Im } f \), \( \exists a, b \in R \) such that \( x = f(a) \) and \( y = f(b) \).

Then \( f(ab) = xy \in f(I) \), i.e., \( ab \in f^{-1}(f(I)) = I \).

\( \therefore a \in I \) or \( b \in I \), i.e., \( x \in f(I) \) or \( y \in f(I) \).

Thus, \( f(I) \) is a prime ideal of \( S \).

iii) \( \phi \text{ is } 1-1 : \phi(I) = \phi(J) \Rightarrow f(I) = f(J) \)

\[ \Rightarrow f^{-1}(f(I)) = f^{-1}(f(J)), \text{ since } N \subseteq I, N \subseteq J. \]

\[ \Rightarrow I = J. \]

\( \phi \text{ is onto:} \) Let \( J \) be a prime ideal of \( S \). Then \( f^{-1}(J) \) is a prime ideal of \( R \) and \( \phi(f^{-1}(J)) = f(f^{-1}(J)) = J \). Thus, \( J \in \text{Im } \phi \).

E15) i) Firstly, \( < p_1, p_2 > \subseteq < p_1 > \cap < p_2 > \), clearly.

Next, if \( \alpha \in < p_1 > \cap < p_2 > \), then \( \alpha = p_1x = p_2y \) for some \( x, y \in Z \). So \( p_1 \mid p_2y \). Therefore, \( p_1 \mid y \). Let \( y = p_1z \). Then \( \alpha = p_1p_2z \in < p_1, p_2 > \). So \( < p_1 > \cap < p_2 > \subseteq < p_1, p_2 > \).

\( \therefore < p_1 > \cap < p_2 > = < p_1, p_2 > \).

Since \( p_1, p_2 \) is not a prime, \( < p_1 > \cap < p_2 > \) is not a prime ideal.

ii) Let \( x \in I_1 \setminus I_2 \) and \( y \in I_2 \setminus I_1 \). Then \( xy \in I_1 \) and \( xy \in I_2 \), since \( I_1 \) and \( I_2 \) are ideals. \( \therefore xy \in I_1 \cap I_2 \).

But \( x \notin I_1 \cap I_2 \) and \( y \notin I_1 \cap I_2 \).

Thus, \( I_1 \cap I_2 \) is not prime.

E16) Suppose \( pZ \subseteq mZ, m \in Z \). Then \( p = mn \) for some \( n \in Z \).

So \( m = \pm 1 \) or \( m = \pm p \), since \( p \) is a prime number.

Thus, \( mZ = Z \) or \( mZ = pZ \).

Thus, \( pZ \) is a maximal ideal of \( Z \).

Now, you know that \( \{0\} \subseteq 2Z \subseteq Z \). Thus, \( \{0\} \) is not a maximal ideal of \( Z \).

E17) Consider \( < 4 > \) in \( Z \).

Since \( 4 \) is not a prime, \( < 4 > \) is not a prime ideal. Hence it cannot be a maximal ideal either.

E18) \( d : C \setminus \{0\} \to N \cup \{0\} : d(x) = 1 \).
For any \( a, b \in \mathbb{C} \setminus \{0\} \),
\[ \text{d}(ab) = 1 = \text{d}(a) . \]
\[ \therefore \text{d}(a) = \text{d}(ab) \forall a, b \in \mathbb{C} \setminus \{0\} . \]
Also, for any \( a, b \in \mathbb{C}, b \neq 0 \),
\[ a = (ab^{-1})b + 0 . \]
So, \( d \) trivially satisfies the second condition for a function to be an Euclidean valuation.
Thus, \( \mathbb{C} \) is a Euclidean domain.

E19) You know that
\[ \deg(f(x)g(x)) = \deg f(x) + \deg g(x) \forall f(x), g(x) \in \mathbb{R}[x] \setminus \{0\} . \]
You also know that given \( f(x), g(x) \in \mathbb{R}[x], g(x) \neq 0, \exists ! q(x) \) and \( r(x) \)
s.t. \( f(x) = q(x)g(x) + r(x) \), with \( \deg r(x) < \deg g(x) \).
Hence \( d \) is a Euclidean valuation on \( \mathbb{R}[x] \), and \( \mathbb{R}[x] \) is a Euclidean domain.
\[ d : \mathbb{Z}[x] \setminus \{0\} \to \mathbb{N} \cup \{0\} : d(f(x)) = \deg f(x) \]
is not a Euclidean valuation, since the division algorithm is not true within \( \mathbb{Z}[x] \). For example, given
\( 3x \) and \( 2x \) in \( \mathbb{Z}[x] \), there are no \( q(x) \) and \( r(x) \) such that
\[ 3x = 2xq(x) + r(x) \]. (Why?)

E20) Apply Theorem 2 to the Euclidean domain \( \mathbb{R}[x] \).

E21) Let \( \mathbb{R} = \mathbb{Z} \). Then \( S = \{ n \in \mathbb{Z} \mid |n| > 1 \} \cup \{0\} \).
Now, \( 2 \in S, 3 \in S \) but \( 2 - 3 \notin S \) since \( |2 - 3| = 1 \).
Thus, \( S \) is not even a subring of \( \mathbb{R} \), and hence \( S \) is not an ideal.

E22) For example, \( \mathbb{Z}[x] \) is a subring of \( \mathbb{Q}[x] \), which is a PID. But \( \mathbb{Z}[x] \) is not a PID.

E23) \( \mathbb{Z} \) is a PID. \( \mathbb{Z}/6\mathbb{Z} \) is not even a domain. Thus, it is not a PID.
However, every ideal in the quotient ring will be a principal ideal.

E24) \( \exists x, y \in \mathbb{R} \) such that \( ax + by = 1 \).
Then \( c = 1, c = (ax + by)c = acx + bcy \).
Since \( a \mid ac \) and \( a \mid bc, a \mid (acx + bcy) = c \).

E25) (i) is not, since it is \( (x - 1)^2 \).
(ii) is not, because of Theorem 4′.
(iii) is, because of Theorem 4′.
(iv) is not, because of Theorem 5.

E26) Let \( p = \text{ab} \). Then \( p \mid ab \Rightarrow p \mid a \) or \( p \mid b \).
Suppose \( p \mid a \). Let \( a = pc \). Then
\[ p = \text{ab} = \text{pcb} \Rightarrow p(1 - cb) = 0 \Rightarrow 1 - cb = 0, \] since \( \mathbb{R} \) is a domain and \( p \neq 0 \). Thus, \( bc = 1 \), i.e., \( b \) is a unit.
Similarly, you can show that if \( p \mid b \), then \( a \) is a unit.
So, \( p = ab \Rightarrow a \) is a unit or \( b \) is a unit, i.e., \( p \) is irreducible.

E27) (i), (iii) since 5 and \( x^2 + x + 1 \) are irreducible in \( \mathbb{Z} \) and \( \mathbb{R}[x] \), respectively.
(ii) is not, since \( x^2 - 1 = (x - 1)(x + 1) \) in \( \mathbb{Q}[x] \).
(iv) is not, since \( \mathbb{Z}[x]/<x> \cong \mathbb{Z} \), which is not a field.

E28) i) 1, ii) 7, iii) 5.

E29) Let \( f(x) = a_0 + a_1x + \cdots + a_nx^n \) and let the content of \( f(x) \) be \( d \). Let \( a_i = db_i \forall i = 0, 1, \ldots, n \). Then the g.c.d of \( b_0, b_1, \ldots, b_n \) is 1. Thus, \( g(x) = b_0 + b_1x + \cdots + b_nx^n \) is primitive. Also, \( f(x) = db_0 + db_1x + \cdots + db_nx^n = d(b_0 + b_1x + \cdots + b_nx^n) = dg(x) \).

E30) Let \( f(x) = \alpha f_i(x), g(x) = \beta g_i(x) \), where \( \alpha \) and \( \beta \) are the contents of \( f(x) \) and \( g(x) \), respectively, and \( f_i(x), g_i(x) \) are primitive. Then, by Gauss’s Lemma, \( f_i(x)g_i(x) \) is primitive, and \( f(x)g(x) = \alpha \beta f_i(x)g_i(x) \). Therefore, \( \alpha \beta \) is the content of \( f(g(x)) \).

E31) \( f(x) = x^n - p = a_0 + a_1x + \cdots + a_nx^n \),
where \( a_0 = -p, a_1 = 0 = \cdots = a_{n-1}, a_n = 1 \).
Thus, \( p \nmid a_i \forall i = 0, 1, \ldots, n - 1 \). \( p \nmid a_0, p \mid a_n \).
So, by Eisenstein’s criterion, \( f(x) \) is irreducible over \( \mathbb{Q} \).

E32) All of them are irreducible – (i) and (ii), because of Eisenstein’s criterion, taking \( p = 3 \); and (iii), because any linear polynomial is irreducible.

E33) Since \( a \neq 0, \pm 1, \exists \) a prime \( q \) such that \( q \mid a \). Also \( q^2 \nmid a \), since \( a \) is square-free. Then, using \( q \) as the prime, we can apply Eisenstein’s criterion, to conclude that \( x^p + a \) is irreducible in \( \mathbb{Z}[x] \). Thus, \( (x^p + a) \) is a prime element of \( \mathbb{Z}[x] \). Hence, \( <x^p + a> \) is a prime ideal of \( \mathbb{Z}[x] \). Hence the result.

E34) Since \((\mathbb{Z}_p^*, \cdot)\) is a group of order \((p - 1)\), \((\bar{a})^{p-1} = 1 \forall \bar{a} \in \mathbb{Z}_p^* \). Hence \( \bar{a}^p = \bar{a} \forall \bar{a} \in \mathbb{Z}_p^* \). Now consider \( x^p + \bar{a} \in \mathbb{Z}_p[x] \).
\( p - a \) is a zero of this polynomial, since \( (p - a)^p + \bar{a} = p - a + \bar{a} = \bar{p} = 0 \) in \( \mathbb{Z}_p \).
Thus, \( x^p + \bar{a} \) is reducible over \( \mathbb{Z}_p \).

E35) You can see that the result is true for \( n = 1 \).
Assume that it holds for some \( m \geq 1 \), i.e., whenever \( p \mid a_1a_2 \cdots a_m \), then \( p \mid a_i \) for some \( i = 1, 2, \ldots, m \).
Now let \( p \mid a_1a_2 \cdots a_{m+1} \). Then \( p \mid (a_1a_2 \cdots a_m)a_{m+1} \).
Since $p$ is a prime element, we find that $p | a_1a_2 \ldots a_m$ or $p | a_{m+1}$.

If $p | a_1a_2 \ldots a_m$, then $p | a_i$ for some $i = 1, \ldots, m$ by our assumption.

If $p \nmid a_1 \ldots a_m$, then $p | a_{m+1}$.

Thus, in either case, $p | a_i$ for some $i = 1, \ldots, m+1$.

So, our result is true for $n = m+1$.

Hence, it is true $\forall n \in \mathbb{N}$.

E36) $3x^5 - 2x^2 + 4x - 6$ is irreducible in $\mathbb{Q}[x]$, using Eisenstein’s criterion with $p = 2$. Since $\mathbb{Q}[x]$ is a PID, every irreducible element is prime.

Hence the given polynomial is prime in $\mathbb{Q}[x]$.

In $\mathbb{Z}_2[x]$ the given polynomial is $x^5$, since $\overline{2} = \overline{0}$ and $\overline{3} = \overline{1}$.

Since $x$ is prime in $\mathbb{Z}_2[x]$, $x^5$ is its prime factorisation.

E37) Let $f(x)$ be a non-zero non-unit in $F[x]$. We will prove that $f(x)$ can be written as a product of irreducible elements, by induction on $\deg f(x)$.

If $\deg f(x) = 1$, then $f(x)$ is linear, and hence irreducible.

Now suppose that the result is true for polynomials of degree $< n$.

Take $f(x)$ of degree $n$. If $f(x)$ is irreducible, there is nothing to prove.

Otherwise, there is a prime element $f_1(x)$ such that $f_1(x) | f(x)$. Let

$$f(x) = f_1(x)g_1(x).$$

Note that $\deg f_1(x) > 0$.

Hence, $\deg g_1(x) < \deg f(x)$. If $g_1(x)$ is prime, we are through.

Otherwise we can find a prime element $f_2(x)$ such that

$$g_1(x) = f_2(x)g_2(x).$$

Then $\deg g_2(x) < \deg g_1(x)$. This process must stop after a finite number of steps, since each time we get polynomials of lower degree. Thus, we shall finally get

$$f(x) = f_1(x)f_2(x) \ldots f_m(x),$$

where each $f(x)$ is prime in $F[x]$.

Now, to show that the factorisation is unique, you should follow the lines of the proof of Theorem 14.

E38) $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Using the norm function, you should check that each of $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

E39) For example, consider

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Let us show that each of these factors is irreducible in $\mathbb{Z}[\sqrt{-3}]$, by contradiction.

Suppose $1 + \sqrt{-3}$ is reducible.

Then $1 + \sqrt{-3} = \alpha \beta$ for some non-units $\alpha, \beta$ in $\mathbb{Z}[\sqrt{-3}]$.

Taking the norm function, we get

$$4 = N(1 + \sqrt{-3}) = N(\alpha)N(\beta).$$

So the only possibility is $N(\alpha) = 2$, $N(\beta) = 2$.

Let $\alpha = a + b\sqrt{-3}$, $a, b \in \mathbb{Z}$.

Then $a^2 + 3b^2 = 2$. 
Ring Theory

If $b \neq 0$, then $a^2 + 3b^2 \geq 2$, and if $b = 0$, then $a^2 = 2$.
Neither case is possible, and we reach a contradiction.

$\therefore 1 + \sqrt{-3}$ is irreducible in $\mathbb{Z}[\sqrt{-3}]$.

Similarly, you can check that the other factors of $4$ are irreducible in $\mathbb{Z}[\sqrt{-3}]$. Also, none of them are associates of each other, since the only units of $\mathbb{Z}[\sqrt{-3}]$ are $1$ and $-1$.

Hence, $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

E40) $\mathbb{Z}[x]$, as you have seen in Theorem 17 and Example 8.

E41) i) False. For example, $x$ is irreducible in $\mathbb{Z}[x]$, but $x$ is zero in $\mathbb{Z}[x]/\langle x \rangle \simeq \mathbb{Z}$, and hence not irreducible.

ii) False. For example, $\mathbb{Z}$ is a UFD, but in $\mathbb{Z}/\langle 6 \rangle$, $4$ has two different prime factorisations, viz., $2 \cdot 2 = 2 \cdot 2 \cdot 2 = 4$.

For another example, $\mathbb{Z}[\sqrt{-5}] \simeq \mathbb{Z}[x]/\langle x^2 + 5 \rangle$ is not a UFD, while $\mathbb{Z}[x]$ is.

iii) False. For example, $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$, a UFD. But $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

iv) True. To see why, let $r$ be a non-zero non-unit in $R$.

Then $r$ is also a non-unit in $R[x]$.

Hence $r = p_1(x)p_2(x)\ldots p_n(x)$ uniquely, where $p_i(x) \in R[x]$ are irreducibles.

So $0 = \deg r = \sum_{i=1}^{n} \deg p_i(x)$.

Hence, $\deg p_i = 0 \forall i = 1, \ldots, n$, i.e., $p_i \in R \setminus \{0\} \forall i = 1, \ldots, n$.

That is, $r = p_1p_2\ldots p_n$ uniquely, where $p_i \in R$ are irreducible in $R$.

Thus, $R$ is a UFD.
UNIT 10  CONGRUENCES

Structure

10.1 Introduction 65
   Objectives
10.2 Basic Results on Congruences 66
10.3 The Chinese Remainder Theorem 79
10.4 The Quadratic Reciprocity Law 88
10.5 Summary 99
10.6 Solutions/Answers 100

10.1 INTRODUCTION

In the previous unit, we discussed integral domains and Euclidean domains. In this unit, we will restrict our attention to a particular Euclidean domain, namely the ring \( \mathbb{Z} \) of integers. We will discuss the notion of congruences and their applications.

Gauss, in his book *Disquisitiones Arithmeticae* formulated the notion of congruences and introduced the notation that we use for congruences at present. Before the publication of the book, number theory was a collection of isolated results due to other mathematicians like Euler, Fermat, Lagrange and Legendre. With the help of the notion of congruences he revolutionised number theory and changed it from a collection of isolated results into a coherent subject. He not only reformulated many results known earlier in terms of congruences, he also proved many new results. In the recent times, congruences have led to many interesting applications in computing.

In our discussion of congruences, we will see some nice applications of the concepts that we discussed in units on groups and rings as well as some nice applications of the theorems we proved there. However, instead of using ring theory and group theory we can prove all the results that we prove using elementary number theory.

In Sec. 9.2, we prove basic results regarding congruences using basic concepts from algebra that you have studied in your degree course. In Sec. 9.3, we will prove the Chinese remainder theorem, which has many applications, and derive some of its consequences. One of the results in the study of congruences, which is important from both the theoretical and applications point of view, is the quadratic reciprocity law. In Sec. 9.4, we will prove quadratic reciprocity which was proved rigorously by Gauss although the statement of the result was known earlier to Euler and Legendre. Here are the objectives of this unit.

Objectives

After studying this unit, you should be able to

- define linear congruences and give examples;
- apply the extended g.c.d to solve the congruence \( ax \equiv b \pmod{n} \), \( a, b, n \in \mathbb{N} \);
- use the Chinese Remainder Theorem to solve simultaneous linear congruences;
• state and apply the quadratic reciprocity law;

• define, and calculate, the Legendre symbol \( \left( \frac{m}{n} \right) \), \( m, n \in \mathbb{Z} \), \( n \) odd;

• solve the equation \( x^2 - a \equiv 0 \pmod{p} \), when \( p \) is a prime and \( a \) and \( p \) are odd numbers coprime to each other, using quadratic reciprocity;

### 10.2 BASIC RESULTS ON CONGRUENCES

In this section, we begin our discussion on congruences. During the course of our discussion, we will apply certain results from ring theory in a particular situation, namely \( R = \mathbb{Z} \). As we have already discussed ring theory in Units 8 and 9, we will refer you to these Units for proofs of the results.

Recall that \( \mathbb{Z} \) is a **Euclidean Domain** and hence a **Principal Ideal Domain (PID)** and a **Unique Factorisation Domain (UFD)**.

If \( n \in \mathbb{Z} \), \( \langle n \rangle \) denotes the ideal generated by \( n \) and \( \mathbb{Z}/\langle n \rangle \) is the quotient ring of the ideal \( \langle n \rangle \). We denote the quotient ring by \( \mathbb{Z}_n \). We have a canonical ring homomorphism

\[
\psi: \mathbb{Z} \rightarrow \mathbb{Z}_n \quad \ldots (1)
\]

We write \( \overline{a} \) for the image \( \psi(a) \) of \( a \in \mathbb{Z} \). Recall that \( \overline{a} = \psi(a) \) is actually a coset and not a single element. In fact

\[
\psi(a) = a + \langle n \rangle = \{a + kn | k \in \mathbb{Z}\}
\]

We call \( \overline{a} \), the **residue class** of \( a \). We have \( \overline{a} = \overline{b} \) if and only if \( a - b \in \langle n \rangle \) or equivalently, \( n \mid (a - b) \). If \( \overline{a} = \overline{b} \), we write \( a \equiv b \pmod{n} \) which is read as ‘\( a \) is congruent to \( b \) modulo \( n \)’. (Note that \( \equiv \) is an equivalence relation.)

**Definition 1**: We say that \( \{a_1, a_2, \ldots, a_n\} \), where \( a_i \in \mathbb{Z} \), is a **complete set of residues modulo \( n \)** if \( a_i \neq a_j \pmod{n} \) for \( i \neq j \). We call \( \{0, 1, 2, \ldots, n - 1\} \) the **canonical set of residues mod \( n \)**.

We will often use the elements of the canonical set of residues as representatives for the residue classes during computations.

The map \( \psi \) gives us a method of translating the results about the ring \( \mathbb{Z}_n \) into an assertion regarding congruences. We will frequently use \( \psi \) to move back and forth between results regarding congruences and results regarding the ring \( \mathbb{Z}_n \).

As an immediate consequence of the ring homomorphism \( \psi \) in [Eqn. (1)], we get the following result:

**Proposition 1**: If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then

\[
a + c \equiv b + d \pmod{n} \quad \ldots (2)
\]

and

\[
ac \equiv bd \pmod{n} \quad \ldots (3)
\]
We leave the proof to you as an exercise. In the next example we give a divisibility test that gives an application of Proposition 1.

**Example 1:** Show that, if \(n = a_k a_{k-1} \cdots a_0\) is the decimal representation of a natural number \(n\), \(n \equiv a_k + a_{k-1} + \cdots + a_0 \pmod{9}\). Deduce that a natural number is divisible by 9 iff the sum of its digits in the decimal representation is divisible by 9.

**Solution:** Since \(10 \equiv 1 \pmod{9}\), it follows from Eqn. (3) that
\[
10^i \equiv 1 \pmod{9} \text{ for all } i \geq 1 \quad \ldots (4)
\]
Suppose the number is \(n = a_k a_{k-1} \cdots a_0\). Then, in decimal notation
\[
n = \sum_{i=0}^{k} a_i 10^i.
\]
It follows from Eqn. (4) that \(n \equiv (a_k + a_{k-1} + \cdots + a_0) \pmod{9}\).
So, \(n \equiv 0 \pmod{9}\) iff \(a_k + a_{k-1} + \cdots + a_0 \equiv 0 \pmod{9}\). In other words, \(n\) is divisible by 9 iff \(a_k + a_{k-1} + \cdots + a_0\) is divisible by 9.

\[\star \star \star\]

Note that Example 1 helps us find the remainder of a number when divided by 9. Let us see how in the next example.

**Example 2:** Find the remainder on dividing 76629 by 9.

**Solution:** We have
\[
7 + 6 = 13 \equiv 4 \pmod{9},
7 + 6 + 6 \equiv 4 + 6 = 10 \equiv 1 \pmod{9},
7 + 6 + 6 + 2 = 1 + 2 \equiv 3 \pmod{9},
7 + 6 + 6 + 2 + 9 \equiv 3 + 9 \equiv 3 \pmod{9}
\]
So, the remainder is 3.

\[\star \star \star\]

Before we proceed further we point out an application of Example 2.

**Remark 1:** A well known application of Example 2 is the method of 'casting out 9s' for checking whether long additions and multiplications that we have performed are correct. Suppose we multiplied 76629 by 1259 and got 96475911 and we want to check whether answer is correct. Using Example 1, we get
\[
76629 \equiv 3 \pmod{9} \text{ and } 1259 \equiv 8 \pmod{9}. \quad \text{So,}
76629 \cdot 1259 \equiv 8 \cdot 3 = 24 \equiv 6 \pmod{9}. \quad \text{Again, using Example 1 to find the remainder on dividing 96475811 by 9, we get 96475811 \equiv 5 \not\equiv 6 \pmod{9}. \quad \text{So, our answer is wrong.}
\]
However, even if the answer got by multiplying the remainders match, the answer may not be correct. For example, suppose we got the answer 96372611 in the previous example. You can check that 96372611 \(\equiv 6 \pmod{9}\), but this answer is not correct. You can also check that this is not right answer.

Try the following exercise to check your understanding of Example 1 and Example 2.

E1) Show that if we write \(n \in \mathbb{N}\) as \(n = a_k a_{k-1} \cdots a_0\) in decimal notation, \(n \equiv a_0 - a_1 + \cdots + (-1)^k a_k \pmod{11}\). Use this to check whether 1901207 is divisible by 11.

E2) Let \(m, n \in \mathbb{N}\). Show that they have the same unit digit if and only if \(n \equiv m \pmod{10}\).
E3) If \(a, b, c, d \in \mathbb{N}\) and \(a \equiv b \pmod{n}\) and \(c \equiv d \pmod{n}\), show that:

i) \(a + c \equiv b + d \pmod{n}\)

ii) \(ac \equiv bd \pmod{n}\).

E4) Show that, for any non-zero \(d \in \mathbb{Z}\) and \(a, b \in \mathbb{Z}\), \(ad \equiv bd \pmod{nd}\) if and only if \(a \equiv b \pmod{n}\).

We now define the g.c.d of two integers.

**Definition 2**: We define the greatest common divisor of \(a\) and \(b \in \mathbb{Z}\) to be the largest integer that divides both \(a, b \in \mathbb{Z}\), at least one of them non-zero. If \(d\) is the greatest common divisor of \(a\) and \(b\) we denote the g.c.d of \(a\) and \(b\) by \((a, b)\) and write \((a, b) = d\).

We have already defined the g.c.d for PIDs in Unit 9. You may be wondering why we have to define the g.c.d again for \(\mathbb{Z}\), which is a PID. The definition in Unit 9 determines the g.c.d only up to multiplication by a unit. However, according to Definition 2, the g.c.d of two integers is a positive integer when at least one of them is not zero and it is unique. We define \((0, 0) = 0\). Also, we have

\[
(d, 0) = |d| \quad \ldots (5)
\]

\[
(a, b) = (b, a) \quad \ldots (6)
\]

\[
(-a, b) = (a, b) \quad \ldots (7)
\]

Using Eqn. (5), we can assume that both \(a\) and \(b\) are non-zero. Using Eqn. (6) and Eqn. (7) we can assume that \(a\) and \(b\) are both positive. Again, using Eqn. (6), we can assume that \(a > b\). The g.c.d of two integers \(a\) and \(b\) satisfies the following conditions:

1) \(d\) divides both \(a\) and \(b\).

2) If \(d'\) divides both \(a\) and \(b\), then \(d'\) divides \(d\).

The next proposition is just a restatement of Theorem 3 in Unit 9 in the case \(R = \mathbb{Z}\).

**Proposition 2**: If \(a, b \in \mathbb{Z}\) and \(d = (a, b)\), we can find \(u, v \in \mathbb{Z}\) such that \(d = au + bv\).

The proof in Unit 9 doesn’t ensure that \(d > 0\). However, in general, any two g.c.d.s differ only by a unit and the only units in \(\mathbb{Z}\) are \(\pm 1\). So, if \(d\) and \(d'\) are two g.c.d.s according to the definition for general PIDs, in the case of \(\mathbb{Z}\) we must have \(d = \pm d'\). So, if \(ux + vy = d\) with \(d < 0\), we have \((-u)x + (-v)y = -d > 0\). So, we can always find \(u\) and \(v\) such that \(ua + vb = d\) with \(d > 0\).

In many situations, we have to find a solution of the congruence

\[
ax \equiv b \pmod{n} \quad \ldots (8)
\]

How can we do this? This is equivalent to finding a solution to the equation

\[
\bar{a}x = \bar{b} \quad \ldots (9)
\]

in \(\mathbb{Z}_n\).

For example, finding a solution to \(3x \equiv 5 \pmod{7}\) is equivalent to finding a solution to the equation \(\bar{3}x = \bar{5}\) in \(\mathbb{Z}_7\).
If \( \overline{a} \) is a unit in \( \mathbb{Z}_n \), then \( x = \overline{a}^{-1}\overline{b} \) is a solution to [Eqn. (9)]. The next proposition tells us when \( \overline{a} \) is a unit in \( \mathbb{Z}_n \).

**Proposition 3**: \( \overline{a} \in \mathbb{Z}^{\langle \langle n \rangle >} \) is a unit if and only if \( (a, n) = 1 \).

**Proof**: Suppose \( (a, n) = 1 \). By Proposition 2 there are \( u, v \in \mathbb{Z} \) such that \( au + vn = d \). Since \( (a, n) = 1 \), we can find \( u \) and \( v \) such that \( au + vn = 1 \). We have

\[
\psi(1) = \psi(au + vn) = \psi(u)\psi(a) + \psi(v)\psi(n) = \psi(u)\psi(a), \text{ since } \psi(n) = 0
\]

\[
= \overline{u} \overline{a} = \overline{1} \text{ since } \psi(1) = 1 \text{ from the RHS}
\]

So, \( \overline{a} \overline{a} = \overline{1} \). Thus, \( \overline{a} = \overline{a}^{-1} \) and \( \overline{a} \) is a unit in \( \mathbb{Z}_n \). We leave it to you to prove that, if \( \overline{a} \) is a unit in \( \mathbb{Z}_n \), then \( (a, n) = 1 \).

**Corollary 1**: If \( (a, n) = 1 \), \( x \in \mathbb{Z} \) such that \( x = \overline{a}^{-1}\overline{b} \) is a solution to the congruence \( ax \equiv b \pmod{n} \).

**Proof**: If \( x \in \mathbb{Z} \) is such that \( x = \overline{a}^{-1}\overline{b} \), then \( ax - b = 0 \) or \( ax - b = 0 \) in \( \mathbb{Z}_n \). In other words \( ax - b = 0 \) in \( \mathbb{Z}_n \). So, \( n \) divides \( ax - b \). This means that \( ax \equiv b \pmod{n} \).

In the proof of Proposition 3, we showed that, if \( (a, n) = 1 \) and \( u \) and \( v \) are such that \( au + vn = 1 \), then \( \overline{u} \) is the inverse of \( \overline{a} \). Translated in terms of congruences, this means that \( u \) is a solution to the equation \( ax \equiv 1 \pmod{n} \). So, to find \( \overline{a}^{-1} \), we have to find \( u \) and \( v \) such that \( au + vn = 1 \). Let us now discuss an algorithm that will help us in finding \( u \) and \( v \). We need the following lemma.

**Lemma 1**: Let \( a, b \in \mathbb{Z} \). We have \( (a, b) = (b, a \pmod{b}) \).

**Proof**: Let \( (a, b) = d \) and \( (b, c) = d' \) where \( c \) is an arbitrary element in the residue class \( a \pmod{b} \), i.e. \( c \equiv a \pmod{b} \). We have \( c - a = bk_0 \) or \( c = a + bk_0 \)

for \( k_0 \in \mathbb{Z} \). Since \( d \mid a \) and \( d \mid b, d \mid c \). Since \( d \) divides both \( b \) and \( c \), \( d \mid d' \).

To complete the proof, we need to show that \( d' \mid d \). Since \( d' \) divides \( b \) and \( c \) it divides \( a = c - bk_0 \). It follows that \( d' \) divides \( d \), the g.c.d of \( a \) and \( b \).

Note that, while finding \( (a, b) \), we can always assume that \( a \geq 0, b \geq 0 \). If \( a < 0 \), using [Eqn. (7)] we can find \((-a, b)\) instead. If \( b < 0 \), we have

\[
(a, b) = (b, a) \text{ using Eqn. (6)}
\]

\[
= (-b, a) \text{ using Eqn. (7)}
\]

and \( -b < 0 \). If both are negative,

\[
(a, b) = (-a, b) \text{ using Eqn. (7)}
\]

\[
= (b, -a) \text{ using Eqn. (6)}
\]

\[
= (-b, -a) \text{ using Eqn. (7)}
\]

\(-a, -b\) are non-negative. Also, using [Eqn. (6)] we can always assume that \( a > b \).

Here is a modern version of the algorithm that is given in Euclid’s *Elements* for finding the g.c.d.
Theorem 1: Let \(a, b\) non-negative natural numbers such that \(a > b\). The following algorithm yields the g.c.d of \(a\) and \(b\).

**Step 1** [Is \(b = 0\)?] If \(b = 0\), \((a, b) = a\). Stop. Otherwise go to Step 2.

**Step 2** [Replace \(a\) by remainder.] Write \(a = qb + d, 0 \leq d < b\). Set \(a \leftarrow b, b \leftarrow d\). Go to Step II. (Here \(\leftarrow\) denotes the assignment operator and \(a \leftarrow b\) means that assign the value of \(b\) to \(a\).)

This algorithm is given in Propositions 1 and 2 of Book 7 of Euclid’s *Elements* which was written around 300 BC. It may have been known to Eudoxus earlier. Euclid gives no proof, but just examples.

**Proof:** We let \(a_1 = a, b_1 = b\). Given \(a_k\) and \(b_k\), we define \(a_{k+1}, b_{k+1}\) recursively as follows: We write

\[
a_{k+1} = b_k, \quad b_{k+1} = d_k, \quad q_{k+1} = \left[\frac{a_{k+1}}{b_{k+1}}\right] = \left[\frac{b_k}{d_k}\right], \quad d_{k+1} = b_k - q_{k+1}d_k
\]

Note that, \(q_{k+1}\) is the quotient on division of \(a_{k+1}\) by \(b_{k+1}\) and \(d_{k+1}\) is the remainder on division of \(a_{k+1}\) by \(b_{k+1}\). We have \(b_{k+1} < b_k\) since \(d_k\) is the remainder on dividing \(a_k\) by \(b_k\). To prove that the above algorithm works, we have to prove that the algorithm stops after finitely many steps and gives \((a, b)\) when it stops.

Since \(b_{k+1} < b_k, b_1 > b_2 > \cdots\) is a strictly decreasing sequence of natural numbers, therefore \(b_k = 0\) for some value of \(k\), say \(k_0\). So, when Step 1 is called in the algorithm after calculating \(a_{k_0}, b_{k_0}\) the algorithm will return \(a_{k_0}\) and stop.

To show that the algorithm returns the correct answer we show by induction that \((a_k, b_k) = (a, b)\) for all \(k \geq 1\). This is true for \(k = 1\). Suppose it is true for \(k\). We need to show that \((a_{k+1}, b_{k+1}) = (a, b)\). We have \(b_{k+1} = d_k = a_k - q_kb_k\). So, \(b_k\) divides \(b_{k+1} - a_k\), i.e. \(b_{k+1} = a_k \pmod{b_k}\). Applying Lemma 1, we have

\[
(a_{k+1}, b_{k+1}) = (b_k, a_k \pmod{b_k}) = (a_k, b_k) = (a, b)
\]

We get the last equality from the induction hypothesis.

Let us look at an example to see how we apply the algorithm.

**Example 3:** Find \((19, 7)\).

**Solution:** In Step 1, since \(b \neq 0\), we go to Step II. We divide 19 by 7 to get \(19 = 7 \cdot 2 + 5\).

We go to Step 1 with the problem of finding \((7, 5)\). Here, \(b = 5 \neq 0\). So, we go to step 2. We have \(7 = 5 \cdot 1 + 2\). We go to Step 1 to find \((5, 2)\).

Again \(b = 2 \neq 0\) and we go to step 2. We have \(5 = 2 \cdot 2 + 1\). We go to Step 1 to find \((2, 1)\).

Again, \(b = 1 \neq 0\) so we go to step 2. We have \((2 = 1 \cdot 2 + 0)\). We go to Step 1 to find \((1, 0)\). Since \(b = 0\) we stop and we have \((19, 7) = a = 1\).

\[
\star \star \star
\]

Here is an exercise to check your understanding of Example 3.

**Exercise 5:** Compute the greatest common divisors of the following pairs of numbers:

i) 65, 25, ii) \(-141, 93\), iii) \(-21, -8\)

We can modify the same algorithm to find \(u\) and \(v\) such that \(au + bv = d\). All we need is to do some additional ‘book keeping’. Let us see how.
Let us write \( a_1 = a, b_1 = b \). We have \( a_1 = b_1 q_1 + d_1 \). When we reach Step II for the \( i^{th} \) time, we will calculate \( a_i, b_i, q_i \) and \( d_i \). Suppose we have calculated \( u_{i-1}, v_{i-1}, u_i, v_i \) such that

\[
\begin{align*}
  u_{i-1}a + v_{i-1}b &= d_{i-1} \quad \ldots \text{(10)} \\
  u_ia + v_ib &= d_i \quad \ldots \text{(11)}
\end{align*}
\]

Suppose we want to calculate \( u_{i+1}, v_{i+1} \) such that

\[
  u_{i+1}a + v_{i+1}b = d_{i+1}.
\]

We have

\[
\begin{align*}
  a_{i-1} &= q_{i-1}b_{i-1} + d_{i-1} \\
  a_i &= q_ib_i + d_i \\
  a_{i+1} &= q_{i+1}b_{i+1} + d_{i+1} \quad \ldots \text{(12)}
\end{align*}
\]

We have \( a_{i+1} = b_i = d_{i-1} \) and \( b_{i+1} = d_i \). Using Eqn. (10), Eqn. (11) and Eqn. (12) we get

\[
  u_{i-1}a + v_{i-1}b = (u_ia + v_ib)q_{i+1} + d_{i+1}
\]

Rearranging, we get

\[
  d_{i+1} = (u_{i-1} - q_{i+1}u_i) a + (v_{i-1} - q_{i+1}v_i) b
\]

Writing

\[
\begin{align*}
  u_{i+1} &= u_{i-1} - u_iq_{i+1} \quad \ldots \text{(13)} \\
  v_{i+1} &= v_{i-1} - v_iq_{i+1} \quad \ldots \text{(14)}
\end{align*}
\]

we have \( u_{i+1}a + v_{i+1}b = d_{i+1} \).

So, Eqn. (13) and Eqn. (14) tells us how to calculate \( u_{i+1} \) and \( v_{i+1} \) if we know \( u_{i-1}, v_{i-1}, u_i, v_i \) and \( q_{i+1} \).

We can take \( u_1 = 1, v_1 = -q_1 \) because \( a_1 - q_1b_1 = d_1 \). To be able to calculate \( u_2, v_2 \) we need two set of values, \( u_0, v_0 \) and \( u_1, v_1 \). What values can we take for \( u_0 \) and \( v_0 \) ? We claim that \( u_0 = 0, v_0 = 1 \) works. If we use these values, we get \( u_2 = -q_2 \) and \( v_2 = 1 + q_1q_2 \) from Eqn. (13) and Eqn. (14) (Check this!) We claim that these are the correct values of \( u_2 \) and \( v_2 \). Let us see why.

We have \( a_2 = b, b_2 = d_1 \). So,

\[
  b = a_2 = b_2q_2 + d_2 = d_1q_2 + d_2 = (a_1 - b_1q_1)q_2 + d_2 = (a - bq_1)q_2 + d_2
\]

or \((-q_2)a + (1 + q_1q_2)b = d_2 \) So, \( u_2 = -q_1 \) and \( v_2 = 1 + q_1q_2 \) and our choice \( u_0 = 0, v_0 = 1 \) works.

Our choice of \( u_0 \) and \( v_0 \) gives the equation \( u_0a + v_0b = 0 \cdot a + 1 \cdot b = b \) and we can think of this as equation for \( d_0 \) since we can think of \( b \) as \( d_0 \). (Recall the relation \( b_1 = d_{i-1} \) and \( b_1 = b \)). So, our choice is not at all unnatural!
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>a₁ = a</td>
<td>b₁ = b</td>
<td>q₁</td>
<td>1</td>
<td>-q₁</td>
<td>d₁</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aᵢ-₁</td>
<td>bᵢ-₁</td>
<td>qᵢ-₁</td>
<td>uᵢ-₁</td>
<td>vᵢ-₁</td>
<td>dᵢ-₁</td>
</tr>
<tr>
<td>aᵢ</td>
<td>bᵢ</td>
<td>qᵢ</td>
<td>uᵢ</td>
<td>dᵢ</td>
<td></td>
</tr>
<tr>
<td>aᵢ+₁</td>
<td>bᵢ+₁</td>
<td>dᵢ+₁</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a) Copy bᵢ below aᵢ

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>a₁ = a</td>
<td>b₁ = b</td>
<td>q₁</td>
<td>1</td>
<td>-q₁</td>
<td>d₁</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aᵢ-₁</td>
<td>bᵢ-₁</td>
<td>qᵢ-₁</td>
<td>uᵢ-₁</td>
<td>vᵢ-₁</td>
<td>dᵢ-₁</td>
</tr>
<tr>
<td>aᵢ</td>
<td>bᵢ</td>
<td>qᵢ</td>
<td>uᵢ</td>
<td>dᵢ</td>
<td></td>
</tr>
<tr>
<td>aᵢ+₁</td>
<td>bᵢ+₁</td>
<td>dᵢ+₁ = aᵢ+₁ - qᵢ+₁bᵢ+₁</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b) Copy dᵢ below bᵢ

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>a₁ = a</td>
<td>b₁ = b</td>
<td>q₁</td>
<td>1</td>
<td>-q₁</td>
<td>d₁</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aᵢ-₁</td>
<td>bᵢ-₁</td>
<td>qᵢ-₁</td>
<td>uᵢ-₁</td>
<td>vᵢ-₁</td>
<td>dᵢ-₁</td>
</tr>
<tr>
<td>aᵢ</td>
<td>bᵢ</td>
<td>qᵢ</td>
<td>uᵢ</td>
<td>dᵢ</td>
<td></td>
</tr>
<tr>
<td>aᵢ+₁</td>
<td>bᵢ+₁</td>
<td>dᵢ+₁</td>
<td>uᵢ+₁ = uᵢ-₁ - qᵢ+₁uᵢ</td>
<td>dᵢ⁺₁</td>
<td></td>
</tr>
</tbody>
</table>

(c) Compute qᵢ⁺₁ and dᵢ⁺₁.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>a₁ = a</td>
<td>b₁ = b</td>
<td>q₁</td>
<td>1</td>
<td>-q₁</td>
<td>d₁</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aᵢ-₁</td>
<td>bᵢ-₁</td>
<td>qᵢ-₁</td>
<td>uᵢ-₁</td>
<td>vᵢ-₁</td>
<td>dᵢ-₁</td>
</tr>
<tr>
<td>aᵢ</td>
<td>bᵢ</td>
<td>qᵢ</td>
<td>uᵢ</td>
<td>dᵢ</td>
<td></td>
</tr>
<tr>
<td>aᵢ+₁</td>
<td>bᵢ+₁</td>
<td>dᵢ⁺₁</td>
<td>uᵢ⁺₁ = uᵢ-₁ - qᵢ⁺₁uᵢ</td>
<td>dᵢ⁺₁</td>
<td></td>
</tr>
</tbody>
</table>

(d) If dᵢ⁺₁ ≠ 0, multiply the numbers in the squares and subtract from the circled number to compute uᵢ⁺₁.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>a₁ = a</td>
<td>b₁ = b</td>
<td>q₁</td>
<td>1</td>
<td>-q₁</td>
<td>d₁</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aᵢ-₁</td>
<td>bᵢ-₁</td>
<td>qᵢ-₁</td>
<td>uᵢ-₁</td>
<td>vᵢ-₁</td>
<td>dᵢ-₁</td>
</tr>
<tr>
<td>aᵢ</td>
<td>bᵢ</td>
<td>qᵢ</td>
<td>uᵢ</td>
<td>dᵢ</td>
<td></td>
</tr>
<tr>
<td>aᵢ+₁</td>
<td>bᵢ+₁</td>
<td>dᵢ⁺₁</td>
<td>uᵢ⁺₁ = uᵢ-₁ - qᵢ⁺₁uᵢ</td>
<td>dᵢ⁺₁</td>
<td></td>
</tr>
</tbody>
</table>

(e) Multiply the numbers in the squares and subtract from the circled number to compute vᵢ⁺₁.

Fig. 1: Computing the values of u and v.

Let us see how to calculate the values of u and v by hand. Fig. 1 explains how to compute aᵢ⁺₁, bᵢ⁺₁, uᵢ⁺₁, vᵢ⁺₁, if we know the values of aᵢ, bᵢ, uᵢ₋₁, vᵢ₋₁, uᵢ, and vᵢ. Note that qᵢ⁺₁ = \( \frac{aᵢ⁺₁}{bᵢ⁺₁} \). Till what point do we carry out this computation? We continue to compute till we get dₖ = 0 or dₖ = 1 for some natural number k ≥ 0. Then, the g.c.d of a is d_k₋₁ and u = u_k₋₁, v = v_k₋₁. The
method we have discussed is known as the extended Euclidean algorithm.

Let us now look at an example.

**Example 4:** Find \( u, v \in \mathbb{Z} \) such that \( 19u + 7v = (19, 7) \).

**Solution:** You can see how to calculate the third row in the table in Fig. 2.

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
\hline
19 & 7 & 2 & 1 & -2 & 5 \\
7 & 5 & 1 & 2 & &
\end{array}
\]

(a) Copy \( b_i \) below \( a_i \).

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
\hline
19 & 7 & 2 & 1 & -2 & 5 \\
7 & 5 & 1 & 2 & &
\end{array}
\]

(b) Copy \( d_i \) below \( b_i \).

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
\hline
19 & 7 & 2 & 1 & -2 & 5 \\
7 & 5 & 1 & 2 & &
\end{array}
\]

(c) Compute \( q_2 \) and \( d_2 \).

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
\hline
19 & 7 & 2 & 1 & -2 & 5 \\
7 & 5 & 1 & 2 & &
\end{array}
\]

(d) Multiply the numbers in squares and subtract from the circled number.

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
\hline
19 & 7 & 2 & 1 & -2 & 5 \\
7 & 5 & 1 & 2 & &
\end{array}
\]

We got \( d = 0 \) in the 5th row. So, values of \( u \) and \( v \) in the fourth row gives us the correct answer, i.e. \((19, 7) = 1, u = 3, v = -8\) and \((3)19 + (-8)7 = 1\). Of course, we could have stopped when we got \( d = 1 \) because \( d = 0 \) for the next row. (Why?) In this case the value of \( u \) and \( v \) in the row with \( d = 1 \) gives the correct answer.

Let us now look at some more examples.

**Example 5:** Use the extended g.c.d algorithm to write the g.c.d of the following pairs of numbers as an integer linear combination of the pairs of numbers:

i) \( 91, 35 \), ii) \(-62, 34\), iii) \(-21, -13\).
Solution:

i) As before, we present the computation in tabular form:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>35</td>
<td>2</td>
<td>-2</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>21</td>
<td>1</td>
<td>-1</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>14</td>
<td>1</td>
<td>2</td>
<td>-5</td>
<td>7</td>
</tr>
<tr>
<td>14</td>
<td>7</td>
<td>2</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

In this example, \( d = 0 \) in the fifth row. So, we can stop here. From the fourth row, the greatest common divisor is 7, the values of \( u \) and \( v \) are \( u = 2 \) and \( v = -5 \).

ii) We find \((62, 34)\). The computation in tabular form is given below:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>62</td>
<td>34</td>
<td>1</td>
<td>-1</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>28</td>
<td>1</td>
<td>-1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>1</td>
<td>-6</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

So, \((62, 34) = 2\). Also \((-6)62 + (11)34 = 2\). So, \(6(-62) + (11)34 = 2\).

iii) We find \((21, 13)\). The computation in tabular form is given below:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>13</td>
<td>1</td>
<td>-1</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>8</td>
<td>1</td>
<td>-1</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>1</td>
<td>-3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>-3</td>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>-5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

We have \((21, 13) = 1\) and \(5(21) + (-8)13 = 1\). So, \((-5)(-21) + 8(-13) = 1\)

***

Here are some exercises for you to try and check your understanding of our discussion calculation of g.c.d.

E6) Use the extended g.c.d algorithm to write the g.c.d of the following pairs of numbers as an integer linear combination of the pairs of numbers:

i) \(65, 25\) ii) \(141, 93\) iii) \(21, 8\) iv) \(-63, 24\) v) \(-170, -25\).

Let us now look at an example to see how to solve congruences of the type in Eqn. (8).

Example 6: Find a solution to the equation \(7x \equiv 5 \pmod{19}\).
Solution: Here $(19, 7) = 1$. From Example 4, we know that $(3)19 + (-8)7 = 1$

Hence, $7^{-1} = -8$. We have,

$$x \equiv 7^{-1} \cdot 5 \equiv -8 \cdot 5 \equiv -40 \equiv 17 \pmod{19}$$

Thus, $x = 17$ is a unique solution to the congruence $7x \equiv 5 \pmod{19}$ modulo $17$ i.e. if $k_0 \in \mathbb{Z}$ satisfies $7k_0 \equiv 5 \pmod{19}$, then $7 \equiv k_0 \pmod{17}$.

\[\ast \ast \ast\]

In the next example we will discuss a word problem inspired by ‘Introduction to number theory’ by Harold M. Stark.

Example 7: A merchant visits a neighbouring town every five months on business. Suppose his first visit is in March. Which of his series of visits will fall in a March again? Which of his series of visits fall in a February for the first time?

Solution: Let number the months $1, 2, \ldots, 12$, starting from January. Then, the visits which fall in March are given by the non-negative solutions to the congruence

$$3 + 5(x - 1) \equiv 3 \pmod{12} \text{ or } 5x \equiv 5 \pmod{12}$$

This is because the number of months on which the merchant visits the neighbouring town forms an arithmetic progression with first term 3 and common difference 5. Also, since there are 12 months in a year, we need to discard multiples of 12 to get the correct month, so we consider the solutions modulo 12.

Using extended gcd algorithm, we get $(-2)12 + (5)5 = 1$, so, $5^{-1} = 5$ in $\mathbb{Z}_{12}$.

Thus, we get $x \equiv 1 \pmod{12}$ or $x = 1 + 12k$, $k \in \mathbb{Z}$, $k \geq 0$. Here $k = 0$ corresponds to the first visit and his second visit will correspond to $k = 1$. So, he will make his $13^{th}$ visit in March again.

To find out which of his visits will fall in February for the first time, we need to solve the congruence $3 + 5(x - 1) \equiv 2 \pmod{12}$, i.e. the congruence $5x \equiv 4 \pmod{12}$. So, $x \equiv 20 \equiv 8 \pmod{12}$. So, his $8^{th}$ visit will fall in February for the first time.

\[\ast \ast \ast\]

We next prove a result regarding cancellation of a constant occurring in both the sides of a congruence.

Proposition 4: If $(a, n) = 1$ and $a\ell \equiv am \pmod{n}$, then $\ell \equiv m \pmod{n}$.

Proof: In $\mathbb{Z}_n$, we can translate $a\ell \equiv am \pmod{n}$ as $\bar{a}\bar{\ell} = \bar{a}\bar{m}$ in $\mathbb{Z}_n$. Since $(a, n) = 1$, $\bar{a}$ is a unit. So, we can multiply both sides of the equation $\bar{a}\bar{\ell} = \bar{a}\bar{m}$ by $\bar{a}^{-1}$ to get $\bar{\ell} = \bar{m}$. Translating this back into congruences, we get what we want. ■

What can we say about the solution to Eqn. (8) in general? Here is the result.

Proposition 5: The congruence $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$. 

75
Proof: Let $d = (n, a)$. If $x \in \mathbb{Z}$ is a solution to Eqn. (8), then $n \mid (ax - b)$. Since $d \mid n, d \mid (ax - b)$. Since $d \mid a, d$ also divides $b$. Conversely, suppose $d \mid b$. Note that, by definition, $d \mid a$ and $d \mid n$. So, the following equation makes sense.

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \quad \ldots (15)$$

Since $(\frac{a}{d}, \frac{n}{d}) = 1$. So, by Corollary 1 it follows that there is a $x_0 \in \mathbb{Z}$ such that

$$\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

for some $k \in \mathbb{Z}$. Using Exercise 4, we get $ax_0 \equiv b \pmod{n}$.

According to Proposition 5, it is not necessary that $(a, n) = 1$ for the congruence $ax \equiv b \pmod{n}$ to have a solution. The result in Corollary 1 to Proposition 3 gives us a method for solving the congruence $ax \equiv b \pmod{n}$ when $(a, n) = 1$. When $(a, n) \neq 1$, we can still solve the congruence in Eqn. (8) provided that the condition in Proposition 3 is satisfied. However, if $(a, n) \neq 1$, Eqn. (8) can have more than one solution modulo $n$. For example, $2x \equiv 4 \pmod{6}$ has two solutions, 2 and 5, but $2 \not\equiv 5 \pmod{6}$. The next proposition gives us all the solutions to Eqn. (8) when $(a, n) \neq 1$ and $(a, n) \mid b$.

**Proposition 6:** Let $d \mid b$ where $(a, n) = d$. Let us write $a_1 = \frac{a}{d}, b_1 = \frac{b}{d}, n_1 = \frac{n}{d}$.

i) The map $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1}$, defined by $\phi(a + (n)) = a + (n_1)$ is a surjective ring homomorphism.

ii) We have $\ker(\phi) = \{i \bar{a} \mid 0 \leq i < d\}$.

iii) Let $x_1 \in \mathbb{Z}_{n_1}$ be a solution to the equation $a_1x_1 = b_1$ in $\mathbb{Z}_{n_1}$ and $x_0 \in \mathbb{Z}_n$ be such that $\phi(x_0) = x_1$, $0 \leq x_0 < n$. The solutions to the equation $ax \equiv b \pmod{n}$ are given by $x_0 + i \bar{a}, 0 \leq i < d$.

**Proof:**

i) We have, if $I$ and $J$ are ideals in a commutative ring $R$ and $I \subset J$, the map $a + I \mapsto a + J$ is a surjective ring homomorphism. Here $(n) \subset (n_1)$

ii) Since $\phi$ is surjective,

$$\frac{|\mathbb{Z}_n|}{|\ker(\phi)|} = \frac{|\mathbb{Z}_n|}{|\ker(\phi)|} = |\mathbb{Z}_{n_1}|$$

Therefore,

$$|\ker(\phi)| = \frac{|\mathbb{Z}_n|}{|\mathbb{Z}_{n_1}|} = \frac{n}{n_1} = d$$

Also, $(\mathbb{Z}_n, +)$ is a cyclic group of order $n$ generated by $1 + (n)$. So, $\ker(\phi)$ is a cyclic subgroup of $\mathbb{Z}_n$ with generator $\frac{n}{d}$.

iii) We have $a_1\bar{x}_0 = \bar{a}_1x_1$ in $\mathbb{Z}_{n_1}$. Translating to congruences, we have $a_1x_0 \equiv a_1x_1 \pmod{n_1}$. Since $x_1$ is a solution to the congruence $a_1x_1 \equiv b_1 \pmod{n_1}$, we have $a_1x_0 \equiv b_1 \pmod{n_1}$. So, using Exercise 4 we get $a_1dx_0 \equiv b_1d \pmod{n_1d}$ or $ax_0 \equiv b \pmod{n}$. If $x_0'$ is a solution to
the congruence \( ax \equiv b \pmod{n} \), then \( a_1d'x_0' \equiv b_1 \pmod{n_1d} \), so \( x_0' \) is a solution to the congruence \( a_1x \equiv b_1 \pmod{n_1} \). Since \( a_1x \equiv b_1 \pmod{n_1} \) has a unique solution modulo \( n_1 \), it follows that \( x_0' \equiv x_1 \pmod{n_1} \). So, \( \phi(x_0 - x_0') = 0 \) and \( x_0' = x_0 + id, 0 \leq i < d \).

The next example shows how to solve the congruence \( ax \equiv b \pmod{n} \), when \( (a, n) \mid b \).

**Example 8:** Solve the congruence \( 15x \equiv 6 \pmod{39} \).

**Solution:** Here, we have \( a = 15, b = 6 \) and \( n = 39 \). We have \( d = (15, 39) = 3 \) and \( 3 \mid 6 \). We have \( a_1 = 5, b_1 = 2 \) and \( n_1 = 13 \). We consider the congruence \( 5x \equiv 2 \pmod{13} \). We compute \( u \) and \( v \) such that \( 5u + 13v = 1 \). The computations are shown below:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>-2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>1</td>
<td>-1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>-5</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

So, \( 2 \cdot 13 + (-5) \cdot 5 = 1 \). Thus \( 5^{-1} = \overline{-5} = 8 \) in \( \mathbb{Z}_{13} \). Multiplying both sides of the congruence \( 5x \equiv 2 \pmod{13} \) by 8, we get \( x \equiv 16 \equiv 3 \pmod{13} \). So, there are three solutions to the congruence, \( 3, 3 + 1 \cdot 13 = 16 \) and \( 3 + 2 \cdot 13 = 29 \).

Here are some exercises for you to try.

E7) Solve the following congruences:
   i) \( 3x \equiv 2 \pmod{17} \)    ii) \( 4x \equiv 6 \pmod{18} \)
   iii) \( 10x \equiv 5 \pmod{85} \)

Note that the units in \( \mathbb{Z}_n \) form a group, usually denoted by \( U(\mathbb{Z}_n) \). From Proposition 3, it follows that

\[
U(\mathbb{Z}_n) = \left\{ \overline{a} \in \mathbb{Z}_n \setminus \{0\} \mid (a, n) = 1 \right\}
\]

If \( S \) is a complete set of residues for \( \mathbb{Z}_n \), then

\[
U(\mathbb{Z}_n) = \left\{ \overline{a} \mid a \in S, (a, n) = 1 \right\}
\]

In particular, we can take \( S = \{1, 2, \ldots, n - 1\} \). Then,

\[
U(\mathbb{Z}_n) = \left\{ \overline{a} \mid 1 \leq a \leq n - 1, (a, n) = 1 \right\}
\] \hspace{1cm} \ldots(16)

**Definition 3:** For \( n \in \mathbb{N} \), we define

\[
\phi(n) = \left| \{ a \mid 1 \leq a \leq n - 1, (a, n) = 1 \} \right|
\] \hspace{1cm} \ldots(17)

\( \phi(n) \) is called the **Euler phi-function**.
From Eqn. (16), we have
\[ \phi(n) = |U(\mathbb{Z}_n)| \quad \ldots (18) \]

The next proposition gives an interesting property satisfied by the Euler’s phi-function.

**Proposition 7 (Euler’s Theorem):** If \((a, n) = 1\), where \(a \in \mathbb{Z}\), then
\[ a^{\phi(n)} \equiv 1 \pmod{n} \quad \ldots (19) \]

**Proof:** For any finite group \(G\) and any \(a \in G\), we have \(a^{|G|} = 1\). In the case of \(U(\mathbb{Z}_n)\), we have \(a^{\phi(n)} = 1 \forall a \in U(\mathbb{Z}_n)\). If \(a \in \mathbb{Z}\) and \((a, n) = 1\), then \(\bar{a} \in U(\mathbb{Z}_n)\) and \(\bar{a}^{\phi(n)} = 1\). Translating this in the language of congruences, \(a^{\phi(n)} \equiv 1 \pmod{n}\). ■

As it stands, Eqn. (19) doesn’t tell us much regarding the computation of \(\phi(n)\). Later, we will see an expression for \(\phi(n)\) in Eqn. (36). However, when \(p\) is a prime, we get the following interesting result immediately.

**Corollary 2 (Fermat’s Little Theorem):** If \(p\) is a prime, \(a \in \mathbb{Z}\) and \((p, a) = 1\).
\[ a^{p-1} \equiv 1 \pmod{p} \quad \ldots (20) \]

**Proof:** For every \(a \in \mathbb{Z}\), \(1 \leq a \leq p - 1\), we have \((a, p) = 1\). So,
\[ |\{a|1 \leq a \leq p - 1, (a, p) = 1\}| = |\{a|1 \leq a \leq p - 1\}| = p - 1 \]

The result now follows from Proposition 7. ■

Let us look at some examples of applications of the Euler’s Theorem and Fermat’s Little Theorem.

**Example 9:** Use Fermat’s Little Theorem to prove the following:

i) 19 divides \(13^{99} + 1\).

ii) If \((a, 133) = 1\), \((b, 133) = 1\), \(a^{18} \equiv b^{18} \pmod{133}\).

iii) For any integer \(a\), \(a^5\) and \(a\) have the same units digit.

**Solution:**

i) We have to use the fact that \(a^{18} \equiv 1 \pmod{19}\). We divide 99 by 18 and get
\[ 99 = 18 \cdot 5 + 9 \]
So, we have
\[ 13^{99} \equiv \left(13^{18}\right)^5 \cdot 13^9 \equiv 13^9 \pmod{19} \]
\[ \equiv (-6)^9 \equiv (-6)(-6)(-6) \equiv 1 \]
\[ \equiv 16 \cdot (-6) \equiv (-3)(-6) \equiv 18 \equiv -1 \pmod{19} \]

Therefore, 19 divides \(13^{99} + 1\).

ii) We have 133 = 7 \cdot 19. Since \((a, 133) = 1\), \((a, 7) = 1\), \((a, 19) = 1\). We have \(a^6 \equiv 1 \pmod{7}\), so \(a^{18} \equiv 1 \pmod{7}\). Also, since \((a, 19) = 1\), \(a^{18} \equiv 1 \pmod{19}\). Therefore, since 7 divides \(a^{18} - 1\), 19 also divides \(a^{18} - 1\) and \(7, 19 = 1\), 133 divides \(a^{18} - 1\), i.e. \(a^{18} \equiv 1 \pmod{133}\). Similarly, \(b^{18} \equiv 1 \pmod{133}\). So,
\[ a^{18} \equiv b^{18} \pmod{133} \]
or 133 divides \(a^{18} - b^{18}\). 

iii) For any integer \(a\), \(a^5\) and \(a\) have the same units digit.

As it stands, Eqn. (19) doesn’t tell us much regarding the computation of \(\phi(n)\).
iii) If \((a, 5) = 1\), then \(a^4 \equiv 1 \pmod{5}\), so 5 divides \(a^5 - a = a(a^4 - 1)\). One of \(a\) or \(a^4 - 1\) has to be even. (Why?). So, 2 divides \(a^5 - a\). Since \((5, 2) = 1\), 10 divides \(a^5 - a\), i.e. \(a^5 \equiv a \pmod{10}\). So \(a^5\) and \(a\) have the same units digit.

If \((a, 5) \neq 1\), since \((a, 5)\) divides 5, we must have \((a, 5) = 5\), i.e. 5 divides \(a\). Let \(a = 5k, k \in \mathbb{Z}\). Then, \(a^5 - a = (5k)((5k)^4 - 1)\). So, 5 divides \(a^5 - a\). If \(k\) is even, 2 divides 5k, so 10 divides \(a^5 - a\). If \(k\) is odd, \((5k)^4 - 1\) is even, so 2 divides \(a^5 - a\). Since both 2 and 5 divide \(a^5 - a\) and \((5, 2) = 1\), 10 divides \(a^5 - a\). So \(a\) and \(a^5\) have the same units digit.

E8) Find the units digit of \(7^{323}\).

E9) If \(a \nmid 11\), show that \(a^5 + 1\) or \(a^5 - 1\) is divisible by 11.

Here are some exercises for you.

---

We close this section here. In the next section, we will see how to solve simultaneous congruences, for example, pairs of congruences of the type \(x \equiv 3 \pmod{11}, x \equiv 2 \pmod{7}\).

### 10.3 THE CHINESE REMAINDER THEOREM

In ancient days, it was required to calculated the date in which certain celestial bodies, rotating around the earth, are at a certain position. Since different celestial bodies have different periods of rotation, solving this involves finding integer solutions to simultaneous congruences. Such congruences were discussed in *Sun Tzu Suan Ching* (Master Sun’s Arithmetical Manual) which was written some time between 280 A.D. and 473. Hence, the method for solving such congruences is known as the Chinese Remainder Theorem.

Aryabhata has discussed solutions of simultaneous congruences in *Aryabhatiya*, written in the 5th century A.D. He devised *kuṭṭāka* for solving simultaneous congruences. Consider the pair of congruences \(x \equiv a \pmod{n_1}\) and \(x \equiv b \pmod{n_2}\). If \(u\) and \(v\) \(\in \mathbb{Z}\) satisfy \(un_1 - vn_2 = b - a\) then \(x = un_1 + a = vn_2 + b\) is a solution to the pair of congruences.

In modern times, modular arithmetic is used to add and multiply large integers in some computers. The idea is as follows: Suppose we have to add two large numbers \(N_1\) and \(N_2\). The numbers may be too large that they may fit within a single word in computer. For example, the word size in 32 bit computers is \(2^{32}\) and \(N_1\) and \(N_2\) may be large compared to this. We can break up the task of adding \(N_1\) and \(N_2\) into adding numbers which are smaller as follows: We pick some natural numbers \(n_1, n_2, \ldots, n_k\) such that all of them are pairwise coprime and smaller than the word size. Suppose \(N_1 \equiv a_1 \pmod{n_1}\) and \(N_2 \equiv b_1 \pmod{n_1}\). We find \((a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)\). Using Chinese Remainder Theorem which we will discuss in this section, we can then find \(N_1 + N_2\) from \((a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)\).

Let us first look at an example involving the Chinese Remainder Theorem.

**Example 10:** A class has to be divided into groups for carrying out an activity. When the teacher divided the class into groups of three, one student was left
and cannot be assigned to any group. When she divided the class into groups of four, two students were left. When she divided the class into groups of five, three students were left. If no class is allowed to have more than 660 students, what is the minimum number of students in the class?

**Solution:** Suppose the minimum number of students in the class is \( x \). Since one student was left if the class was divided into three groups, \( x \equiv 1 \pmod{3} \). Similarly, from the other information we have, we get the congruences \( x \equiv 2 \pmod{4} \) and \( x \equiv 3 \pmod{5} \). So, we have to find the smallest solution to the simultaneous congruences

\[
\begin{align*}
  x &\equiv 1 \pmod{3} \\
  x &\equiv 2 \pmod{4} \\
  x &\equiv 3 \pmod{5}
\end{align*}
\]


We will see how to solve the above congequences this using the Chinese Remainder Theorem in Example II.

Let us now state and prove the Chinese Remainder Theorem.

**Theorem 2:** If \( n_1, n_2, \ldots, n_k \) are pairwise relatively prime integers (i.e. \( (n_i, n_j) = 1 \) if \( i \neq j \)) and \( a_1, a_2, \ldots, a_k \) are any integers, there is a solution \( x_0 \) to the following simultaneous congruences:

\[
\begin{align*}
  x &\equiv a_1 \pmod{n_1} \\
  x &\equiv a_2 \pmod{n_2} \\
  \vdots \\
  x &\equiv a_n \pmod{n_k}
\end{align*}
\]

If \( x_0 \) and \( x'_0 \) are two solutions, then \( x_0 \equiv x'_0 \pmod{N} \), where \( N = n_1n_2\cdots n_k \).

**Proof:** Let us first solve a special case of Eqn. (21). Let us fix an \( i \) and suppose that \( a_i = 1 \) and \( a_j = 0 \), for \( j \neq i \). We look at the congruences

\[
\begin{align*}
  x &\equiv 0 \pmod{n_1} \\
  x &\equiv 0 \pmod{n_2} \\
  \vdots \\
  x &\equiv 1 \pmod{n_i} \\
  x &\equiv 0 \pmod{n_{i+1}} \\
  \vdots \\
  x &\equiv 0 \pmod{n_k}
\end{align*}
\]

Let

\[
N_i = \prod_{j \neq i} n_j \quad \ldots (23)
\]

Then, \((N_i, n_i) = 1\) and we can find integers \( u_i \) and \( v_i \) such that \( u_iN_i + v_i n_i = 1 \). This gives the congruences

\[
\begin{align*}
  u_iN_i &\equiv 1 \pmod{n_i} \quad \ldots (24) \\
  u_iN_i &\equiv 0 \pmod{n_j} \quad \text{for } j \neq i \quad \ldots (25)
\end{align*}
\]
since \( N_i \) is divisible by \( n_j \) if \( j \neq i \). So, \( x_i = u_iN_i \) satisfies

\[
x_i \equiv 0 \pmod{n_j} \quad \text{for } j \neq i \quad \ldots \text{(26)}
\]

and \( x_i \equiv 1 \pmod{n_i} \quad \ldots \text{(27)} \)

For each \( i \), \( 1 \leq i \leq k \) we find an \( x_i \) satisfying Eqn. (26) and Eqn. (27). We can use the \( x_i \)s to get an \( x \) satisfying by taking \( x = a_1x_1 + a_2x_2 + \ldots + a_kx_k \). So, if \( x \equiv a_jx_j \equiv a_j \pmod{n_j} \) for \( 1 \leq i \leq k \) since \( a_jx_j \equiv 0 \pmod{n_i} \) if \( j \neq i \).

If \( x_0, x'_0 \) are two solutions to the simultaneous congruences in Eqn. (21), then \( x_0 \equiv x'_0 \pmod{n_i} \) for \( 1 \leq i \leq k \) since \( a_jx_j \equiv 0 \pmod{n_i} \) if \( j \neq i \). Since \( n_i \) are pairwise coprime, \( N = \prod n_i \) also divides \( x_0 - x'_0 \), i.e. \( x_0 \equiv x'_0 \pmod{N} \).

While Theorem 2 tell us that a solution to Eqn. (21) exists, it does not tell us how to construct such a solution. However, we can work this out from the proof itself. In the proof of Theorem 2, we saw that we have to construct \( x_i \) such that

\[
x_i \equiv 0 \pmod{n_j} \quad \text{for } j \neq i \quad \text{and} \quad x_i \equiv 1 \pmod{n_i}.
\]

Then, we take the linear combination \( \sum_{i=1}^{n} a_ix_i \). We constructed such an \( x_i \) by taking the solution \( u_i \) to the congruences in Eqn. (24) and Eqn. (25) and multiplying it by \( N_i \). The congruence in Eqn. (24) implies that \( u_i = N_i^{-1} \) in \( \mathbb{Z}_{n_i} \). So, if we choose \( N'_i \) such that \( N'_i = N_i^{-1} \) in \( \mathbb{Z}_{n_i} \), the congruence in Eqn. (24) is satisfied for \( u_i = N'_i \). For all \( j \neq i \), since \( N_j \equiv 0 \pmod{n_i} \), \( N'_iN_j \equiv 0 \pmod{n_i} \). So, we choose \( x_i \) such that \( x_i = N'_iN_i \) in \( \mathbb{Z}_{n_i} \), multiply the \( x_i \) by \( a_i \) and sum them up to get a solution to the congruence in Eqn. (21). So, if Eqn. (21) is solvable, \( x = \sum_{i=1}^{k} a_iN_iN'_i \) is a solution to it, where

\[
N = \prod_{j} n_j \quad \text{and} \quad N'_i = N_i^{-1} \quad \text{in } \mathbb{Z}_{n_i} \]

To find the smallest non-negative solution, we take the smallest non-negative residue of \( x \pmod{N} \).

**Step by Step procedure for solving Eqn. (21)**

1. First, we compute \( N_i \) using Eqn. (23). We then reduce it modulo \( \pmod{n_i} \)

2. Compute \( N'_i \) which is such that \( N_iN'_i \equiv 1 \pmod{n_i} \). If \( n_i \) is small enough take powers \( N_i, N_i^2 \) etc. \( \pmod{n_i} \) till we get \( N_i^{k} = 1 \). Then, \( N_i^{-1} \pmod{n_i} \equiv N'_i \). If \( n_i \) is large, we use the extended euclidean algorithm to find the inverse.

3. Find \( a_iN_iN'_i \pmod{n_i} \). Find

\[
\alpha = \sum_{i=1}^{k} a_iN_iN'_i
\]

If \( \alpha \) is negative, add \( N = \prod n_i \) as many times as necessary to make the value positive if a positive solution is required. If the answer is positive and greater than \( N \) divide \( \alpha \) by \( N \) and take the remainder.
Let us look at an example that illustrates the above procedure.

**Example 11:** Solve the following congruences that we set up in Example 10:

\[ x \equiv 1 \pmod{3} \quad x \equiv 2 \pmod{4} \quad x \equiv 3 \pmod{5} \]

**Solution:** Let us take \( n_1 = 3, n_2 = 4 \) and \( n_3 = 5 \). Then \( N = 60 \). Let us now compute \( N_i \)s and \( N'_i \)s.

\[
\begin{align*}
N_1 &= 4 \cdot 5 = 20 \\
N_2 &= 3 \cdot 5 = 15 \\
N_3 &= 3 \cdot 4 = 12
\end{align*}
\]

We have \( N_1 \equiv 2 \pmod{3} \), \( N_1^2 = 4 \equiv 1 \pmod{3} \) so, we take \( N'_1 = 2 \).

We have \( N_2 \equiv 3 \pmod{4} \), \( N_2^2 = 9 \equiv 1 \pmod{5} \). So, \( N'_2 = 3 \).

We have \( N_3 = 12 \equiv 5 \pmod{7} \). \( N_3^2 = 25 \equiv 4 \pmod{7} \), \( N_3^3 = 20 \equiv 6 \pmod{7} \), \( N_3^4 = 30 \equiv 2 \pmod{7} \), \( N_3^5 = 10 \equiv 3 \pmod{7} \) and \( N_3^6 \equiv 1 \pmod{7} \). So, \( N'_3 = 3 \).

\[
x = a_1 N'_1 N_1 + a_2 N'_2 N_2 + a_3 N'_3 N_3
\]

\[
= 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 238
\]

So, there can’t be more than 60 students in the classes, we take the smallest non-negative residue of 238 (mod 60) which is 58. So, there are 58 students in the class.

***

**Remark 2:** A word of caution is in order. Note that, in Example 11 we have taken the actual values of \( N_i \) and we have not reduced them \( \pmod{n_j} \). If we had done so, we would have got a wrong answer. In this case we have \( N_1 \equiv 2 \pmod{3} \), \( N_2 \equiv 3 \pmod{4} \) and \( N_3 \equiv 2 \pmod{5} \). If we use the reduced values of \( N_i \)s, we get \( x = 1 \cdot 2 \cdot 2 + 2 \cdot 3 \cdot 3 + 3 \cdot 2 \cdot 3 = 40 \) and \( 40 \not\equiv 2 \pmod{4} \).

The issue is that \( N_i \equiv 0 \pmod{n_j} \) for \( j \neq i \), but \( N_i \) may not be zero \( \pmod{n_j} \) after reducing it modulo \( n_i \). For example, \( N_i = 20 \equiv 0 \pmod{5} \). We have \( 20 \equiv 2 \pmod{3} \) and \( 2 \not\equiv 0 \pmod{5} \).

Here is a slightly more elaborate example.

**Example 12:** Solve the following set of congruences:

\[
\begin{align*}
x &\equiv 3 \pmod{14} \quad \ldots(28) \\
4x &\equiv 5 \pmod{15} \quad \ldots(29) \\
x &\equiv 9 \pmod{19} \quad \ldots(30)
\end{align*}
\]

**Solution:** Notice that (Eqn. 29) is not in the form given in (Eqn. 21). Since \( (4, 15) = 1 \), we can convert it to equivalent form by multiplying both sides of Eqn. (29) by the inverse of \( 4 \pmod{15} \) which is \( 4 \) itself. So, Eqn. (29) becomes \( x \equiv 20 \equiv 5 \pmod{15} \). So, the set of congruences reduces to

\[
\begin{align*}
x &\equiv 3 \pmod{14} \quad \ldots(31) \\
x &\equiv 5 \pmod{15} \quad \ldots(32) \\
x &\equiv 9 \pmod{19} \quad \ldots(33)
\end{align*}
\]
We have \( N_1 = 15 \cdot 19 = 285, N_2 = 14 \cdot 19 = 266 \) and \( N_3 = 210 \). As you can see the numbers are somewhat large. We use the extended euclidean algorithm to find \( N_i' \), the inverse of \( N_i \mod n_i \).

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
 * & * & * & 0 & 1 & * \\
 285 & 14 & 20 & 1 & -20 & 5 \\
 14 & 5 & 2 & -2 & 41 & 4 \\
 5 & 4 & 1 & 3 & -61 & 1 \\
\end{array}
\]

We have, \((3)285 + (-61)14 = 1\), so \( N_1' = 3 \).

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
 * & * & * & 0 & 1 & * \\
 266 & 15 & 17 & 1 & -17 & 11 \\
 15 & 11 & 1 & -1 & 18 & 4 \\
 11 & 4 & 2 & 3 & -53 & 3 \\
 4 & 3 & 1 & -4 & 71 & 1 \\
\end{array}
\]

We have \((-4)266 + (71)15 = 1\), so \( N_2' = -4 \).

\[
\begin{array}{cccccc}
 a & b & q & u & v & d \\
 * & * & * & 0 & 1 & * \\
 210 & 19 & 11 & 1 & -11 & 1 \\
\end{array}
\]

We have \((1)210 - (11)19 = 1\). So, \( N_3' = 1 \). We have

\[
x = \sum_{i=1}^{3} a_i N_i N_i' = 3 \cdot 285 \cdot 3 + 5 \cdot 266 \cdot (-4) + 9 \cdot 210 \cdot 1 = -865
\]

which is negative. We have \( N = 14 \cdot 15 \cdot 19 = 3990 \) and \(-865 + 3990 = 3125\).

Of course, we could have have take \( N_2' = 11 \) instead of \(-4\). In that case the answer would have been 19085 and the remainder of 19085 on division by 3990 is 3125 again.

***

You have already studied the structure of \( \mathbb{Z}_n \) as an abelian group in Unit 5. Let us now use Theorem 2 to find out more about the ring structure of \( \mathbb{Z}_n \). Let \( n \) be a natural number \( n = \prod_{i=1}^{k} p_i^{\alpha_i} \) and \( p_i \) distinct. Then, since \( \langle n \rangle \subset \langle p_i^{\alpha_i} \rangle \) for \( 1 \leq i \leq k \), we have ring homomorphisms \( g_i : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_i^{\alpha_i}} \).

(See third isomorphism theorem, Unit 8, Exercise 38.) Putting together the \( g_i \)'s, we have a ring homomorphism

\[
g : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}, m \mapsto (g_1(m), g_2(m), \ldots, g_k(m)) \quad \text{(34)}
\]

**Proposition 8** : The map given by Eqn. (34) is an isomorphism of rings.

**Proof** : Since each \( g_i \) is a ring homomorphism from \( \mathbb{Z}_n \) to \( \mathbb{Z}_{p_i^{\alpha_i}} \), \( g \) is a ring homomorphism. Let \( (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \). Then,

\[
g(m) = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_k)
\]

83
if and only if \( m \) is the solution to the congruences

\[
m \equiv a_1 \pmod{p_1^{\alpha_1}} \\
m \equiv a_2 \pmod{p_2^{\alpha_2}} \\
\vdots \\
m \equiv a_k \pmod{p_k^{\alpha_k}}
\]

By Chinese Remainder Theorem, given any

\[(\overline{a_1}, \overline{a_2}, \overline{a_3}, \ldots, \overline{a_k}) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}},
\]

there is always an \( m \in \mathbb{Z} \) such that \( m \equiv a_i \pmod{p_i^{\alpha_i}} \). So, the map \( g \) given by is surjective. The map is also injective because the Chinese Remainder Theorem also says that if \( m, m' \) are two solutions to the congruences \( x \equiv a_i \pmod{p_i^{\alpha_i}} \), then \( m \equiv m' \pmod{n} \). ■

As an immediate consequence of Proposition 8, we get the following result:

**Corollary 3**: Let \( n \) be a natural number \( n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \). Then, the map \( g \) in Proposition 8 induces an isomorphism of groups

\[
g : U(\mathbb{Z}_n) \longrightarrow U\left(\mathbb{Z}_{p_1^{\alpha_1}}\right) \times U\left(\mathbb{Z}_{p_2^{\alpha_2}}\right) \times \cdots \times U\left(\mathbb{Z}_{p_k^{\alpha_k}}\right) \quad \cdots (35)
\]

Further,

\[
\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \quad \cdots (36)
\]

Also,

\[
\phi(mn) = \phi(m)\phi(n) \text{ if } (m, n) = 1 \quad \cdots (37)
\]

**Proof**: Since \( g \) is a ring isomorphism, if \( u \) is a unit such that \( uv = 1 \), it follows that \( g(u)g(v) = 1 \). So, \( g(u) \) is unit. Therefore

\[
g(\mathbb{U}(\mathbb{Z}_n)) \subseteq U\left(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}\right) .
\]

Since \( g \) given by Eqn. (34) is one-one, its restriction to \( \mathbb{U}(\mathbb{Z}_n) \) is also one-one.

Let us now prove that \( g \) given by Eqn. (34) when restricted to \( \mathbb{U}(\mathbb{Z}_n) \) is also onto. Let

\[
u' \in U\left(\mathbb{Z}_{p_1^{\alpha_1}}\right) \times U\left(\mathbb{Z}_{p_2^{\alpha_2}}\right) \times \cdots \times U\left(\mathbb{Z}_{p_k^{\alpha_k}}\right) \subseteq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} .
\]

Then, since \( g \) given by Eqn. (34) is a onto map, there is a \( u \in \mathbb{Z}_n \) such that \( g(u) = u' \). We need to prove that \( u \) is a unit, i.e. \( u \in \mathbb{U}(\mathbb{Z}_n) \). Since \( u' \) is a unit, there is a \( v' \) such that \( u'v' = 1 \). Let \( v \in \mathbb{Z}_n \) be such that \( g(v) = v' \). We have \( g(uv) = g(u)g(v) = u'v' = 1 \). Since \( g(1) = 1 \) and \( g \) is one-one, it follows that \( uv = 1 \). So, \( u \) is also a unit.

Thus \( g \) induces an isomorphism between the groups \( \mathbb{U}(\mathbb{Z}_n) \) and

\[
\mathbb{U}\left(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}\right) .
\]

Further, we have

\[
\mathbb{U}\left(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}\right) = \mathbb{U}\left(\mathbb{Z}_{p_1^{\alpha_1}}\right) \times \mathbb{U}\left(\mathbb{Z}_{p_2^{\alpha_2}}\right) \times \cdots \times \mathbb{U}\left(\mathbb{Z}_{p_k^{\alpha_k}}\right)
\]
This proves that the map in Eqn. (35) is an isomorphism.

We know that \( \phi(n) = |U(Z_n)| \). From Eqn. (35), it follows that

\[
|U(Z_n)| = \prod_{i=1}^{k} |U(Z_{p_i^{\alpha_i}})|
\]

To prove Eqn. (36) it is enough to show that

\[
|U(Z_{p^\alpha})| = p^{\alpha-1}(p - 1) = p^\alpha - p^{\alpha-1}
\]  

\( \ldots \) (38)

and

\[
\phi(n) = n \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right) = \prod_{i=1}^{k} p_i^{\alpha_i-1}(p_i - 1)
\]  

\( \ldots \) (39)

We have

\[
\prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right)
\]

\[
= \prod_{i=1}^{k} p_i^{\alpha_i} \left( 1 - \frac{1}{p_i} \right) = \prod_{i=1}^{k} p_i^{\alpha_i-1}(p_i - 1)
\]

This proves Eqn. (39) Let us now check Eqn. (38) Now,

\[\{ a \mid 0 \leq a \leq p^\alpha - 1, \, p \mid a \} = \{ kp \mid 0 \leq k < p^\alpha-1 \}\]

and \(|\{ kp \mid 0 \leq k < p^\alpha-1 \}| = p^\alpha-1\). Note that \((a, p^\alpha) = 1 \iff p \nmid a\). So,

\[|U(Z_{p^\alpha})| = |\{ a \mid 0 \leq a < p^\alpha - 1 \}| - |\{ a \mid 0 \leq a < p^\alpha - 1, \, p \mid a \}| = p^\alpha - p^{\alpha-1}\]

The result in Eqn. (37) is an immediate consequence of Eqn. (36).

Here are some exercises for you to check your understanding of our discussion so far.

E10) Solve the following set of simultaneous congruences:

\[x \equiv 2 \pmod{5} \quad x \equiv 4 \pmod{7} \quad x \equiv 3 \pmod{11}\]

E11) Solve the following set of simultaneous congruences:

\[3x \equiv 2 \pmod{4} \quad 8x \equiv 4 \pmod{9} \quad x \equiv 3 \pmod{11}\]

E12) Three cyclists are training in a circular velodrome. A spectator arrives at the start line of the velodrome at a certain time \( t_0 \). The first cyclist crosses the starting line 1 second after \( t_0 \), the second cyclist crosses the starting line 2 seconds after \( t_0 \) and the third cyclist crosses the starting line 3 seconds after \( t_0 \). The first cyclist takes 4 seconds to complete one round of the velodrome, the second cyclist takes 5 seconds to complete one round of the velodrome and the third cyclist takes 7 seconds to complete one round of the velodrome. How many seconds after \( t_0 \) will all the cyclists cross the starting line at the same time?
E13) Suppose \( R \) is a commutative ring with unity such that
\[
R = R_1 \times R_2 \times \cdots \times R_k,
\]
where \( R_1, R_2, \ldots, R_k \) are commutative rings with unity. Prove that
\[
U(R) = U(R_1) \times U(R_2) \times \cdots \times U(R_k)
\]

As you know already, \((\mathbb{Z}_n, +)\) is a cyclic group. We will now discuss the structure of \((U(\mathbb{Z}_n), \cdot)\). Using Eqn. (34), we can restrict ourselves to the structure of \( U(\mathbb{Z}_p^\alpha) \), where \( p \) is a prime. Let us first discuss the case \( \alpha = 1 \). We first prove that \( \mathbb{Z}_p \) is a finite field.

**Proposition 9 :** \((\mathbb{Z}_p, +, \cdot)\) is a field for any prime \( p \).

**Proof:** We have to show that every nonzero element in \( \mathbb{Z}_p \) is invertible. If \( \bar{a} \neq 0 \), we have \((a, p) = 1\). The result now follows from Proposition 3. ■

**Proposition 10 :** If \( \mathbb{F} \) is a finite field, then \( \mathbb{F}^* = \mathbb{F} \setminus \{0\} \) is a cyclic group.

You will see a proof of this in Unit 12. Since \( U(\mathbb{Z}_p) \) is cyclic, it generated by some \( \bar{a} \in U(\mathbb{Z}_p) \). So, the following definition makes sense.

**Definition 4 :** Let \( p \) be a prime. We call \( a \in \mathbb{Z} \) a **primitive root** \( \mod p \) if \( U(\mathbb{Z}_p) = \langle \bar{a} \rangle \).

Note that, if \( a \in \mathbb{Z} \) is primitive root \( \mod p \), all the primitive roots \( \mod p \) are given by \( \{ a^i \mid (i, p-1) = 1 \} \). So, if we find one primitive root \( \mod p \), we can find all the primitive roots \( \mod p \). How do we find a primitive root \( \mod p \) when \( p \) is an odd prime? A straightforward method is to start from 2 and check the order of all the elements to see if any of them has order \( p-1 \). Of course we omit squares like 4, 9 etc. because they cannot be primitive roots \( \mod p \). In general we can omit any power \( a^i \mod p \) if \( (i, p-1) > 1 \). (Why?)

**Lemma 2 :** Let \( G \) be a finite cyclic group of order \( n \) and let \( g \in G \). Suppose \( n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \), where \( p_1, p_2, \ldots, p_k \) are distinct primes \( e_1, e_2, \ldots, e_k \in \mathbb{N} \). Write \( n_j = \frac{n}{p_j} \) and \( g_j = g^{p_j} \) for \( j = 1, \ldots, k \). Then, \( g \) has order \( n \) if and only if \( g_j^{p_j^{-1}} \neq 1 \) for \( j = 1, 2, \ldots, k \).

**Proof:** let \( o(g) \) denote the order of \( g \in G \). In general, we have
\[
o \left( g^k \right) = \frac{o(g)}{(k, o(g))}.
\]
Suppose \( g \) has order \( n \). Use Eqn. (40) to show that \( g_j = g^{p_j} \) has order \( p_j^{e_j} \). So, \( g_j^{p_j^{-1}} \neq 1 \).

Conversely, suppose that \( g_j^{p_j^{-1}} \neq 1 \) for each \( j \). We have \( o(g) \mid n \) since \( g^n = 1 \).

Further, \( g_j \) has order \( p_j^{e_j} \). Since \( o(g_j) = o \left( g^{p_j} \right) \) and \( o \left( g^k \right) \mid o(g) \) for all \( k \in \mathbb{N} \), from Eqn. (40), it follows that \( p_j^{e_j} \mid o(g) \). Since \( p_j^{e_j}, p_2^{e_2}, \ldots \) are pairwise coprime, it follows that \( n \mid o(g) \). Since \( n \mid o(g) \) and \( o(g) \mid n \), it follows that \( o(g) = n \). ■
The following algorithm uses Lemma 2 to check whether an element \( g \) in a cyclic group generates \( G \) or not.

1. Factorise \( n \): 
   \[ n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}. \]

2. Set \( n_i = \prod_{j \neq i} p_j^{e_j} = \frac{n}{p_i^{e_i}}. \) Find \( g_i = g^{n_i}, 1 \leq i \leq k. \) If \( g_i = 1 \) for some \( i \), \( g \) is not a generator of \( G \).

3. If none of the \( g_i \) are one, compute \( g_i^{p_i-1}. \) If any of them is 1, \( g \) is not a generator of \( G \) and we are done. If none of them is one, \( g \) is a generator of \( G \) and we are done.

Let us look at an example.

**Example 13:** Find a primitive root \((\text{mod } 23)\).

**Solution:** We first check if \( 2 \) \((\text{mod } 23)\) is a primitive root. We have 
\[ o(U(\mathbb{Z}_{23})) = 22 = 2 \cdot 11. \] So,
\[ p_1 = 2, p_2 = 11, e_1 = 1, e_2 = 1, n_1 = 11, n_2 = 2. \]

We have \( g_1 = 2^{11}. \) Let us compute \( g^{11}. \) We use a little trick called ‘square and multiply’ to speed up our computations. If we write 11 in binary notation,
\[ 11 = 1 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3, \]
so
\[ g^{11} = g^{1+1\cdot2+0\cdot2^2+1\cdot2^3} = g \cdot g^2 \cdot g^8. \]

We repeatedly square \( 2 \) \((\text{mod } 23)\) to get
\[ 2^2 = 4, 2^4 = 16, 2^8 \equiv 16^2 \equiv 3 \pmod{23}. \]

So,
\[ 2^{11} \equiv 2 \cdot 2^2 \cdot 2^8 \equiv 2 \cdot 4 \cdot 3 \equiv 24 \equiv 1 \pmod{23}. \]

So, \( o(2) \mid 11 \) and \( o(U(\mathbb{Z}_{23})) \) is 1 or 11. Since \( o(2) \neq 1 \), we have \( o(2) = 11. \) Since \( o(2) \neq 22 \) we conclude that 2 is not a primitive root \((\text{mod } 23)\).

Let us try 3. We calculate \( g_1 = 3^{11}. \) Repeatedly squaring 3, we get
\[ 3^2 = 9, 3^4 \equiv 12 \pmod{23}, 3^8 \equiv 6 \pmod{23} \]
\[ 3^{11} \equiv 3 \cdot 3^2 \cdot 3^8 \equiv 3 \cdot 9 \cdot 6 \equiv 1 \pmod{23}. \]

So, \( o(3) = 11 \) and 3 is not a primitive root.

Let us try 5 next. We calculate \( g_1 = 5^{11}. \) We have
\[ 5^2 = 25 \equiv 2 \pmod{23}, 5^4 \equiv 2^2 \equiv 4 \pmod{23}, 5^8 \equiv 16 \pmod{23} \]
\[ 5^{11} \equiv 5 \cdot 2 \cdot 16 \equiv 22 \pmod{23}. \]

So, \( 511 \equiv 5 \cdot 2 \cdot 16 \equiv 22 \pmod{23}. \) So, \( g_1^{p_1-1} = 22^{2^0} = 22 \not\equiv 1 \pmod{23}. \)
We have \( g_2 = g_2^{n^2} = 5^2 = 25 \equiv 2 \pmod{23} \). Also,
\[
g_2^{p_{11}^{\alpha_1 - 1}} = 2^{5^0} = 2 \not\equiv 1 \pmod{23}.
\]
So, 5 is a primitive root \( \pmod{23} \).

\[\text{**} \]

Here is an exercise for you.

E14) Find a primitive root of \( \pmod{43} \).

E15) If \( p \) is a prime of the form \( 4t + 1 \), show that \( a \) is a primitive root \( \pmod{p} \) if and only if \( -a \) is a primitive root \( \pmod{p} \).

We briefly describe the structure of \( U(\mathbb{Z}_n) \) in general without proofs because the proofs are not particularly instructive. From Eqn. (35), we need to find only the structure of \( U(\mathbb{Z}_{p^\alpha}) \) for \( \alpha \geq 2 \), where \( p \) is a prime.

**Proposition 11**: If \( p \) is an odd prime, \( U(\mathbb{Z}_{p^\alpha}) \) is cyclic for \( \alpha \geq 1 \). Further

\[
U(\mathbb{Z}_{2^\alpha}) = \begin{cases} 
\langle 1 \rangle, & \text{if } \alpha = 1 \\
\langle -1 \rangle, & \text{if } \alpha = 2 \\
\langle -1 \rangle \times \langle 5 \rangle, & \text{if } \alpha \geq 2
\end{cases}
\]

We close this section here. In the next section, we will discuss the solutions of quadratic congruences, i.e., congruences of the type \( x^2 \equiv a \pmod{n} \).

**10.4 THE QUADRATIC RECIPROCITY LAW**

In this section, we will prove the quadratic reciprocity law which was proved by Gauss in his path breaking work *Disquisitiones Arithmeticae*. When he did this work, he was not even 18 years old. The statement of this result was known to Euler, Legendre and other mathematicians, but none of them were able to prove it. Gauss called the result ‘Theorem Aureum’ meaning ‘Golden theorem’. He gave several proofs of the theorem. Many proofs were given by others also. The proof we will give is due to Eisenstein, one of the gifted students of Gauss.

(Eisenstein, like Galois, Abel, Riemann and others died at a young age.)

Let us consider the congruence \( x^2 \equiv m \pmod{n} \) where \( m \) and \( n \) are odd. Suppose

\[
n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}
\]

where \( p_i \) are prime and \( a_i \in \mathbb{N} \). Then, \( x_0 \) is a solution to the congruence \( x^2 \equiv m \pmod{n} \) if and only if \( x_0 \) is a solution to the congruences

\[
\begin{align*}
x^2 &\equiv m \pmod{p_1^{a_1}} \\
x^2 &\equiv m \pmod{p_2^{a_2}} \\
\vdots \\
x^2 &\equiv m \pmod{p_k^{a_k}}
\end{align*}
\]

The following result tells us that to solve the congruences in Eqn. (41), we need to find solutions only for prime modulus:
Proposition 12: Let $p$ be an odd prime and suppose that $a \in \mathbb{Z}$ is such that $(a, p) = 1$. If $x^2 \equiv a \pmod{p}$ has a solution, then $x^2 \equiv a \pmod{p^k}$ also has a solution for $k \in \mathbb{N}, k \geq 2$.

Note that, the result is no longer true if $p = 2$. (See Exercise 16.)

We can prove Proposition 12 by starting with a root of $x^2 \equiv a \pmod{p}$ and repeatedly applying the following lemma.

Lemma 3: Let $k \in \mathbb{N}, k \geq 1$ and $p$ be an odd prime. If $\alpha \in \mathbb{Z}$ is a solution to the congruence $x^2 \equiv a \pmod{p^k}$, where $(a, p) = 1$, there is an $\alpha' \in \mathbb{Z}$ such that $\alpha \equiv \alpha' \pmod{p^k}$ and $\alpha'^2 \equiv a \pmod{p^{k+1}}$.

Proof: If $\alpha^2 \equiv a \pmod{p^{k+1}}$, we can take $\alpha' = \alpha$ and we are done. So, let us assume $\alpha^2 \not\equiv a \pmod{p^{k+1}}$, i.e. $p^k \mid (\alpha^2 - a)$, $p^{k+1} \nmid (\alpha^2 - a)$. Therefore,

$$\alpha^2 - a = u^k \text{ with } (u, p) = 1 \quad \ldots (42)$$

Consider the ‘Taylor series expansion’ of $x^2 - a$ about $\alpha$:

$$x^2 - a = \alpha^2 - a + 2\alpha(x - \alpha) + (x - \alpha)^2 \quad \ldots (43)$$

We need to find an $\alpha'$ such that

$$\alpha^2 - a + 2\alpha(\alpha' - \alpha) + (\alpha' - \alpha)^2 \equiv 0 \pmod{p^{k+1}} \quad \ldots (44)$$

$$\alpha' \equiv \alpha \pmod{p^k} \quad \ldots (45)$$

If $\alpha' = \alpha + v p^k$ then Eqn. (45) is satisfied. So, if we can find a $v$ such that $\alpha' = \alpha + v p^k$ satisfies Eqn. (44), we are done. Let us put $\alpha' = \alpha + v p^k$ in Eqn. (44) and see if we can solve for $v$. Note that $p^{2k} \mid (\alpha' - \alpha)^2$, so $p^{k+1} \mid (\alpha' - \alpha)^2$. So, Eqn. (44) reduces to

$$u^k + 2\alpha v p^k \equiv 0 \pmod{p^{k+1}} \quad \ldots (46)$$

where $u$ is defined as in Eqn. (42). From the congruence in Eqn. (46) it follows that

$$u + 2\alpha v \equiv 0 \pmod{p} \text{ or } 2\alpha v \equiv -u \pmod{p} \quad \ldots (47)$$

We can solve the last equation for $v$ since $(2\alpha, p) = 1$. This is because, if $p \mid \alpha$, from the congruence $\alpha^2 \equiv a \pmod{p^k}$, it will follow that $p \mid a$, a contradiction to our choice of $a$.

Because of Proposition 12, we can restrict ourselves to finding the solutions of $x^2 \equiv a \pmod{p}$ where $p$ is a prime and $(a, p) = 1$.

Definition 5 (Quadratic Residue): We say that $a \in \mathbb{Z}$, $(a, p) = 1$, is a quadratic residue modulo $p$ if the congruence $x^2 \equiv a \pmod{p}$ has a solution.

Note that $a \in \mathbb{Z}$, $(a, p) = 1$ is a quadratic residue if $\bar{a}$ is a square in $\mathbb{Z}_p^*$
**Definition 6 (Legendre Symbol):** Let \( p \) be an odd prime and \( a \in \mathbb{Z} \) be coprime to \( p \). Then, the Legendre Symbol \( \left( \frac{a}{p} \right) \) is defined by

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1, & \text{if } a \text{ is a quadratic residue (mod } p) \\
-1, & \text{if } a \text{ is not a quadratic residue (mod } p). 
\end{cases}
\]  

\[\text{... (48)}\]

**Remark 3:** Note that \( \left( \frac{a}{p} \right) \) is 1 or -1 according as \( a \) is a square in \( \mathbb{Z}_p^* \) or not.

So, \( \left( \frac{a}{p} \right) \) is determined by the residue class of a modulo \( p \). Therefore,

\[
\left( \frac{a}{p} \right) = \left( \frac{a'}{p} \right) \text{ if } a \equiv a' \pmod{p}.
\]

In the next example, we will calculate all the quadratic residues (mod 7).

**Example 14:** Find the quadratic residues modulo 7.

**Solution:** From the definition, it is clear that whether \( a \in \mathbb{Z} \) is a quadratic residue modulo 7 or not depends only on whether its residue class modulo 7 is a square in \( \mathbb{Z}_7^* \) or not. So, let us first find all the squares in \( \mathbb{Z}_7^* \).

\[
\begin{array}{cccccc}
\bar{a} & 1 & 2 & 3 & 4 & 5 \\
\bar{a}^2 & \bar{1} & \bar{4} & \bar{2} & \bar{2} & \bar{4} & \bar{1}
\end{array}
\]

So, \( a \in \mathbb{Z}, (a, 7) = 1 \) is a quadratic residue modulo 7 if and only if \( \bar{a} = \bar{1}, \bar{2}, \bar{4} \).

***

In the example above, we computed all the squares modulo 7 to find the quadratic residues (mod 7). This is a very tedious procedure if the prime \( p \) is large. There is a simple criterion due to Euler that helps us to check whether \( a \) is a quadratic residue modulo \( p \) or not.

**Theorem 3 (Euler’s Criterion):** If \( p > 2 \) is any prime and \( a \in \mathbb{Z}, (a, p) = 1 \), then

\[
a^{(p-1)/2} \equiv \left( \frac{a}{p} \right) \pmod{p} \quad \text{... (49)}
\]

In particular, \( a \mapsto \left( \frac{a}{p} \right) \) induces a group homomorphism \( \mathbb{Z}_p^* \longrightarrow \{1, -1\} \).

To prove this we need the following fact about cyclic groups.

**Lemma 4:** Let \( G \) be a cyclic group of order \( n \) and suppose \( d \mid n \). Then, \( G \) has a unique subgroup of order \( d \) given by

\[
\left\{ x \in G \mid x^d = 1 \right\} \quad \text{... (50)}
\]

Further,

\[
\left\{ x \in G \mid x^d = 1 \right\} = \left\{ x^{\bar{a}} \mid x \in G \right\} \quad \text{... (51)}
\]

We ask you to prove the lemma in Exercise 17.
Proof of Euler’s Criterion: Note that $x \mapsto x^n$ is a group homomorphism in any abelian group. Consider the homomorphism $f: \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$ given by $x \mapsto x^{\frac{p-1}{2}}$.

The group $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1$. We have $\left( x^{\frac{p-1}{2}} \right)^2 = 1$, so $x^{\frac{p-1}{2}}$ is in the unique subgroup of order 2 of $\mathbb{Z}_p^*$, namely $\{1, -1\}$. In other words, $x^{\frac{p-1}{2}} = \pm 1$. The result in Eqn. (49) will follow if we show that $f(a) = 1$ if $a$ is a quadratic residue and it is $-1$ if it is a quadratic non-residue. Since we already have $f(a) = a^{\frac{p-1}{2}} \in \{1, -1\}$ it is enough to show that the kernel of $f$ is precisely $\{ x^2 \mid x \in \mathbb{Z}_p^* \}$. If we apply Lemma 4 with $n = p - 1$ and $d = \frac{p-1}{2}$ we have

$$\left\{ x \in \mathbb{Z}_p^* \mid x^{\frac{p-1}{2}} = 1 \right\} = \left\{ x^2 \mid x \in \mathbb{Z}_p^* \right\}$$

So, the kernel of $f$ is $\{ x^2 \mid x \in \mathbb{Z}_p^* \}$.

We have $$(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p}$$ since $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$. The fact that $a \mapsto \left( \frac{a}{p} \right)$ is a homomorphism follows from Eqn. (49).

Let us now look at an example that explains how to use Eqn. (49) for finding the Legendre symbol.

**Example 15:** Find the following Legendre symbols:

a) $\left( \frac{3}{7} \right)$
b) $\left( \frac{19}{41} \right)$
c) $\left( \frac{6}{11} \right)$

**Solution:**

a) We have $3^{\frac{7-1}{2}} \equiv 3^3 \equiv 6 \equiv -1 \pmod{7}$. So, $\left( \frac{3}{7} \right) = -1$.

b) We have to find $19^{\frac{41-1}{2}} \equiv 19^{20} \pmod{41}$. We have $20 = 2^1 + 2^2 + 2^4 + 1 + 23 + 0 + 2^4 + 1$. Using the ‘square and multiply trick’ we used earlier, we have

$$19^2 = 361 \equiv 33 \pmod{41}$$
$$\therefore 19^4 \equiv 33^2 = 1089 \equiv 23 \pmod{41}$$
$$\therefore 19^8 \equiv 23^2 = 529 \equiv 37 \pmod{41}$$
$$\therefore 19^{16} \equiv 37^2 = 1369 \equiv 16 \pmod{41}$$
$$\therefore 19^{20} = 19^{16} 19^4 \equiv 16.23 \equiv 40 \equiv -1 \pmod{41}$$

So, $\left( \frac{19}{41} \right) = -1$.

c) We have $\left( \frac{6}{11} \right) = \left( \frac{2}{11} \right) \left( \frac{3}{11} \right)$. (Recall that $a \mapsto \left( \frac{a}{p} \right)$ is a group homomorphism from $\mathbb{Z}_p^*$ to $\{1, -1\}$.) We have $2^5 = 32 \equiv -1 \pmod{11}$. So, $\left( \frac{2}{11} \right) = -1$. Also, $5 = 1 \cdot 1 + 2 \cdot 0 + 2^2 \cdot 1$. We have $3^2 = 9 \pmod{11}$,
\[3^4 = 81 \equiv 4 \pmod{11}\]. So, \[3^5 \equiv 3 \cdot 3^4 = 3 \cdot 4 \equiv 1 \pmod{11}\]. So, 
\[\left(\frac{6}{11}\right) = -1.\]
Of course, we can evaluate \(6^5 \pmod{11}\) directly also.

***

The following exercises gives you some practice in finding the Legendre symbol. Also, you will find an outline of the proof of Lemma 4 in the exercises. Try these exercises now.

E16) Prove that Proposition 12 is not true for \(p = 2\).

E17) Prove Lemma 4 as follows:
   a) Prove that \(\{x \mid x^d = 1\}\) has order \(d\). Deduce that this is the unique subgroup of order \(d\).
   b) Show that \(\{x^n \mid x \in G\}\) is a group of order \(d\). Deduce Eqn. (51).

E18) Find the following Legendre symbols:
   a) \(\left(\frac{5}{11}\right)\)
   b) \(\left(\frac{15}{19}\right)\)

Note that, the ring homomorphism \(\psi : \mathbb{Z} \rightarrow \mathbb{Z}_n\) induces a ring homomorphism \(\tilde{\psi} : \mathbb{Z}[x] \rightarrow \mathbb{Z}_n[x]\) given by
\[\tilde{\psi} \left( \sum a_i x^i \right) = \sum \psi(a_i) x^i\]

If \(p(x) \in \mathbb{Z}\), we will call \(\tilde{\psi}(p(x))\) the reduction of \(p(x)\) modulo \(n\).

Consider the polynomial \(x^2 - 7\). If we reduce it modulo 3, this polynomial becomes \(x^2 - 1\). Since 1 is a quadratic residue modulo 3, this polynomial splits into linear factors in the field \(\mathbb{Z}_p\). On the other hand, if we reduce the polynomial modulo 5, the polynomial becomes \(x^2 - 2\) and this does not split into linear factors because \(\left(\frac{2}{5}\right) \equiv 2 \cdot 2 \equiv 4 \equiv -1 \pmod{5}\), and so \(\left(\frac{2}{5}\right) = -1\).

We have the following question: Is it possible to describe all the primes \(p\) such that \(x^2 - 7\) splits into linear factors modulo \(p\)? More generally, given a prime \(q\), is it possible to describe all the primes \(p\) such that \(x^2 - q\) splits into linear factors modulo \(p\)? The quadratic reciprocity law helps us to answer the question when \(p\) is an odd prime.

Theorem 4 (Quadratic Reciprocity): If \(p\) and \(q\) are odd primes,
\[
\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad \ldots (52)
\]

Remark 4: The quadratic reciprocity is stated often in the following form also.
\[
\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad \ldots (53)
\]

This follows from Eqn. (52) because \(\left(\frac{q}{p}\right) = \pm 1\).
When \( p = 2 \), we have the following result.

**Proposition 13**: If \( p \) is an odd prime, we have

\[
\left( \frac{2}{p} \right) = \frac{p^2 - 1}{8} = \begin{cases} 
1, & \text{if } p \equiv \pm 1 \pmod{8} \\
-1, & \text{if } p \equiv \pm 3 \pmod{8}
\end{cases}
\ldots (54)
\]

In other words, \( 2 \) is a quadratic residue modulo \( p \) if \( p \equiv \pm 1 \pmod{8} \) and it is a quadratic non-residue if \( p \equiv \pm 3 \pmod{8} \).

Regarding the polynomial \( x^2 + 1 \equiv 0 \pmod{p} \), we have the following result:

**Proposition 14**: If \( p \) is an odd prime, we have

\[
\left( \frac{-1}{p} \right) = \begin{cases} 
1, & \text{if } p \equiv 1 \pmod{4} \\
-1, & \text{if } p \equiv 3 \pmod{4}
\end{cases}
\ldots (55)
\]

Before we prove these results, let us look at some examples. We can simplify the computation of the Legendre symbol if we use quadratic reciprocity. Let us see how.

**Example 16**: Compute the following Legendre symbols:

i) \( \left( \frac{109}{331} \right) \)  
ii) \( \left( \frac{34}{71} \right) \)  
iii) \( \left( \frac{229}{41} \right) \)  
iv) \( \left( \frac{73}{191} \right) \)

**Solution**: 

i) We have \( \left( \frac{109}{331} \right) = (-1)^{\frac{109-1}{2} \frac{331-1}{2}} \left( \frac{331}{109} \right) = \left( \frac{4}{109} \right) = 1 \) since remainder on division of 331 by 109 is four. We have \( \left( \frac{4}{331} \right) = 1 \) since \( 2^2 = 4 \).

(Note that \( \left( \frac{a^2}{p} \right) = 1 \) for any \( a \in \mathbb{Z} \). Why?)

ii) We have \( \left( \frac{34}{71} \right) = \left( \frac{2}{71} \right) \left( \frac{17}{71} \right) \). We have \( 71 \equiv -1 \pmod{8} \), so from Proposition 13, \( \left( \frac{2}{71} \right) = 1 \). Applying quadratic reciprocity,

\[
\left( \frac{17}{71} \right) = (-1)^{17-1 \frac{71-1}{2}} \left( \frac{71}{17} \right) = \left( \frac{71}{17} \right) = \left( \frac{3}{17} \right)
\]

since \( 71 \equiv 3 \pmod{17} \). We have \( \left( \frac{3}{17} \right) = (-1)^{\frac{3-1}{2} \frac{17-1}{2}} \left( \frac{17}{3} \right) = \left( \frac{2}{3} \right) = -1 \). So,

\[
\left( \frac{34}{71} \right) = \left( \frac{2}{71} \right) \left( \frac{17}{71} \right) = -1.
\]

iii) Since the number at the top is bigger than the number at the bottom we divide 229 by 41 to get the remainder 24. So, we have

\[
\left( \frac{229}{41} \right) = \left( \frac{24}{41} \right) = \left( \frac{3 \cdot 8}{41} \right) = \left( \frac{2}{41} \right) \left( \frac{4}{41} \right) \left( \frac{3}{41} \right) = \left( \frac{2}{41} \right) \left( \frac{3}{41} \right)
\]

since, 4 being a square, \( \left( \frac{4}{41} \right) = 1 \). Since \( 41 \equiv 1 \pmod{8} \), from
Proposition 13, it follows that \( \left( \frac{2}{41} \right) = 1 \). So,

\[
\left( \frac{229}{41} \right) = \left( \frac{3}{41} \right) = (-1)^{\frac{3-1}{2} \cdot \frac{41-1}{2}} \left( \frac{41}{3} \right) = \left( \frac{41}{3} \right) = \left( \frac{2}{3} \right) \equiv 2 \equiv -1 \pmod{3}.
\]

So, \( \left( \frac{229}{41} \right) = -1 \).

iv) We have

\[
\left( \frac{73}{191} \right) = (-1)^{\frac{73-1}{2} \cdot \frac{191-1}{2}} \left( \frac{191}{73} \right) = \left( \frac{45}{73} \right) = \left( \frac{9}{73} \right) \left( \frac{5}{73} \right) = \left( \frac{5}{73} \right) = (-1)^{\frac{5-1}{2} \cdot \frac{73-1}{2}} \left( \frac{73}{5} \right) = \left( \frac{3}{5} \right) \equiv 3 \equiv 9 \equiv -1 \pmod{5}.
\]

So, \( \left( \frac{73}{191} \right) = -1 \).

***

Try the following exercise to check your understanding of Example 16:

E19) Compute the following Legendre symbols:

i) \( \left( \frac{109}{347} \right) \)  
ii) \( \left( \frac{71}{107} \right) \)  
iii) \( \left( \frac{41}{61} \right) \)  
iv) \( \left( \frac{97}{239} \right) \)

Let us now go back to the original question that motivated our discussion on quadratic reciprocity, namely, given \( a \in \mathbb{Z} \), \( a \) not a square, the description of primes \( p \) such that \( a \) is a square \( \pmod{p} \).

Example 17: Describe the primes \( p \) for which \( x^2 - 7 \) splits into linear factors \( \pmod{p} \).

Solution: For \( p = 2 \), we get the polynomial \( x^2 - 7 \) when we reduce \( x^2 - 7 \) modulo 2 and \( x^2 - T = (x - T)^2 \).

Let \( p \) be any odd prime. Using Eqn. (53), we have

\[
\left( \frac{7}{p} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{p}{7} \right) = \left( \frac{(-1)^{p-1}}{2} \right) \left( \frac{p}{7} \right) = \left( \frac{-1}{2} \right) \left( \frac{p}{7} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{p}{7} \right) \ldots (56)
\]

We want to know the primes for which the RHS of Eqn. (56) is 1. It is 1 if both \( (-1)^{\frac{p-1}{2}} \) and \( \left( \frac{p}{7} \right) \) are \(-1\) or both are 1.

Let us first consider the case where \( (-1)^{\frac{p-1}{2}} = 1 \) and \( \left( \frac{p}{7} \right) = 1 \). From Proposition 14 we must have \( p \equiv 1 \pmod{4} \). Also, from the table of squares in Example 14 we have \( p \equiv 1, 2 \) or \( 4 \pmod{7} \). So, \( p \) should satisfy one of the following set of congruences:

\[
p \equiv 1 \pmod{4} \quad p \equiv 1 \pmod{4} \quad p \equiv 1 \pmod{4} \\
p \equiv 1 \pmod{7} \quad p \equiv 2 \pmod{7} \quad p \equiv 4 \pmod{7}
\]
As we saw in the previous section, we will first solve the congruences

\[
\begin{align*}
   x_1 &\equiv 1 \pmod{4} & x_2 &\equiv 0 \pmod{4} \\
   x_1 &\equiv 0 \pmod{7} & x_2 &\equiv 1 \pmod{7}
\end{align*}
\]

The solutions are \(x_1 = 21\) and \(x_2 = 8\). So, the solution of the congruences

\[
\begin{align*}
   p &\equiv 1 \pmod{4} \\
   p &\equiv 1 \pmod{7}
\end{align*}
\]

is \(x_1 + x_2 = 29 \equiv 1 \pmod{28}\). Here is the complete table:

<table>
<thead>
<tr>
<th>Congruences</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>(p \equiv 1 \pmod{4})</td>
<td>(p \equiv 1 \pmod{7})</td>
</tr>
<tr>
<td>(p \equiv 1 \pmod{4})</td>
<td>(p \equiv 2 \pmod{7})</td>
</tr>
<tr>
<td>(p \equiv 1 \pmod{4})</td>
<td>(p \equiv 4 \pmod{7})</td>
</tr>
</tbody>
</table>

The other possibility is \((-1)_{p-1}^{p} = -1\) and \(\left(\frac{p}{7}\right) = -1\). In this case \(p \equiv 3 \pmod{4}\) and \(p \equiv 3, 5\) or \(6 \pmod{7}\). As before, this leads to the following set of congruences:

\[
\begin{align*}
   p &\equiv 3 \pmod{4} \\
   p &\equiv 3 \pmod{7} \\
   p &\equiv 5 \pmod{7} \\
   p &\equiv 6 \pmod{7}
\end{align*}
\]

Here is the complete table:

<table>
<thead>
<tr>
<th>Congruences</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>(p \equiv 3 \pmod{4})</td>
<td>(p \equiv 3 \pmod{7})</td>
</tr>
<tr>
<td>(p \equiv 3 \pmod{4})</td>
<td>(p \equiv 5 \pmod{7})</td>
</tr>
<tr>
<td>(p \equiv 3 \pmod{4})</td>
<td>(p \equiv 6 \pmod{7})</td>
</tr>
</tbody>
</table>

So, \(x^2 - 7\) splits completely modulo \(p\) for an odd prime \(p\) if \(p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}\).

***

**Remark 5**: If we don’t have Eqn. (56) to check whether \(x^2 - 7\) splits into linear factors modulo a prime \(p\), we will be forced to find \(\left(\frac{7}{p}\right)\) for each \(p\). However, with the help of Eqn. (56) we are able to reduce this to checking whether \(p\) is in one of the finitely many residue classes modulo \(p\), which is much easier to do!

For example, if we want to check whether \(x^2 - 7\) splits in 263081503 or not, we need not compute \(\frac{7^{263081503-1}}{2} = 7^{131540751} \pmod{263081503}\). We find that \(263081503 \equiv 27 \pmod{28}\) and 27 figures in the list of residue classes we have obtained in Example 17. So, \(x^2 - 7\) splits into linear factors modulo 263081503!
Let us now prove quadratic reciprocity. The proof is along the lines of a proof of Eisenstein presented in the book *Course in Arithmetic* by J. P. Serre, pages 9–10. For proving quadratic reciprocity, we need some preliminary results.

Let $p$ be a prime. Let $S$ be any set such that $\mathbb{Z}_p^*$ is the disjoint union of $S$ and $-S$, where $-S = \{-s|s \in S\}$. The set $\{1, 2, \ldots, \frac{p-1}{2}\}$ has this property. So, we will choose $S = \{1, 2, \ldots, \frac{p-1}{2}\}$. For $s \in S$ and $a \in \mathbb{Z}_p^*$, either $sa$ or $-sa$ is in $S$. So, we can write $sa = e_s(a)s_a$ where $e_s(a) = \pm 1$ and $s_a \in S$. Note that $e_s(a) = 1$ if $as \in S$ and $e_s(a) = -1$, if $as \in -S$. For example, let us take $p = 7$, $S = \{1, 2, 3\}$.

If $a = 6$, $s = 3$, $sa = 18 \equiv 4 \equiv 3 \equiv (1)3 \pmod{7}$. So, $e_3(6) = 1$ and $6 \equiv 3$ in this case.

**Proposition 15 (Gauss’ Lemma):** For any prime $p$ and $a \in \mathbb{Z}$, $p \nmid a$

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a) \quad \ldots (57)$$

**Proof:** If $s$ and $s'$ are two distinct elements of $S$, then $s \neq s'$. If $s = s'$, then $e_s(\alpha)s = e_{s'}(\alpha)s'$ or $e_s(\alpha)s = e_{s'}(\alpha)s'$. Therefore, $s = \pm s'$, which contradicts the choice of $S$. So, $s \mapsto s_a$ is a bijection of $S$ to itself. Multiplying the equalities $\alpha s = e_s(\alpha)s$, we get

$$\prod_{s \in S} s = \left(\prod_{s \in S} e_s(\alpha)\right) \prod_{s \in S} s = \left(\prod_{s \in S} e_s(\alpha)\right) \prod_{s \in S} s$$

Hence

$$\prod_{s \in S} s = \left(\prod_{s \in S} e_s(\alpha)\right) \prod_{s \in S} s$$

The result now follows from Euler’s criterion.

We need a few more auxiliary lemmas to prove the quadratic reciprocity.

**Lemma 5:** For all $n \geq 1$, we have

$$x^{2n+1} - \frac{1}{x^{2n+1}} = \left(x - \frac{1}{x}\right)^{2n+1} + \sum_{i=0}^{n-1} a_{i,n} \left(x - \frac{1}{x}\right)^{2i+1} \quad \ldots (58)$$

where $a_{i,n} \in \mathbb{Z}$.

The proof of Lemma 5 is not difficult. First, verify it for $n = 1, 2, 3$. You will be able to prove the lemma with the insight gained from this. We leave it to you as an exercise. (See Exercise 20.)

We also need the following trigonometric lemma.

**Lemma 6:** We have

$$\frac{\sin(2\ell + 1)x}{\sin x} = (-4)^{\ell} \prod_{1 \leq j \leq \ell} \left(\sin^2 x - \sin^2 \frac{2\pi j}{2\ell + 1}\right) \quad \ldots (59)$$
Proof: Let us divide Eqn. (58) by $x - \frac{1}{x}$ to get
\[
\frac{x^{2\ell+1} - \frac{1}{x^{2\ell+1}}}{x - \frac{1}{x}} = \left(x - \frac{1}{x}\right)^{2\ell} + \sum_{i=0}^{\ell-1} a_i,\ell \left(x - \frac{1}{x}\right)^{2i} .
\] . . . (60)

Let us substitute $e^{ix}$ for $x$ in Eqn. (60). Then, the LHS of Eqn. (60) becomes
\[
\frac{x^{2\ell+1} - \frac{1}{x^{2\ell+1}}}{x - \frac{1}{x}} = \frac{e^{(2\ell+1)ix} - e^{-(2\ell+1)ix}}{e^{ix} - e^{-ix}} = \frac{\sin(2\ell + 1)x}{\sin x} .
\] . . . (61)
The RHS of Eqn. (60) becomes
\[
(2i)^{2\ell}\sin^{2\ell} x + \sum_{j=1}^{\ell-1} a_j,\ell (2i)^{2j} \sin^{2j} x = (-4)^{\ell} \sin^{2\ell} x + \sum_{j=1}^{\ell-1} (-4)^{j} a_j,\ell \sin^{2j} x
\]

Let us write
\[
P(T) = (-4)^{\ell} T^{\ell} + \sum_{j=1}^{\ell-1} (-4)^{j} a_j,\ell T^j .
\] . . . (62)

Then,
\[
\frac{\sin(2\ell + 1)x}{\sin x} = P(\sin^2 x)
\] . . . (63)

So, we have
\[
P\left(\sin^2 \frac{2\pi j}{2\ell + 1}\right) = \frac{\sin(2\ell + 1)\frac{2\pi j}{2\ell + 1}}{\sin \frac{2\pi j}{2\ell + 1}} = 0 \text{ for } 1 \leq j \leq \ell
\] . . . (64)

In other words,
\[
\sin^2 \frac{2\pi j}{2\ell + 1}, 1 \leq j \leq \ell
\]
are the roots of the polynomial $P(T)$. So,
\[
P(T) = (-4)^{\ell} \prod_{j=1}^{\ell} \left( T - \sin^2 \frac{2\pi j}{2\ell + 1}\right)
\]

Setting $T = \sin^2 x$ in the last equation we get the required result.

We can now prove quadratic reciprocity.

Proof of quadratic reciprocity: Let $p$ and $q$ be distinct, odd primes. As before, let
\[
S = \left\{ 1, 2, \ldots, \frac{p-1}{2} \right\}
\]
From Proposition 15, Gauss lemma, we get
\[
\left(\frac{q}{p}\right) = \prod_{s \in S} e_s(q)
\]
From \( qs = e_s(q)s_q \), we have
\[
\sin \frac{2\pi}{p} qs = e_s(q) \sin \frac{2\pi}{p} s_q
\]
(Note that, if \( a \equiv a' \pmod{p} \), then \( \sin \frac{2\pi a}{p} = \sin \frac{2\pi a'}{p} \). This is because we can write \( a = a' + pr \) for some \( r \in \mathbb{Z} \) and so \( \sin \frac{2\pi a}{p} = \sin \left( 2\pi + \frac{2\pi a'}{p} \right) = \sin \frac{2\pi a'}{p} \).

So, it makes sense to write \( \sin \frac{2\pi s}{p} \) for \( s \in \mathbb{Z}^* \).

Multiplying these equations and taking into account that \( s \mapsto s_q \) is a bijection, we get
\[
\left( \frac{q}{p} \right) = \prod_{s \in S} e_s(q) = \prod_{s \in S} \frac{\sin \frac{2\pi qs}{p}}{\sin \frac{2\pi s}{p}}
\]

By applying Lemma 6 with \( q = 2\ell + 1 \) we can write this as
\[
\left( \frac{q}{p} \right) = \prod_{s \in S} (-4)^{\frac{s-1}{2}} \prod_{t \in T} \left( \sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q} \right) = (-1)^{\frac{(q-1)p-1}{4}} \prod_{s \in S,t \in T} \left( \sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q} \right)
\]
where \( T \) is the set \( \{ 1, 2, \ldots, \frac{q-1}{2} \} \). Interchanging the roles of \( p \) and \( q \), we obtain similarly
\[
\left( \frac{p}{q} \right) = (-1)^{\frac{(q-1)p-1}{4}} \prod_{s \in S,t \in T} \left( \sin^2 \frac{2\pi t}{q} - \sin^2 \frac{2\pi s}{p} \right)
\]

The factors giving \( \left( \frac{q}{p} \right) \) and \( \left( \frac{p}{q} \right) \) are identical up to sign. Since there are \( \frac{(p-1)(q-1)}{4} \) of these, we have
\[
\left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) (-1)^{\frac{(p-1)(q-1)}{4}}
\]

Let us now prove Proposition 13 and Proposition 14.

**Proof of Proposition 13:** We use Gauss lemma. Proposition 15 to prove this. Let us take \( a = 2 \) and \( S = \{ 1, 2, \ldots, \frac{p-1}{2} \} \). We have \( e_s(2) = 1 \) if \( 2s \leq \frac{p-1}{2} \) and \( e_s(2) = -1 \) otherwise. From this, we get \( \left( \frac{2}{p} \right) = (-1)^n(p) \) where \( n(p) \) is the number of integers \( s \) such that \( \frac{p-1}{4} < s \leq \frac{p-1}{2} \).

**Case 1:** \( p \equiv 1 \pmod{4} \). Let \( p = 1 + 4k \). Then, \( \frac{p-1}{4} = k \), \( \frac{p-1}{2} = 2k \) and \( n(p) \) is the number of \( s \) with \( k < s \leq 2k \). So, \( n(p) = k \) in this case. Therefore,
\[
\begin{align*}
n(p) \text{ is even} & \iff k \text{ is even} \iff p = 4(2m) + 1 = 8m + 1 \\
n(p) \text{ is odd} & \iff k \text{ is odd} \iff p = 4(2m + 1) + 1 = 8m + 5
\end{align*}
\]
Therefore

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1, & \text{if } p \equiv 1 \pmod{8} \\
-1, & \text{if } p \equiv 5 \pmod{8}
\end{cases}
\]

**Case 2:** \( p \equiv 3 \pmod{4} \). Let \( p = 4k + 3 \). Then, \( \frac{p-1}{4} = k + \frac{1}{2}, \) \( \frac{2}{p} = 2k + 1 \) and \( n(p) \) is the number of \( s \) with \( k + 1 \leq s \leq 2k + 1 \). So, \( n(p) = k + 1 \). Therefore,

\[
\begin{align*}
n(p) \text{ is even} & \iff k \text{ is odd} \iff p = 4(2m + 1) + 3 = 8m + 7 \\
n(p) \text{ is odd} & \iff k \text{ is even} \iff p = 4(2m) + 3 = 8m + 3
\end{align*}
\]

\[
\left( \frac{2}{p} \right) = \begin{cases} 
1, & \text{if } p \equiv 7 \pmod{8} \\
-1, & \text{if } p \equiv 3 \pmod{8}
\end{cases}
\]

To complete the proof, note that \( 7 \equiv -1 \pmod{8} \) and \( 5 \equiv -3 \pmod{8} \). ■

Let us now prove Proposition 14.

**Proof of Proposition 14:** If \(-1\) is a square in \( \mathbb{Z}_p^* \), say \( y^2 = -1 \), then \( y^4 = 1 \) and \( y^2 \neq 1 \). So, \( y \) is an element of order 4 and hence \( 4 \mid (p - 1) \), i.e. \( p \equiv 1 \pmod{4} \). Conversely, if \( p \equiv 1 \pmod{4} \), then \( p - 1 \). Since \( \mathbb{Z}_p^* \) is cyclic there is an element \( y \in \mathbb{Z}_p^* \) of order 4. Then \( y^2 \neq 1 \) since \( y \) has order 4. Also \( (y^2)^2 = y^4 = 1 \), so \( y^2 = -1 \) and so \( -1 \) is a square in \( \mathbb{Z}_p^* \). ■

---

E20) Prove Lemma 5.

E21) If \( p = 2^k + 1 \), for some \( k \geq 1 \) is a prime, show that 3 is a primitive root for \( U(\mathbb{Z}_p) \).

E22) If \( p = 8t + 3 \) is a prime such that \( q = \frac{p+1}{2} \) is also a prime, show that 2 is a primitive root for \( p \).

---

We close this section here. In the next section we will summarise our discussion in this Unit.

### 10.5 SUMMARY

In this Unit, we have discussed the following:

1. Method for solving linear congruences (modn);
2. How to use Chinese Remainder Theorem to solve simultaneous linear congruences;
3. The structure of the unit groups of the rings \( \mathbb{Z}_{p^r} \) when \( p \) is a prime.
4. How to calculate the Legendre symbol;
5. How to solve the equation \( x^2 - a = 0 \pmod{p} \), when \( p \) is a prime and \( a \) and \( p \) are odd numbers coprime to each other, using quadratic reciprocity;
10.6 SOLUTIONS/ANSWERS

E1) We have \(11 \equiv -1 \pmod{10}\). So,
\[
n = \sum_{i=0}^{k} a_i 11^i \equiv \sum_{i=0}^{k} (-1)^i a_i = a_0 - a_1 + \cdots + (-1)^k a_k
\]
We have
\[
7 - 0 + 2 - 1 + 0 - 9 = -1, \quad 7 - 0 + 2 - 1 + 0 - 9 + 1 \equiv 0 \pmod{11}
\]
So, the number is divisible by 11.

E2) Adding terms with zero coefficients if necessary, we can assume that
\[
n = \sum_{i=0}^{k} a_i 10^i, \quad m = \sum_{i=0}^{n} b_i 10^i, \quad 0 \leq a_i, b_i \leq 9 \quad \text{for} \ i = 0, 1, 2, \ldots, k
\]
Then
\[
n - m = \sum_{i=1}^{k} (a_i - b_i) 10^i + (a_0 - b_0) \equiv (a_0 - b_0) \pmod{10} \quad \text{(65)}
\]
since the sum is divisible by 10. If \(a_0 = b_0\), it follows from Eqn. (65) that
\(n \equiv m \pmod{10}\).

Conversely, if \(n \equiv m \pmod{10}\), it follows from Eqn. (65) that
\(a_0 \equiv b_0 \pmod{10}\). So, 10 divides \(|a_0 - b_0|\). Since \(0 \leq a_0, b_0 \leq 9\), it follows that \(0 \leq |a_0 - b_0| \leq 9\). (Why?) Therefore, \(a_0 = b_0\). (Why?)

E3) i) We have \(a \equiv b \pmod{n}\) is equivalent to \(\psi(a) = \psi(b)\) and
\(c \equiv d \pmod{n}\) is equivalent to \(\psi(c) = \psi(d)\). To show that
\(a + c \equiv b + d \pmod{n}\), we have to show that \(a + c = b + d\). We have
\[
\begin{align*}
\frac{a + c}{\psi(a) + \psi(c)} &= \psi(a + c) = \psi(a) + \psi(c) \\
&= \psi(b) + \psi(d) \\
&= \psi(b + d) = b + d
\end{align*}
\]
ii) This follows from the fact that \(\psi(ac) = \psi(a)\psi(c)\).

E4) If \(a \equiv b \pmod{n}\), we have \(a - b = nk\) for some \(k \in \mathbb{Z}\). Multiplying both sides by \(d\), we get \(ad - bd = nkd\), so \(ad \equiv bd \pmod{nd}\).

Conversely, if \(ad \equiv bd \pmod{nd}\), we have \(ad - bd = mnd\), \(m \in \mathbb{Z}\).

Dividing both sides of the last equation by \(d\), we get \(a - b = mn\) or
\(a \equiv b \pmod{n}\).

E5) i) In Step I, we have the pair 65, 25 and \(b = 25 \neq 0\). So, we go to Step II. We write 65 = 25 \cdot 2 + 15. We go to Step I to find (25, 15).

Again, \(b = 15 \neq 0\), so we to Step II. We write 25 = 15 \cdot 1 + 10. We go to Step I to find (15, 10).

In Step I, \(b = 10 \neq 0\), so we go to Step II. We write 15 = 10 \cdot 1 + 5. We go to Step I to find (10, 5).

In Step I, \(b = 5 \neq 0\). We go to Step II and write 10 = 5 \cdot 2 + 0. We go to Step I to find (5, 0) = 5. So, (65, 25) = 5.
ii) From \( \text{Eqn. (7)} \) we have \((-141, 93) = (141, 93) \). So, we proceed to find \((141, 93)\). In Step I, we have \( b = 93 \neq 0 \). So, we go to Step II. We write \( 141 = 93 \cdot 1 + 48 \). We go to Step I to find \((93, 48)\). In Step I, we have \((93, 48) \) and \( b = 48 \neq 0 \). We go to Step II and write \( 93 = 48 \cdot 1 + 45 \). We go to Step I to find \((48, 45)\). In Step I, we have \((48, 45) \) and \( b = 45 \neq 0 \). We go to Step II and write \( 48 = 45 \cdot 1 + 3 \) and go to Step I to find \((45, 3)\). In Step I, we have \((45, 3) \). We go to Step II and write \( 45 = 3 \cdot 15 + 0 \). We go to Step I to find \((3, 0)\). In Step I, we have \((3, 0)\), i.e. \( b = 0 \), so \( a = 3 \) is the g.c.d. Therefore, \((-141, 93) = 3\).

ii) We have \((-21, -8) = (21, 8) = (8, 21) = (21, 8) \). In Step I, we have \( b = 8 \neq 0 \). So, we go to Step II and write \( 21 = 8 \cdot 2 + 5 \). We go to Step I to find \((8, 5)\). In Step I, we have \( b = 5 \neq 0 \). So, we go to Step II and write \( 8 = 5 \cdot 1 + 3 \). We go to Step I to find \((5, 3)\). In Step I, we have \( b = 3 \neq 0 \), so we go to Step II and write \( 5 = 3 \cdot 1 + 2 \). We go to Step I to find \((3, 2)\). In Step I, we have \( b = 1 \neq 0 \), so we go to Step II and write \( 3 = 2 \cdot 1 + 1 \). We go to Step I to find \((2, 1)\). In Step I, we have \( b = 1 \neq 0 \). We go to Step II, we have \( 2 = 1 \cdot 2 + 0 \). We go to Step I to find \((1, 0)\). In Step I, \( b = 0 \) so \((21, 8) = a = 1\).

E6)  

i) The computation is given below:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>25</td>
<td>2</td>
<td>1</td>
<td>-2</td>
<td>15</td>
</tr>
<tr>
<td>25</td>
<td>15</td>
<td>1</td>
<td>-1</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>15</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>-5</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

From the fourth row, \((65, 25) = 5\), \( u = 2 \), \( v = -5 \).

ii) The computation is shown below:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>141</td>
<td>93</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>48</td>
</tr>
<tr>
<td>93</td>
<td>48</td>
<td>1</td>
<td>-1</td>
<td>2</td>
<td>45</td>
</tr>
<tr>
<td>48</td>
<td>45</td>
<td>1</td>
<td>2</td>
<td>-3</td>
<td>3</td>
</tr>
<tr>
<td>45</td>
<td>3</td>
<td>15</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

From the fourth row, \((141, 93) = 3\), \( u = 2 \) and \( v = -3 \).

iii) The computation is given below:

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>u</th>
<th>v</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>-2</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>1</td>
<td>-1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>-3</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

In the fifth row, we get \( d = 1 \), so we stop. We have \((21, 8) = 1\), \( u = 1 \) and \( v = -3 \).
iv) We compute \((63, 24)\). The computation is given below:

\[
\begin{array}{cccccc}
a & b & q & u & v & d \\
* & * & 0 & 1 & * \\
63 & 24 & 2 & 1 & -2 & 15 \\
24 & 15 & 1 & -1 & 3 & 9 \\
15 & 9 & 1 & 2 & -5 & 6 \\
9 & 6 & 1 & -3 & 8 & 3 \\
6 & 3 & 2 & -2 & 0 & 0 \\
\end{array}
\]

We have \((63, 24) = 3\) and \((-3)63 + (8)24 = 1\). So, \((3)(-63) + (8)24 = 3\).

v) We find \((170, 25)\). The computation is given below:

\[
\begin{array}{cccccc}
a & b & q & u & v & d \\
* & * & 0 & 1 & * \\
170 & 25 & 6 & 1 & -6 & 20 \\
25 & 20 & 1 & -1 & 7 & 5 \\
20 & 5 & 4 & & 0 & 0 \\
\end{array}
\]

We have, \((170, 25) = 5\) and \((-1)170 + (7)25 = 5\). So, \((1)(-170) + (-7)(-25) = 5\).

E7) i) We have to find \(\bar{3}^{-1} \mod 17\). So, we have to find \(u\) and \(v\) such that \(3u + 17v = 1\). As before, we use the extended euclidean algorithm. The computation is given below:

\[
\begin{array}{cccccc}
a & b & q & u & v & d \\
* & * & 0 & 1 & * \\
17 & 3 & 5 & 1 & -5 & 2 \\
3 & 2 & 1 & -1 & 6 & 1 \\
\end{array}
\]

We have \((-1)17 + (6)3 = 1\). So, \(3^{-1} = \bar{6}\). Multiplying both sides of the congruence \(3x \equiv 2 \mod 17\) by \(6\), we get, \(x \equiv 12 \mod 17\).

ii) Here, \((4, 18) = 2\), and \(2 \mid 6\), so this has a solution. We first divide both sides of the congruence by \(2\) to get \(2x \equiv 3 \mod 9\). We proceed as before and find \(u = -4\), \(v = 1\) satisfying \(2u + 9v = 1\). So, \(\bar{2}^{-1} = \bar{-4} = \bar{5}\). Multiplying both sides of the congruence \(2x \equiv 3 \mod 9\) by \(5\), we get \(x \equiv 15 \equiv 6 \mod 9\). From Proposition 6, it follows that \(6 + 0 \cdot 9 = 6, 6 + 1 \cdot 9 = 15\) are the solutions to the congruence \(4x \equiv 6 \mod 18\).

iii) We have \((10, 85) = 5\) and \(5 \mid 5\). We consider the congruence \(2x \equiv 1 \mod 17\). We proceed as before to find \(u = 1, v = -8\), i.e. \((1)17 + (-8)2 = 1\). So, \(\bar{2}^{-1} = \bar{-4} = \bar{5}\). Multiplying both sides of the congruence \(2x \equiv 1 \mod 17\) by \(-8\), we get \(x \equiv -8 \equiv 9 \mod 17\). So, the solutions are \(9 + 0 \cdot 17 = 9, 9 + 1 \cdot 17 = 26, 9 + 2 \cdot 17 = 43, 9 + 3 \cdot 17 = 60\) and \(9 + 4 \cdot 17 = 77\).

E8) Since \((7, 10) = 1\) and \(\phi(10) = 4\), we have \(7^4 \equiv 1 \mod 10\). Since \(323 = 4 \cdot 80 + 3\), it follows that \(7^{323} = (7^4)^{80} \cdot 7^3 \equiv 7^3 \equiv 3 \mod 10\). So, the units digit of \(7^{323}\) is \(3\).

E9) By Fermat’s little theorem, \(a^{10} \equiv 1 \mod 11\). Since \(\mathbb{Z}_{11}\) is a field, the equation \(x^2 - 1 = 0\) has only two solutions, Since \(a^5\) is a solution, \(a^5 = \pm 1\), in \(\mathbb{Z}_{11}\). So, \(11 \mid (a^5 - 1) (a^5 + 1)\).
E10) We take $n_1 = 5$, $n_2 = 7$ and $n_3 = 11$. Then

\[
\begin{align*}
N_1 &= 77 \equiv 2 \pmod{5} & 2^{-1} &= 3 \text{ in } \mathbb{Z}_5 & N_1' &= 3 \\
N_2 &= 55 \equiv 6 \pmod{7} & 6^{-1} &= 6 \text{ in } \mathbb{Z}_7 & N_2' &= 6 \\
N_3 &= 35 \equiv 2 \pmod{11} & 6^{-1} &= 6 \text{ in } \mathbb{Z}_7 & N_3' &= 6
\end{align*}
\]

So,

\[
x = a_1N_1N_1' + a_2N_2N_2' + a_3N_3N_3' = 2 \cdot 77 \cdot 3 + 4 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 = 2412
\]

The smallest non-negative solution is the smallest non-negative residue of 2412 (mod 385) which is 102.

E11) First, we convert the congruences to the standard form. We have $3^{-1} = 3$ in $\mathbb{Z}_4$. So, multiplying both sides of the first congruence by 3 we get $x \equiv 2 \pmod{4}$. We have $8^{-1} = 8$ in $\mathbb{Z}_9$. Multiplying both sides of the second congruence by 8, we get $x \equiv 5 \pmod{9}$. So, the modified set of congruences are

\[
\begin{align*}
x &\equiv 2 \pmod{4} \\
x &\equiv 5 \pmod{9} \\
x &\equiv 3 \pmod{11}
\end{align*}
\]

We have $N_1 = 99$, $N_2 = 44$ and $N_3 = 36$. We have $N_1' = 3$, $N_2' = 8$ and $N_3' = 4$. We have $x = 2 \cdot 99 + 5 \cdot 44 + 3 \cdot 36 = 2786$. Dividing by $N = 396$, the remainder is 14.

E12) Let us suppose all the cyclists cross the starting line together $x$ seconds after $t_0$. Then, the first cyclist was at the starting line at time $t_0 + 1$ and she reaches the starting line at time $x + t_0$ having completed $k_1$ rounds of the velodrome. In the total time elapsed which is $x + t_0 = (t_0 + 1) = x - 1$, she has completed $k_1$ rounds. So, $x - 1 = 4k_1$ or $x = 1 + 4k_1$. Similarly, for the second and the third cyclists we get the equations $x = 2 + 5k_2$, $x = 3 + 7k_3$. So, we need to find the smallest positive integer solution to the congruences $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$ and $x \equiv 3 \pmod{7}$. As you can easily work out, the solution is $x = 17$, i.e. the cyclists will cross the starting line together 17 seconds after $t_0$.

E13) Suppose $a = (a_1, a_2, \ldots, a_k)$ is a unit in $R$. Then, there is a $b = (b_1, b_2, \ldots, b_k \in R)$ such that

\[
ab = (a_1, a_2, \ldots, a_k) (b_1, b_2, \ldots, b_k \in R) = (1, 1, \ldots, 1) \quad \text{k times}
\]

Therefore, we have

\[
(a_1b_1, a_2b_2, \ldots, a_kb_k) = (1, 1, \ldots, 1) \quad \text{k times}
\]

or $a_ib_i = 1$ for $i = 1, 2, \ldots, k$. So, each $a_i$ is a unit in $R_i$, $i = 1, 2, \ldots, k$.

E14) We have $43 - 1 = 42 = 2 \cdot 3 \cdot 7$. So $n_1 = 21$, $n_2 = 14$ and $n_3 = 6$. Here, $e_1 = 1$, $e_2 = 1$, $e_3 = 1$. 

103
Let us first check if 2 is a primitive. So, we take $g = 2$ and calculate $g_1 = 2^{21} = 2^{21} \pmod{43}$. We have

$$21 = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4.$$ 

So,

$$2^{21} = 2 \cdot 2^2 \cdot 2^4 = 2 \cdot 2^4 \cdot 2^16.$$ 

Computing powers of 2, we get

$$2^2 \equiv 4 \pmod{43}, \ 2^4 \equiv 16 \pmod{43}, \ 2^8 \equiv 16^2 \equiv 256$$

$$\equiv 41 \equiv -2 \pmod{43}, \ 2^{16} \equiv 41^2 \equiv (-2)^2 \equiv 4 \pmod{43}.$$ 

We have

$$2^{21} = 2 \cdot 2^{2^2} \cdot 2^{2^4} = 2 \cdot 2^4 \cdot 2^{16}.$$ 

So, $g_1^{p^{e_1-1}} = (-1)^{2^0} = -1 \not\equiv 1 \pmod{43}$. We have

$$g_2 = g^{n_2} = 2^{14} = 2^2 \cdot 2^4 \cdot 2^8 \equiv 4 \cdot 16 \cdot (-2) \equiv 1 \pmod{43}.$$ 

So, $g_2^{p^{e_2-1}} = g_2 \equiv 1 \pmod{43}$. So, 2 is not a primitive root $\pmod{43}$.

Let us now check if 3 is a primitive root. We have

$$g_1 = g^{n_1} = 3^{21} = 3 \cdot 3^4 \cdot 3^{16}.$$ 

Computing powers of 3, we get

$$3^2 \equiv 9 \pmod{43}, \ 3^4 \equiv 38 \equiv -5 \pmod{54}, \ 3^8 \equiv 25 \pmod{43},$$

$$3^{16} \equiv 625 \equiv 23 \pmod{43}.$$ 

We have

$$g_1 = 3^{21} \equiv 3 \cdot (-5) \cdot 23 \equiv 42 \equiv 1 \pmod{43}.$$ 

So, $g_1^{p^{e_1-1}} \equiv 42 \not\equiv 1 \pmod{43}$.

Computing as before, We have

$$g_2 = g^{n_2} = 3^{14} \equiv 36 \pmod{43}, \ g_2^{p^{e_2-1}} = g_2 \equiv 36 \not\equiv 1 \pmod{43}.$$ 

We have $g_3 = 3^6 \equiv 41$, $g_3^{p^{e_3-1}} = g_3 \not\equiv 1 \pmod{43}$. Therefore, 3 is a primitive root $\pmod{43}$.

E15) Suppose $a$ is a primitive root $\pmod{p}$ and $-a$ is not a primitive root $\pmod{p}$. Then $(-a)^k = 1$ for some $k \in \mathbb{N}, k < p - 1$. It follows that $(-1)^ka^k = 1$. If $(-1)^k = 1$, then $a^k = 1$ for $k < p - 1$ and this contradicts our assumption that the order of $a$ is $p - 1$. So, we must have $(-1)^k = -1$ or $a^k = -1$. Therefore, $a^{2k} = 1$, so $p - 1$ divides $2k$ and $(p - 1)m = 2k$. So, $\frac{p - 1}{2}m = k$. Since $k < p - 1$, it follows that $m = 1$. So, $k = \frac{p - 1}{2}$ and $\frac{p - 1}{2}$ is even because $\frac{p - 1}{2} = 2t$. Therefore $(-1)^k = 1$ which is a contradiction. Since $-(-a) = a$ it follows from what we have proved that whenever $-a$ is a primitive root, a is also a primitive root.
E16) Let us take \( p = 2 \) and \( a = 5 \), \( k = 3 \) in Proposition 12. Then \( a \equiv 1 \pmod{2} \), so 1 is a solution to the congruence \( x^2 \equiv 5 \pmod{2} \). However, \( x^2 \equiv 5 \pmod{8} \) has no solution. From Proposition 11, 5 generates a subgroup of order 2. If \( b \) is such that \( b^2 \equiv 5 \pmod{8} \), then from Proposition 11, then it will have order 4. This is not possible because \( \mathbb{U}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \).

E17) Let \( K = \{ x \in G \mid x^d = 1 \} \). Since \( G \) is cyclic, let \( G = \langle g \rangle \).

a) Suppose \( x^d = 1 \). Let \( x = g^m \), \( 0 \leq m \leq n - 1 \). Then \( x^d = g^{md} = 1 \), so \( n \mid md \) or \( \frac{n}{d} \mid m \). Let \( m = k \frac{n}{d} \). Since \( 0 \leq m < n \), \( 0 \leq k \frac{n}{d} < n \) or \( 0 \leq k < d \). So, there are at most \( d \) values for \( k \). Therefore, there are at most \( d \) elements in \( G \) satisfying \( x^d = 1 \). On the other hand \( g^\frac{n}{d} \) satisfies \( x^d = 1 \) and it generates a subgroup of order \( d \) and every \( x \) element of this group will satisfy \( x^d = 1 \). Further, if \( H \) any subgroup of \( G \) of order \( d \), every element \( x \in H \) will also satisfy \( x^d = 1 \) and so \( H \subset K \).

Since \( |H| = |K| \), \( H = K \).

b) It is a subgroup of \( K \) defined in the solution to part a). You have to prove that \( g^\frac{n}{d} \) has order \( d \). The result will then follow.

E18) a) We have to find \( 5^5 \pmod{11} \). We have

\[
5^2 = 25 \equiv 3 \pmod{11} \\
5^4 \equiv 3^2 \equiv 9 \pmod{11} \\
5^5 \equiv 9 \times 5 = 45 \equiv 1 \pmod{11}
\]

So, \( \left( \frac{5}{11} \right) = 1 \). We leave part b) to you.

E19) i) We have

\[
\binom{109}{347} = (-1)^{109-347} \binom{347}{109} = \left( \frac{20}{109} \right) = \left( \frac{4}{109} \right) \left( \frac{5}{109} \right) = \left( \frac{5}{109} \right)
\]

since \( \left( \frac{4}{109} \right) = 1 \). We have

\[
\left( \frac{5}{109} \right) = \left( \frac{109}{5} \right) = \left( \frac{4}{5} \right) = 1
\]

ii) We have

\[
\binom{71}{107} = (-1)^{71-107} \binom{107}{71} = -\left( \frac{36}{71} \right) = -1
\]

since \( \left( \frac{36}{71} \right) = 1 \).

iii) We have

\[
\binom{41}{61} = (-1)^{41-61} \binom{61}{41} = \left( \frac{20}{41} \right) = \left( \frac{4}{41} \right) \left( \frac{5}{41} \right) = \left( \frac{5}{41} \right)
\]

\[
= \left( \frac{5}{41} \right) = (-1)^{41-51} \binom{41}{5} = \left( \frac{1}{5} \right) = 1
\]
iv) We have
\[
\begin{align*}
\left( \frac{97}{239} \right) &= (-1)^{\frac{231-1}{2}} \left( \frac{239}{97} \right) = \left( \frac{239}{97} \right) = \left( \frac{45}{97} \right) \\
&= \left( \frac{9}{97} \right) \left( \frac{5}{97} \right) = \left( \frac{5}{97} \right) = (-1)^{\frac{97-1}{2}} \left( \frac{97}{5} \right) \\
&= \left( \frac{2}{5} \right) = 2^2 = 4 \equiv -1 \pmod{5}.
\end{align*}
\]

E20) **Proof:** Note that, the lemma says that \(x^{2n+1} - \frac{1}{x^{2n+1}}\) is the sum of 
\(\left(x - \frac{1}{x}\right)^{2n+1}\) with a polynomial in
\(\left(x - \frac{1}{x}\right), \left(x - \frac{1}{x}\right)^3, \ldots, \left(x - \frac{1}{x}\right)^{2n-1}\)
with integer coefficients.

We apply induction on \(n\). For \(n = 1\), we have
\[
x^3 - \frac{1}{x} = \left(x - \frac{1}{x}\right)^3 + 3 \left(x - \frac{1}{x}\right).
\]
So, the result is true for \(n = 1\).

Suppose for all \(k \leq n - 1\), we have
\[
x^{2k+1} - \frac{1}{x^{2k+1}} = \left(x - \frac{1}{x}\right)^{2k+1} + \sum_{i=0}^{k-1} a_{i,k} \left(x - \frac{1}{x}\right)^{2i+1} \ldots \text{(66)}
\]
where \(a_{i,k} \in \mathbb{Z}\).

\[
\left(x - \frac{1}{x}\right)^{2n+1} = x^{2n+1} + \sum_{i=1}^{n} (-1)^i C(2n + 1, i)x^{2n+1-i} \frac{1}{x^i}
\]
\[+ \sum_{i=n+1}^{2n} (-1)^i C(2n + 1, i)x^{2n+1-i} \frac{1}{x^i} - \frac{1}{x^{2n+1}} \]
\[\therefore x^{2n+1} - \frac{1}{x^{2n+1}} = \left(x - \frac{1}{x}\right)^{2n+1} - \sum_{i=1}^{n} (-1)^i C(2n + 1, i)x^{2n+1-2i}
\]
\[+ \sum_{i=n+1}^{2n} (-1)^i C(2n + 1, i)x^{2n+1-2i} \ldots \text{(67)}
\]

To complete the proof, we have to show that
\[
\sum_{i=1}^{n} (-1)^i C(2n + 1, i)x^{2n+1-2i} + \sum_{i=n+1}^{2n} (-1)^i C(2n + 1, i)x^{2n+1-2i} \ldots \text{(68)}
\]
is a polynomial in
\[
\left(x - \frac{1}{x}\right), \left(x - \frac{1}{x}\right)^3, \ldots, \left(x - \frac{1}{x}\right)^{2n-1}
\]
with integer coefficients.

We now group the term in the first sum corresponding to \( i = 1 \), which is 
\(-C(2n + 1, 1)x^{2n-1}\), with the term corresponding to \( i = 2n \) in the second sum which is

\[
(-1)^{2n}C(2n + 1, 2n)x^{-(2n-1)} = C(2n + 1, 2n)x^{-(2n-1)}
\]

\[
= C(2n + 1, 1)x^{-(2n-1)}
\]

since \( C(n, r) = C(n, n - r) \). We get the term

\[
C(2n + 1, 1) \left( x^{2n-1} - \frac{1}{x^{2n-1}} \right).
\]

Similarly, we group together the term corresponding to \( i = 2 \) in the first sum with the term corresponding to \( 2n - 1 \) in the second sum to get

\[
C(2n + 1, 2) \left( x^{2n-3} - \frac{1}{x^{2n-3}} \right)
\]

In general, we group the term corresponding to \( i = m \) in the first sum and the term corresponding to \( 2n - (m - 1) \) in the second sum. The term corresponding to \( i = m \) in the first sum is

\[
(-1)^{m}C(2n + 1, m)x^{2(n-m)+1}
\]

The sum corresponding to \( i = 2n - (m - 1) \) is the second term is

\[
(-1)^{2n-m+1}C(2n + 1, 2n - m + 1)x^{2n+1-(2n-m+1)}\frac{1}{x^{2n-m+1}}
\]

\[
= (-1)^{m}C(2n + 1, 2n - m + 1)x^{2n+1-(2n-m+1)-(2n-m+1)}
\]

\[
= (-1)^{m}C(2n + 1, m)x^{-(2(n-m)+1)}
\]

Grouping the terms in [Eqn. (69)] and [Eqn. (70)] together, we get the term

\[
(-1)^{m}C(2n + 1, m) \left( x^{2(n-m)+1} - x^{-(2(n-m)+1)} \right)
\]

Thus, the sum in [Eqn. (68)] equals

\[
\sum_{i=1}^{n} (-1)^i C(2n + 1, i) \left( x^{2(n-i)+1} - x^{-(2(n-i)+1)} \right)
\]

\[\ldots (71)\]

Since \( 2(n-i) + 1 \leq 2(n-1) + 1 \), by induction hypothesis, for \( i \leq n - 1 \), we get that \( x^{2(n-i)+1} - x^{-(2(n-i)+1)} \) is a polynomial in

\[
\left( x - \frac{1}{x} \right), \left( x - \frac{1}{x} \right)^3, \ldots, \left( x - \frac{1}{x} \right)^{2(n-i)+1}
\]

with integer coefficients. So, it now follows that

\[
-\sum_{i=1}^{n} (-1)^i C(2n + 1, i) \left( x^{2(n-i)+1} - x^{-(2(n-i)+1)} \right) = \sum_{i=1}^{n-1} a_{n,i} \left( x - \frac{1}{x} \right)^{2i+1}
\]

for some \( a_{n,i} \in \mathbb{Z} \). ■
E21) Note that \(| U(\mathbb{Z}_p) | = 2^{2k} \) so, if \( g \) is any primitive root for \( U(\mathbb{Z}_p) \), \( g^m \) is also a primitive root for any odd integer \( k \). So, it is enough that \( 3 = g^m \) for some odd \( k \). But, this is the same as showing \( \left( \frac{3}{p} \right) = -1 \). By the quadratic reciprocity, we have

\[
\left( \frac{3}{p} \right) = (-1)^{\frac{p-1}{2} \cdot 2^k} \left( \frac{p}{3} \right) = \left( \frac{2^{2k} + 1}{3} \right)
\]

If \( k = 1 \), we have \( 2^2 = 4 \equiv 1 \) (mod 3), so \( 2^2 + 1 \equiv 2 \) (mod 3) and \( \left( \frac{2^2 + 1}{3} \right) = -1 \). For \( k > 1 \), we have

\[
2^{2k} + 1 = \left( 2^2 \right)^{2^{k-1}} + 1 = (4)^{2^{k-1}} + 1 \equiv 2 \pmod{3}
\]

and we are done.

E22) We have \(| U(\mathbb{Z}_p) | = 2q \) where \( q \) is a prime. To show that 2 is a primitive root, we need to show that \( 2^2 \not\equiv 1 \pmod{p} \), \( 2^q \not\equiv 1 \pmod{p} \) since 2 and \( q \) are the only proper divisors of \(| U(\mathbb{Z}_p) | \). We have \( 2^2 = 4 \not\equiv 1 \pmod{3} \) because \( 4 - 1 = 3 < p \).

Let us now consider \( 2^q \). We have \( 2^q = 2 \cdot \frac{p-1}{2} = \left( \frac{2}{p} \right) \). Since \( p \equiv 3 \pmod{8} \), it follows that \( \left( \frac{2}{p} \right) = -1 \), so \( 2^q \equiv -1 \pmod{p} \).