UNIT 10 CONGRUENCES

Structure **Page No.**

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.

P. Fermat
(1601–1665)

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.

C. F. Gauss
(1777–1855)

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 $\frac{\mathbb{Z}}{\langle n \rangle}$ 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

$$\psi : \mathbb{Z} \longrightarrow \mathbb{Z}_n \qquad \ldots(1)$$

We write $\bar{a}$ for the image $\psi(a)$ of $a \in \mathbb{Z}$. Recall that $\bar{a} = \psi(a)$ 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 $\bar{a}$, the **residue class** of a. We have $\bar{a} = \bar{b}$ if and only if $a - b \in \langle n \rangle$ or equivalently, $n \mid (a - b)$. If $\bar{a} = \bar{b}$, we write $\mathbf{a \equiv b \pmod{n}}$ 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 $a_i \not\equiv a_j \pmod{n}$ 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 ψ gives us a method of translating the results about the ring $\mathbb{Z}_n$ into an assertion regarding congruences. We will frequently use ψ 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 ψ in Eqn. (1), we get the following result:

Proposition 1 : If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n} \qquad \ldots(2)$$

and

$$ac \equiv bd \pmod{n} \qquad \ldots(3)$$

. ■

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

$$10^i \equiv 1 \pmod 9 \text{ for all } i \geq 1 \qquad \ldots(4)$$

Suppose the number is $n = a_k a_{k-1} \ldots a_0$. 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.

* * *

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.

* * *

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 $76629 \equiv 3 \pmod 9$ and $1259 \equiv 8 \pmod 9$. So, $76629 \cdot 1259 \equiv 8 \cdot 3 = 24 \equiv 6 \pmod 9$. Again, using Example 1 to find the remainder on dividing 96475811 by 9, we get $96475811 \equiv 5 \not\equiv 6 \pmod 9$. 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.ds differ only by a unit and the only units in $\mathbb{Z}$ are ± 1. So, if d and d' are two g.c.ds 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

$$\bar{a}\,\bar{x} = \bar{b} \quad \ldots(9)$$

in $\mathbb{Z}_n$.

For example, finding a solution to $3x \equiv 5 \pmod{7}$ is equivalent to finding a solution to the equation $\bar{3}\bar{x} = \bar{5}$ in $\mathbb{Z}_7$.

If $\bar{a}$ is a unit in $\mathbb{Z}_n$, then $x = \bar{a}^{-1}\bar{b}$ is a solution to Eqn. (9). The next proposition tells us when is $\bar{a}$ a unit in $\mathbb{Z}_n$.

Proposition 3 : $\bar{a} \in \frac{\mathbb{Z}}{\langle n \rangle}$ 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 $ua + vn = d$. Since $(a, n) = 1$, we can find u and v such that $ua + vn = 1$. We have

$$\begin{aligned}\psi(1) = \psi(ua + vn) &= \psi(u)\psi(a) + \psi(v)\psi(n) \\ &= \psi(u)\psi(a), \text{ since } \psi(n) = \bar{0} \\ &= \bar{u}\,\bar{a} = \bar{1} \text{ since } \psi(1) = \bar{1} \text{ from the RHS}\end{aligned}$$

So, $\bar{a}\,\bar{u} = \bar{1}$. Thus, $\bar{u} = \bar{a}^{-1}$ and $\bar{a}$ is a unit in $\mathbb{Z}_n$. We leave it to you to prove that, if $\bar{a}$ is a unit in $\mathbb{Z}_n$, then $(a, n) = 1$. ■

Corollary 1 : If $(a, n) = 1$, $x \in \mathbb{Z}$ such that $\bar{x} = \bar{a}^{-1}.\bar{b}$ is a solution to the congruence $ax \equiv b \pmod{n}$.

Proof: If $x \in \mathbb{Z}$ is such that $\bar{x} = \bar{a}^{-1}\bar{b}$, then $\bar{a}\bar{x} = \bar{b}$ or $\bar{a}\bar{x} - \bar{b} = \bar{0}$ in $\mathbb{Z}_n$. In other words $\overline{ax - b} = \bar{0}$ 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 $ua + vn = 1$, then $\bar{u}$ is the inverse of $\bar{a}$. Translated in terms of congruences, this means that u is a solution to the equation $ax \equiv 1 \pmod{n}$. So, to find $\bar{a}^{-1}$, 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

$$\begin{aligned}(a, b) &= (b, a) \text{ using Eqn. (6)} \\ &= (-b, a) \text{ using Eqn. (7)}\end{aligned}$$

and $-b < 0$. If both are negative,

$$\begin{aligned}(a, b) &= (-a, b) \text{ using Eqn. (7).} \\ &= (b, -a) \text{ using Eqn. (6)} \\ &= (-b, -a) \text{ using Eqn. (7)}\end{aligned}$$

$-a$, $-b$ 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 Propostions 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

$$a_{k+1} = b_k,\ b_{k+1} = d_k, q_{k+1} = \left[\frac{a_{k+1}}{b_{k+1}}\right] = \left[\frac{b_k}{d_k}\right], d_{k+1} = b_k - q_{k+1}d_k$$

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 $b_{k+1} = d_k < b_k$ 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 $b_{k+1} = d_k = a_k - q_k b_k$. So, b_k divides $b_{k+1} - a_k$, i.e. $b_{k+1} \equiv a_k \pmod{b_k}$. 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.

* * *

Here is an exercise to check your understanding of Example 3.

E5) 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 $a_1 = b_1q_1 + d_1$. 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

$$u_{i-1}a + v_{i-1}b = d_{i-1} \quad \ldots(10)$$
$$u_ia + v_ib = d_i \quad \ldots(11)$$

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

$$\begin{aligned} a_{i-1} &= q_{i-1}b_{i-1} + d_{i-1} \\ a_i &= q_ib_i + d_i \\ a_{i+1} &= q_{i+1}b_{i+1} + d_{i+1} \quad \ldots(12) \end{aligned}$$

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

$$d_{i+1} = \left(u_{i-1} - q_{i+1}u_i\right) a + \left(v_{i-1} - q_{i+1}v_i\right) b$$

Writing

$$u_{i+1} = u_{i-1} - u_iq_{i+1} \quad \ldots(13)$$
$$v_{i+1} = v_{i-1} - v_iq_{i+1} \quad \ldots(14)$$

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 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 $u_0 = 0$, $y_0 = 1$ 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 $b_i = d_{i-1}$ and $b_1 = b$). So, our choice is not at all unnatural!

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
$a_1 = a$	$b_1 = b$	q_1	1	$-q_1$	d_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{i-1}	b_{i-1}	q_{i-1}	u_{i-1}	v_{i-1}	d_{i-1}
a_i	b_i	q_i	u_i	v_i	d_i
$a_{i+1} = b_i$					

(a) Copy b_i below a_i

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
$a_1 = a$	$b_1 = b$	q_1	1	$-q_1$	d_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{i-1}	b_{i-1}	q_{i-1}	u_{i-1}	v_{i-1}	d_{i-1}
a_i	b_i	q_i	u_i	v_i	d_i
a_{i+1}	$b_{i+1} = d_i$				

(b) Copy d_i below b_i

a	b	q	u	v	
$*$	$*$	$*$	0	1	$*$
$a_1 = a$	$b_1 = b$	q_1	1	$-q_1$	d_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{i-1}	b_{i-1}	q_{i-1}	u_{i-1}	v_{i-1}	d_{i-1}
a_i	b_i	q_i	u_i	v_i	d_i
a_{i+1}	b_{i+1}	$\boxed{q_{i+1}} = \left\lfloor \frac{a_{i+1}}{b_{i+1}} \right\rfloor$			$d_{i+1} = a_{i+1} - q_{i+1}b_{i+1}$

(c) Compute q_{i+1} and $d_i + 1$.

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
$a_1 = a$	$b_1 = b$	q_1	1	$-q_1$	d_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{i-1}	b_{i-1}	q_{i-1}	$\textcircled{u_{i-1}}$	v_{i-1}	d_{i-1}
a_i	b_i	q_i	$\boxed{u_i}$	v_i	d_i
a_{i+1}	b_{i+1}	$\boxed{q_{i+1}}$	$u_{i+1} = u_{i-1} - q_{i+1}u_i$		d_{i+1}

(d) If $d_{i+1} \neq 0$, multiply the numbers in the squares and subtract from the circled number to compute u_{i+1}.

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
$a_1 = a$	$b_1 = b$	q_1	1	$-q_1$	d_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{i-1}	b_{i-1}	q_{i-1}	u_{i-1}	$\textcircled{v_{i-1}}$	d_{i-1}
a_i	b_i	q_i	u_i	$\boxed{v_i}$	d_i
a_{i+1}	b_{i+1}	$\boxed{q_{i+1}}$	u_{i+1}	$v_{i+1} = v_{i-1} - q_{i+1}v_i$	d_{i+1}

(e) Multiply the numbers in the squares and subtract from the circled number to compute v_{i+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 a_{i+1}, b_{i+1}, u_{i+1}, v_{i+1}, if we know the values of a_i, b_i, u_{i-1}, v_{i-1}, u_i, and v_i. Note that $q_{i+1} = \left\lfloor \frac{a_{i+1}}{b_{i+1}} \right\rfloor$. Till what point do we carry out this computation? We continue to compute till we get $d_k = 0$ or $d_k = 1$ for some natural number $k \geq 0$. 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.

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
19	7	2	1	-2	5
7					

(a) Copy b_i below a_i

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
19	7	2	1	-2	5
					5

(b) Copy d_i below b_i.

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
19	7	2	1	-2	5
7	5	1			2

(c) Compute q_2 and d_2.

a	b	q	u	v	d
$*$	$*$	$*$	⓪	1	$*$
19	7	2	$\boxed{1}$	-2	5
7	5	$\boxed{1}$	$-1 = 0 - (1 \times 1)$		2

(d) Multiply the numbers in squares and subtract from the circled number.

a	b	q	u	v	d
$*$	$*$	$*$	0	①	$*$
19	7	2	1	$\boxed{-2}$	5
7	5	$\boxed{1}$	-1	$3 = 1 - (1 \times -2)$	2

(e) Multiply the numbers in squares and subtract from the circled number.

Fig. 2: Computing the values of u and v.

We can compute the remaining rows similarly. The complete table is given below:

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
19	7	2	1	–2	5
7	5	1	–1	3	2
5	2	2	3	–8	1
2	1	2			0

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.

Aryabhatta, in Aryabhatiya (A.D. 499) gave an algorithm for integer solutions of equations of the form ax – by = n. His description of the algorithm is cryptic. Bhaskara I, in the sixth century further clarified the algorithm. He called the algorithm kuṭṭaka, meaning pulverisation. See the link below for an expository article:

Solution:

i) As before, we present the computation in tabular form:

a	b	q	u	v	d
*	*	*	0	*	*
91	35	2	1	–2	21
35	21	1	–1	3	14
21	14	1	2	–5	7
14	7	2			0

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:

a	b	q	u	v	d
*	*	*	0	1	*
62	34	1	1	–1	28
34	28	1	–1	2	6
28	6	4	5	–9	4
6	4	1	–6	11	2
4	2	2			0

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:

a	b	q	u	v	d
*	*	*	0	1	*
21	13	1	1	–1	8
13	8	1	–1	2	5
8	5	1	2	–3	3
5	3	1	–3	5	2
3	2	1	5	–8	1
2	1	2			0

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, $\overline{7}^{-1} = \overline{-8}$. We have,

$$x \equiv \overline{7}^{-1} \cdot \overline{5} \equiv \overline{-8} \cdot \overline{5} \equiv \overline{-40} \equiv \overline{17} \pmod{19}$$

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 $7 \equiv k_0 \pmod{17}$.

* * *

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, . . .,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 mechant visits the neighbouring town forms an arithmetic progression with first term 3 and common difference 5. Also, since there are 12 months in an year, we need to discard multiples of 12 to get the correct month, so we consider the solutions modulo 12.

Using extended g.c.d algorithm, we get (–2)12 + (5)5 = 1, so, $\overline{5}^{-1} = \overline{5}$ 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.

* * *

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 $\overline{a}\overline{\ell} = \overline{a}\,\overline{m}$ in $\mathbb{Z}_n$. Since (a, n) = 1, $\overline{a}$ is a unit. So, we can multiply both sides of the equation $\overline{a}\overline{\ell} = \overline{a}\,\overline{m}$ by $\overline{a}^{-1}$ to get $\overline{\ell} = \overline{m}$. 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) | b.

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.

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \qquad \ldots(15)$$

Since $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$. 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 $\phi\colon \mathbb{Z}_n \to \mathbb{Z}_{n_1}$, defined by $\phi(a + (n)) = a + (n_1)$ is a surjective ring homomorphism.

ii) We have $\ker(\phi) = \left\{ i\bar{\frac{n}{d}} \mid 0 \leq i < d \right\}$.

iii) Let $\overline{x_1} \in \mathbb{Z}_{n_1}$ be a solution to the equation $\overline{a_1}x = \overline{b_1}$ in $\mathbb{Z}_{n_1}$ and $x_0 \in \mathbb{Z}_n$ be such that $\phi(\overline{x_0}) = \overline{x_1}$, $0 \leq x_0 < n$. The solutions to the equation $ax \equiv b \pmod{n}$ are given by $x_0 + i\frac{n}{d}$, $0 \leq i \leq d$.

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 ring homomorphism. Here $(n) \subset (n_1)$

ii) Since ϕ is surjective,

$$\frac{|\mathbb{Z}_n|}{|\ker(\phi)|} = \left|\frac{\mathbb{Z}_n}{\ker(\phi)}\right| = \left|\mathbb{Z}_{n_1}\right|$$

Therefore,

$$|\ker(\phi)| = \frac{|\mathbb{Z}_n|}{\left|\mathbb{Z}_{n_1}\right|} = \frac{n}{n_1} = d$$

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 $\overline{\frac{n}{d}}$.

iii) We have $\overline{a_1}\,\overline{x_0} = \overline{a_1}\,\overline{x_1}$ 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 $a_1 d x_0' \equiv b_1 d \pmod{n_1 d}$, so x_0' is a solution to the congruence $a_1 x \equiv b_1 \pmod{n_1}$. Since $a_1 x \equiv b_1 \pmod{n_1}$ has a unique solution modulo n_1, it follows that $x_0' \equiv x_1 \pmod{n_1}$. So, $\phi(x_0 - x_0') = \overline{0}$ and $x_0' = x_0 + i\frac{n}{d}$, $0 \leq i < d$.

■

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:

a	b	q	u	v	d
*	*	*	0	1	*
13	5	2	1	–2	3
5	3	1	–1	3	2
3	2	1	2	–5	1
2	1	2			0

So, $(2)13 + (-5)5 = 1$. Thus $\overline{5}^{-1} = \overline{-5} = \overline{8}$ 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

$$U(\mathbb{Z}_n) = \left\{ \overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\} \,\middle|\, (a, n) = 1 \right\}$$

If S is a complete set of residues for $\mathbb{Z}_n$, then

$$U(\mathbb{Z}_n) = \{\overline{a} \mid a \in S, (a, n) = 1\}$$

In particular, we can take $S = \{1, 2, \ldots, n-1\}$. Then,

$$U(\mathbb{Z}_n) = \{\overline{a} \mid 1 \leq a \leq n-1, (a, n) = 1\} \quad \ldots(16)$$

Definition 3 : For $n \in \mathbb{N}$, we define

$$\phi(n) = |\{a \mid 1 \leq a \leq n-1, (a, n) = 1\}| \quad \ldots(17)$$

$\phi(n)$ is called the **Euler phi-function**.

L. Euler
(1707–1783)

(The name is pronounced as Oiler.)

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

$$\begin{aligned} 13^{99} &\equiv \left(13^{18}\right)^5 \cdot 13^9 \equiv 13^9 \pmod{19} \\ &\equiv (-6)^9 \equiv (-6)^8(-6) \equiv (36)^4 \cdot (-6) \equiv (-2)^4 \cdot (-6) \equiv 16 \cdot (-6) \\ &\equiv (-3)(-6) \equiv 18 \equiv -1 \pmod{19} \end{aligned}$$

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,

$$a^{18} \equiv b^{18} \pmod{133} \text{ or } 133 \text{ divides } a^{18} - b^{18}$$

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, $a^5 - a = (5k)\left((5k)^4 - 1\right)$. 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.

* * *

Here are some exercises for you.

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.

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.

Aryabhatta has discussed solutions of simultaneous congruences in *Āryabhatiya*, written in the 5th century A.D. He devised *kuṭṭaka* 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 $N_1 \equiv a_i \pmod{n_i}$ and $N_2 \equiv b_i \pmod{n_i}$. 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

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 3 \pmod 5$$

* * *

We will see how to solve the above congruneces this using the Chinese Remainder Theorem in Example 11.

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:

$$\left.\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_n \pmod{n_k} \end{aligned}\right\} \quad \ldots(21)$$

If x_0 and x_0' are two solutions, then $x_0 \equiv x_0' \pmod N$, where $N = n_1 n_2 \cdots n_k$.

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

$$\left.\begin{aligned} x &\equiv 0 \pmod{n_1} \\ x &\equiv 0 \pmod{n_2} \\ &\vdots \\ x &\equiv 1 \pmod{n_i} \\ x &\equiv 0 \pmod{n_{i+1}} \\ &\vdots \\ x &\equiv 0 \pmod{n_k} \end{aligned}\right\} \quad \ldots(22)$$

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 $u_i N_i + v_i n_i = 1$. This gives the congruences

$$u_i N_i \equiv 1 \pmod{n_i} \quad \ldots(24)$$
$$u_i N_i \equiv 0 \pmod{n_j} \text{ for } j \neq i \quad \ldots(25)$$

since N_i is divisible by n_j if $j \neq i$. So, $x_i = u_i N_i$ satisfies

$$x_i \equiv 0 \pmod{n_j} \text{ for } j \neq i \quad \ldots(26)$$

$$\text{and } x_i \equiv 1 \pmod{n_i} \quad \ldots(27)$$

For each i, $1 \leq i \leq k$ we find an x_i satisfying Eqn. (26) and Eqn. (27). We can use the x_is to get an x satisfying by taking $x = a_1x_1 + a_2x_2 + \cdots + a_kx_k$. So, $x \equiv a_ix_i \equiv a_i \pmod{n_i}$ 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), $x_0 \equiv a_i \pmod{n_i}$ and $x_0' \equiv a_i \pmod{n_i}$, so $x_0 \equiv x_0' \pmod{n_i}$ or $n_i \mid (x_0 - x_0')$ for each 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 $x_i \equiv 0 \pmod{n_j}$ for $j \neq i$ and $x_i \equiv 1 \pmod{n_i}$. 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 $\overline{u_i} \equiv \overline{N_i}^{-1}$ in $\mathbb{Z}_{n_i}$. So, if we choose N_i' such that $\overline{N_i'} = \overline{N_i}^{-1}$ in $\mathbb{Z}_{n_i}$, the congruence in Eqn. (24) is satisfied for $u_i = N_i'$. For all $j \neq i$, since $N_i \equiv 0 \pmod{n_j}$, $N_i'N_i \equiv 0 \pmod{n_j}$. So, we choose x_i such that $\overline{x_i} = \overline{N_i}\,\overline{N_i'}$ 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

$$N = \prod_j n_j \qquad N_i = \prod_{j \neq i} n_j \qquad \overline{N_i'} = \overline{N_i}^{-1} \text{ in } \mathbb{Z}_{n_i}$$

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 $N_iN_i' \equiv \pmod{n_i}$. 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, $N_i^{k-1} \pmod{n_i} \equiv N_i'$. 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 α is negative, add $N = \prod_i n_i$ 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 α 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_is and N_i's.

$$N_1 = 4 \cdot 5 = 20$$
$$N_2 = 3 \cdot 5 = 15$$
$$N_3 = 3 \cdot 4 = 12$$

We have $N_1 \equiv 2 \pmod 3$, $N_1^2 = 4 \equiv 1 \pmod 3$ so, we take $N_1' = 2$.

We have $N_2 \equiv 3 \pmod 4$, $N_2'^2 = 9 = 1 \pmod 5$. So, $N_2' = 3$.

We have $N_3 = 12 \equiv 5 \pmod 7$. $N_3^2 \equiv= 25 = 4 \pmod 7$, $N_3'^3 = 20 \equiv 6 \pmod 7$, $N_3'^4 = 30 \equiv 2 \pmod 7$, $N_3^5 = 10 \equiv 3 \pmod 7$ and $N_3'^6 \equiv 1 \pmod 7$. So, $N_3' = 3$.

$$\begin{aligned} x &= a_1N_1N_1' + a_2N_2N_2' + a_3N_3N_3' \\ &= 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 238 \end{aligned}$$

So, there can't be more than 60 students in the classes, we take the smallest non-negative residue of $238 \pmod{60}$ 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 $(\text{mod } n_i)$. 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_is, 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:

$$x \equiv 3 \pmod{14} \quad \ldots(28)$$
$$4x \equiv 5 \pmod{15} \quad \ldots(29)$$
$$x \equiv 9 \pmod{19} \quad \ldots(30)$$

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

$$x \equiv 3 \pmod{14} \quad \ldots(31)$$
$$x \equiv 5 \pmod{15} \quad \ldots(32)$$
$$x \equiv 9 \pmod{19} \quad \ldots(33)$$

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 $N_i \pmod{n_i}$.

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

We have, (3)285 + (–61)14 = 1, so $N_1' = 3$.

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

We have (–4)266 + (71)15 = 1, so $N_2' = -4$.

a	b	q	u	v	d
*	*	*	0	1	*
210	19	11	1	–11	1

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 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $\alpha_i \geq 1$ 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 $g_i : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_i^{\alpha_i}}$. (See third isomorphism theorem, Unit 8, Exercise 38.) Putting together the g_is, we have a ring homomorphism

$$g : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}, m \mapsto (g_1(m), g_2(m), \ldots, g_k(m)) \quad \ldots (34)$$

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 $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_k}) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$. Then,

$$g(m) = (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_k})$$

if and only if m is the solution to the congruences

$$\begin{aligned} m &\equiv a_1 \pmod{p_1^{\alpha_1}} \\ m &\equiv a_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ m &\equiv a_k \pmod{p_k^{\alpha_k}} \end{aligned}$$

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

$$g : U(\mathbb{Z}_n) \longrightarrow U\left(\mathbb{Z}_{p_1^{\alpha_1}}\right) \times U\left(\mathbb{Z}_{p_2^{\alpha_2}}\right) \times \cdots \times U\left(\mathbb{Z}_{p_k^{\alpha_k}}\right) \qquad \ldots(35)$$

Further,

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \qquad \ldots(36)$$

Also,

$$\phi(mn) = \phi(m)\phi(n) \text{ if } (m, n) = 1 \qquad \ldots(37)$$

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 $g(U(\mathbb{Z}_n)) \subset U\left(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}\right)$. Since g given by Eqn. (34) is one-one, its restriction to $U(\mathbb{Z}_n)$ is also one-one.

Let us now prove that g given by Eqn. (34), when restricted to $U(\mathbb{Z}_n)$ is also onto. Let

$$u' \in U\left(\mathbb{Z}_{p_1^{\alpha_1}}\right) \times U\left(\mathbb{Z}_{p_2^{\alpha_2}}\right) \times \cdots \times U\left(\mathbb{Z}_{p_k^{\alpha_k}}\right) \subset \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

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. $u \in U(\mathbb{Z}_n)$. 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 $U(\mathbb{Z}_n)$ and $U\left(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}\right)$. Further, we have

$$U\left(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}\right) = U\left(\mathbb{Z}_{p_1^{\alpha_1}}\right) \times U\left(\mathbb{Z}_{p_2^{\alpha_2}}\right) \times \cdots \times U\left(\mathbb{Z}_{p_k^{\alpha_k}}\right)$$

This proves that the map in Eqn. (35) is an isomorphism.

We know that $\phi(n) = |U(\mathbb{Z}_n)|$. From Eqn. (35), it follows that

$$|U(\mathbb{Z}_n)| = \prod_{i=1}^{k} \left| U\left(\mathbb{Z}_{p^{\alpha_i}}\right) \right|$$

To prove Eqn. (36) it is enough to show that

$$\left| U\left(\mathbb{Z}_{p^{\alpha}}\right) \right| = p^{\alpha-1}(p-1) = p^{\alpha} - p^{\alpha-1} \quad \ldots(38)$$

and

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1) \quad \ldots(39)$$

We have

$$n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1)$$

This proves Eqn. (39). Let us now check Eqn. (38). Now,

$$\left\{a \mid 0 \le a \le p^{\alpha} - 1, p \mid a\right\} = \left\{kp \mid 0 \le k < p^{\alpha-1}\right\}$$

and $\left|\left\{kp \mid 0 \le k < p^{\alpha-1}\right\}\right| = p^{\alpha-1}$. Note that $(a, p^{\alpha}) = 1 \Leftrightarrow p \nmid a$. So,

$$|U\left(\mathbb{Z}_{p^{\alpha}}\right)| = \left|\{a \mid 0 \le a < p^{\alpha} - 1\}\right| - |\{a \mid 0 \le a < p^{\alpha} - 1, p \mid a\}| = p^{\alpha} - p^{\alpha-1}$$

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 take 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 $U\left(\mathbb{Z}_{p^\alpha}\right)$, 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 : $\left(\mathbb{Z}_p, +, \cdot\right)$ is a field for any prime p.

Proof: We have to show that every nonzero element in 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 $U\left(\mathbb{Z}_p\right)$ is cyclic, it generated by some $\bar{a} \in U\left(\mathbb{Z}_p\right)$. 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 $U\left(\mathbb{Z}_p\right) = \langle \bar{a} \rangle$.

Note that, if $a \in \mathbb{Z}$ is primitive root (mod p), all the primitive roots (mod p) are given by $\left\{ a^i \middle| (i, p-1) = 1 \right\}$. 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 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 $n_j = \frac{n}{p^{e_j}}$ and $g_j = g^{n_j}$ for $j = 1, \ldots, k$. Then, g has order n if and only if $g_j^{p_j^{e_j - 1}} \neq 1$ for $j = 1, 2, \ldots k$.

Proof: let o(g) denote the order of $g \in G$. In general, we have

$$o\left(g^k\right) = \frac{o(g)}{(k, o(g))}. \qquad \ldots (40)$$

Suppose g has order n. Use Eqn. (40) to show that $g_j = g^{n_j}$ has order $p_j^{e_j}$. So, $g_j^{p_j^{e_j - 1}} \neq 1$.

Conversely, suppose that $g_j^{p_j^{e_j - 1}} \neq 1$ for each j. We have $o(g) \mid n$ since $g^n = 1$. Further, g_j has order $p_j^{e_j}$. Since $o(g_j) = o\left(g^{n_j}\right)$ and $o\left(g^k\right) \mid o(g)$ for all $k \in \mathbb{N}$, from Eqn. (40), it follows that $p^{e_j} \mid o(g)$. Since $p_1^{e_1}, p_2^{e_2}, \cdots$ 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 $g_i = g^{p_i^{n_i}}$, $1 \leq i \leq k$. If $g_i = 1$ for some i, g is not a generator of G.
3. If none of the g_i are one, compute $g_i^{p_i^{e_i - 1}}$. 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 $\pmod{23}$.

Solution: We first check if $2 \pmod{23}$ 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

$$g^{11} = g^{1+1\cdot 2+0\cdot 2^2+1\cdot 2^3} = g \cdot g^2 \cdot g^8.$$

We repeatedly square $2 \pmod{23}$ 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, $o(\bar{2}) \mid 11$ and $o(U(\mathbb{Z}_{23}))$ is 1 or 11. Since $o(\bar{2}) \neq 1$, we have $o(\bar{2}) = 11$. Since, $o(\bar{2}) \neq 22$ we conclude that $\bar{2}$ is not a primitive root $\pmod{23}$.

Let us try 3. We calculate $g_1 = g^{11}$. 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, $o(\bar{3}) = 11$ and $\bar{3}$ is not a primitive root.

Let us try 5 next. We calculate $g_1 = g^{11}$. We have

$$5^2 = 25 \equiv 2 \pmod{23}, 5^4 \equiv 2^2 \equiv 4 \pmod{23},\ 5^8 \equiv 16 \pmod{23}$$

So, $5^{11} \equiv 5 \cdot 2 \cdot 16 \equiv 22 \pmod{23}$. So, $g_1^{p_1^{e_1-1}} = 22^{2^0} = 22 \not\equiv 1 \pmod{23}$.

We have $g_2 = g^{n_2} = 5^2 = 25 \equiv 2 \pmod{23}$. Also,

$$g_2^{p_2^{e_2-1}} = 2^{5^0} = 2 \not\equiv 1 \pmod{23}.$$

So, 5 is a primitive root (mod 23).

* * *

Here is an exercise for you.

E14) Find a primitive root of (mod 43).

E15) If p is a prime of the form $4t + 1$, show that a is a primitive root (mod p) if and only if –a is a primitive root (mod p).

We briefly describe the structure of $U(\mathbb{Z}_n)$ in general without proofs because the proofs are not particulary instructive. From Eqn. (35), we need to find only the structure of $U\left(\mathbb{Z}_{p^\alpha}\right)$ for $\alpha \geq 2$, where p is a prime.

Proposition 11 : If p is an odd prime, $U\left(\mathbb{Z}_{p^\alpha}\right)$ is cyclic for $\alpha \geq 1$. Further

$$U(\mathbb{Z}_{2^\alpha}) = \begin{cases} \langle \overline{1} \rangle, & \text{if } \alpha = 1 \\ \langle \overline{-1} \rangle, & \text{if } \alpha = 2 \\ \langle \overline{-1} \rangle \times \langle \overline{5} \rangle, & \text{if } \alpha \geq 2 \end{cases}$$

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

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where p_i are prime and $\alpha_i \in \mathbb{N}$. 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

$$\left.\begin{aligned} x^2 &\equiv m \pmod{p_1^{\alpha_1}} \\ x^2 &\equiv m \pmod{p_2^{\alpha_2}} \\ &\vdots \\ x^2 &\equiv m \pmod{p_k^{\alpha_k}} \end{aligned}\right\} \quad \ldots(41)$$

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 $x^2 \equiv a \left(\mathrm{mod}\ p^k\right)$ also has 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 $x^2 \equiv a \left(\mathrm{mod}\ p^k\right)$, where $(a, p) = 1$, there is an $\alpha' \in \mathbb{Z}$ such that $\alpha \equiv \alpha' \left(\mathrm{mod}\ p^k\right)$ and $\alpha'^2 \equiv a \left(\mathrm{mod}\ p^{k+1}\right)$.

Proof: If $\alpha^2 \equiv a \left(\mathrm{mod}\ p^{k+1}\right)$, we can take $\alpha' = \alpha$ and we are done. So, let us assume $\alpha^2 \not\equiv a \left(\mathrm{mod}\ p^{k+1}\right)$, i.e $p^k \mid (\alpha^2 - a)$, $p^{k+1} \nmid (\alpha^2 - a)$. Therefore,

$$\alpha^2 - a = up^k \text{ with } (u, p) = 1 \qquad \ldots(42)$$

Consider the 'Taylor series expansion' of $x^2 - a$ about α:

$$x^2 - a = \alpha^2 - a + 2\alpha(x - \alpha) + (x - \alpha)^2 \qquad \ldots(43)$$

We need to find an α' such that

$$\alpha^2 - a + 2\alpha(\alpha' - \alpha) + (\alpha' - \alpha)^2 \equiv 0 \left(\mathrm{mod}\ p^{k+1}\right) \qquad \ldots(44)$$

$$\alpha' \equiv \alpha \left(\mathrm{mod}\ p^k\right) \qquad \ldots(45)$$

If $\alpha' = \alpha + vp^k$ then Eqn. (45) is satisfied. So, if we can find a v such that $\alpha' = \alpha + vp^k$ satisfies Eqn. (44), we are done. Let us put $\alpha' = \alpha + vp^k$ 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

$$up^k + 2\alpha vp^k \equiv 0 \left(\mathrm{mod}\ p^{k+1}\right). \qquad \ldots(46)$$

where u is defined as in Eqn. (42). From the congruence in Eqn. (46) it follows that

$$u + 2\alpha v \equiv 0 \pmod{p} \text{ or } 2\alpha v \equiv -u \pmod{p} \qquad \ldots(47)$$

We can solve the last equation for v since $(2\alpha, p) = 1$. This is because, if $p \mid \alpha$, from the congruence $\alpha^2 \equiv a \left(\mathrm{mod}\ p^k\right)$, 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

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if a is a quadratic residue } (\text{mod } p). \\ -1, & \text{if a is not a quadratic residue } (\text{mod } p). \end{cases} \quad \ldots(48)$$

Remark 3 : Note that $\left(\frac{a}{p}\right)$ is 1 or -1 according as $\bar{a}$ 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, $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ 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 $\mathbb{Z}_7^*$.

$\bar{a}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{a}^2$	$\bar{1}$	$\bar{4}$	$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$

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 11). 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

$$a^{\frac{(p-1)}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \quad \ldots(49)$$

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

$$\left\{ x \in G \,\middle|\, x^d = 1 \right\} \quad \ldots(50)$$

Further,

$$\left\{ x \in G \,\middle|\, x^d = 1 \right\} = \left\{ x^{\frac{n}{d}} \,\middle|\, x \in G \right\} \quad \ldots(51)$$

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 $f\colon \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$ 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 $\{\overline{1}, \overline{-1}\}$. In other words, $x^{\frac{p-1}{2}} = \overline{\pm 1}$. The result in Eqn. (49) will follow if we show that $f(a) = \overline{1}$ if a is a quadratic residue and it is $\overline{-1}$ if it is a quadratic non-residue. Since we already have $f(a) = a^{\frac{p-1}{2}} \in \{\overline{1}, \overline{-1}\}$ it is enough to show that the kernel of f is precisely $\left\{x^2 \,\middle|\, x \in \mathbb{Z}_p^*\right\}$. If we apply Lemma 4 with $n = p-1$ and $d = \frac{p-1}{2}$ we have

$$\left\{x \in \mathbb{Z}_p^* \,\middle|\, x^{\frac{p-1}{2}} = 1\right\} = \left\{x^2 \,\middle|\, x \in \mathbb{Z}_p^*\right\}$$

So, the kernel of f is $\left\{x^2 \,\middle|\, x \in \mathbb{Z}_p^*\right\}$.

We have $(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p$ since $(\overline{ab})^{\frac{p-1}{2}} = \overline{a}^{\frac{p-1}{2}} \overline{b}^{\frac{p-1}{2}}$. 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 $20 = 2^{1\cdot 0 + 2\cdot 0 + 2^2\cdot 1 + 2^3\cdot 0 + 2^4\cdot 1}$. Using the 'square and multiply trick' we used earlier, we have

$$\begin{aligned} 19^2 &= 361 \equiv 33 \pmod{41} \\ \therefore 19^4 &\equiv 33^2 = 1089 \equiv 23 \pmod{41} \\ \therefore 19^8 &\equiv 23^2 = 529 \equiv 37 \pmod{41} \\ \therefore 19^{16} &\equiv 37^2 = 1369 \equiv 16 \pmod{41} \\ \therefore 19^{20} = 19^{16}19^4 &\equiv 16.23 \equiv 40 \equiv -1 \pmod{41} \end{aligned}$$

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, $\left(\frac{6}{11}\right) = -1.1 = -1$. 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 $\left\{ x \,\middle|\, x^d = 1 \right\}$ has order d. Deduce that this is the unique subgroup of order d.

b) Show that $\left\{ x^{\frac{n}{d}} \,\middle|\, x \in G \right\}$ 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 $\psi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ induces a ring homomorphism $\widetilde{\psi} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_n[x]$ given by

$$\widetilde{\psi}\left(\sum a_i x^i\right) = \sum \psi(a_i)\, x^i$$

If $p(x) \in \mathbb{Z}$, we will call $\widetilde{\psi}(p(x))$ the reduction of p(x) modulo n.

Consider the polynomial $x^2 - 7$. If we reduce it modulo 3, this polynomial becomes $x^2 - \overline{1}$. 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 $x^2 - \overline{2}$ and this does not split into linear factors because $\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \equiv 4 \equiv -1 \pmod{5}$, 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,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \qquad \ldots(52)$$

Remark 4 : The quadratic reciprocity is stated often in the following form also.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \qquad \ldots(53)$$

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases} \quad \ldots(54)$$

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

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases} \quad \ldots(55)$$

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,

$$\left(\frac{17}{71}\right) = (-1)^{\frac{17-1}{2}\frac{71-1}{2}} \left(\frac{71}{17}\right) = \left(\frac{71}{17}\right) = \left(\frac{3}{17}\right)$$

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,

$$\left(\frac{229}{41}\right) = \left(\frac{3}{41}\right) = (-1)^{\frac{3-1}{2}\frac{41-1}{2}}\left(\frac{41}{3}\right) = \left(\frac{41}{3}\right)$$
$$= \left(\frac{2}{3}\right) \equiv 2^{\frac{3-1}{2}} \equiv 2 \equiv -1 \pmod 3.$$

So, $\left(\frac{229}{41}\right) = -1$.

iv) We have

$$\left(\frac{73}{191}\right) = (-1)^{\frac{73-1}{2}\frac{191-1}{2}}\left(\frac{191}{73}\right) = \left(\frac{45}{73}\right) = \left(\frac{9\cdot 5}{73}\right) = \left(\frac{9}{73}\right)\left(\frac{5}{73}\right)$$
$$= \left(\frac{5}{73}\right) = (-1)^{\frac{5-1}{2}\frac{73-1}{2}}\left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} = 9 \equiv -1 \pmod 5$$

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 (mod p).

Example 17: Describe the primes p for which $x^2 - 7$ splits into linear factors modulo p.

Solution: For p = 2, we get the polynomial $x^2 - \bar{1}$ when we reduce $x^2 - 7$ modulo 2 and $x^2 - \bar{1} = (x - \bar{1})^2$.

Let p be any odd prime. Using Eqn. (53), we have

$$\left(\frac{7}{p}\right) = (-1)^{3\left(\frac{p-1}{2}\right)}\left(\frac{p}{7}\right) = \left((-1)^{\frac{p-1}{2}}\right)^3\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right) \quad \ldots(56)$$

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 $p \equiv 1, 2 \text{ or } 4 \pmod 7$. So, p should satisfy one of the following set of congruences:

$p \equiv 1 \pmod 4$	$p \equiv 1 \pmod 4$	$p \equiv 1 \pmod 4$
$p \equiv 1 \pmod 7$	$p \equiv 2 \pmod 7$	$p \equiv 4 \pmod 7$

As we saw in the previous section, we will first solve the congruences

$$x_1 \equiv 1 \pmod 4 \qquad x_2 \equiv 0 \pmod 4$$
$$x_1 \equiv 0 \pmod 7 \qquad x_2 \equiv 1 \pmod 7$$

The solutions are $x_1 = 21$ and $x_2 = 8$. So, the solution of the congruences

$$p \equiv 1 \pmod 4$$
$$p \equiv 1 \pmod 7$$

is $x_1 + x_2 = 29 \equiv 1 \pmod{28}$. Here is the complete table:

Congruences	Solution
$p \equiv 1 \pmod 4$ $p \equiv 1 \pmod 7$	$x_1 + x_2 = 29 \equiv 1 \pmod{28}$
$p \equiv 1 \pmod 4$ $p \equiv 2 \pmod 7$	$x_1 + 2x_2 = 21 + 16 = 37 \equiv 9 \pmod{28}$
$p \equiv 1 \pmod 4$ $p \equiv 4 \pmod 7$	$x_1 + 4x_2 = 21 + 32 = 53 \equiv 25 \pmod{28}$

The other possibility is $(-1)^{\frac{p-1}{2}} = -1$ 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:

$$p \equiv 3 \pmod 4 \qquad p \equiv 3 \pmod 4 \qquad p \equiv 3 \pmod 4$$
$$p \equiv 3 \pmod 7 \qquad p \equiv 5 \pmod 7 \qquad p \equiv 6 \pmod 7$$

Here is the complete table:

Congruences	Solution
$p \equiv 3 \pmod 4$ $p \equiv 3 \pmod 7$	$3x_1 + 3x_2 = 63 + 24 = 87 \equiv 3 \pmod{28}$
$p \equiv 3 \pmod 4$ $p \equiv 5 \pmod 7$	$3x_1 + 5x_2 = 63 + 40 = 103 \equiv 19 \pmod{28}$
$p \equiv 3 \pmod 4$ $p \equiv 6 \pmod 7$	$3x_1 + 6x_2 = 63 + 48 \equiv 27 \pmod{28}$

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 $7^{\frac{263081503-1}{2}} = 7^{131540751} \pmod{263081503}$. 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 ∈ S}. The set $\left\{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\right\}$ has this property. So, we will choose S = $\left\{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\right\}$. For s ∈ S and a ∈ $\mathbb{Z}_p^*$, 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 ∈ S and $e_s(a) = -1$, if as ∈ –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 $6_3 = 3$ in this case.

Proposition 15 (Gauss' Lemma): For any prime p and a ∈ $\mathbb{Z}$, p ∤ a

$$\left(\frac{a}{p}\right) = \prod_{s\in S} e_s(a) \qquad \ldots(57)$$

Proof: If s and s′ are two distinct elements of S, then $s_{\bar{a}} \neq s_{\overline{a'}}$. If $s_{\bar{a}} = s_{\overline{a'}}$, then $e_s(\bar{a})\bar{a}s = e_{s'}(\bar{a})\bar{a}s'$ or $e_s(\bar{a})s = e_{s'}(\bar{a})s'$. 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 $\bar{a}s = e_s(\bar{a})s_{\bar{a}}$, we get

$$\bar{a}^{\frac{p-1}{2}} \prod_{s\in S} s = \left(\prod_{s\in S} e_s(\bar{a})\right) \prod_{s\in S} s_{\bar{a}} = \left(\prod_{s\in S} e_s(\bar{a})\right) \prod_{s\in S} s$$

Hence

$$\bar{a}^{\frac{p-1}{2}} = \left(\prod_{s\in S} e_s(\bar{a})\right)$$

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 ≥ 1, we have

$$x^{2n+1} - \frac{1}{x^{2n+1}} = \left(x - \frac{1}{x}\right)^{2n+1} + \sum_{i=0}^{n-1} a_{i,n} \left(x - \frac{1}{x}\right)^{2i+1} \qquad \ldots(58)$$

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

$$\frac{\sin(2\ell+1)x}{\sin x} = (-4)^{\ell} \prod_{1\le j\le \ell} \left(\sin^2 x - \sin^2 \frac{2\pi j}{2\ell+1}\right) \qquad \ldots(59)$$

Proof: Let us divide Eqn. (58) by $x - \frac{1}{x}$ to get

$$\frac{x^{2\ell+1} - \frac{1}{x^{2\ell+1}}}{x - \frac{1}{x}} = \left(x - \frac{1}{x}\right)^{2\ell} + \sum_{i=0}^{\ell-1} a_{i,\ell} \left(x - \frac{1}{x}\right)^{2i}. \quad \ldots(60)$$

Let us substitute e^{ix} for x in Eqn. (60). Then, the LHS of Eqn. (60) becomes

$$\frac{x^{2\ell+1} - \frac{1}{x^{2\ell+1}}}{x - \frac{1}{x}} = \frac{e^{(2\ell+1)ix} - e^{-(2\ell+1)ix}}{e^{ix} - e^{-ix}} = \frac{\sin(2\ell+1)x}{\sin x} \quad \ldots(61)$$

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

$$P(T) = (-4)^{\ell} T^{\ell} + \sum_{j=1}^{\ell-1}(-4)^j a_{j,\ell} T^j \quad \ldots(62)$$

Then,

$$\frac{\sin(2\ell+1)x}{\sin x} = P(\sin^2 x) \quad \ldots(63)$$

So, we have

$$P\left(\sin^2 \frac{2\pi j}{2\ell+1}\right) = \frac{\sin(2\ell+1)\frac{2\pi j}{2\ell+1}}{\sin \frac{2\pi j}{2\ell+1}} = 0 \text{ for } 1 \leq j \leq \ell \quad \ldots(64)$$

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

$$S = \left\{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\right\}$$

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 $\sin\frac{2\pi a}{p} = \sin\left(2r\pi + \frac{2\pi a'}{p}\right) = \sin\frac{2\pi a'}{p}$. So, it makes sense to write $\sin\frac{2\pi s}{p}$ for $s \in \mathbb{Z}_p^*$.)

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

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{s\in S}(-4)^{\frac{q-1}{2}}\prod_{t\in T}\left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right)\\ &= (-1)^{\frac{(q-1)(p-1)}{4}}\prod_{s\in S,t\in T}\left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right)\end{aligned}$$

where T is the set $\left\{\overline{1}, \overline{2}, \ldots, \overline{\frac{q-1}{2}}\right\}$. 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 $S = \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\}$. 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,

$$\begin{aligned}&n(p) \text{ is even } \Leftrightarrow k \text{ is even } \Leftrightarrow p = 4(2m) + 1 = 8m + 1\\ &n(p) \text{ is odd } \Leftrightarrow k \text{ is odd } \Leftrightarrow p = 4(2m + 1) + 1 = 8m + 5\end{aligned}$$

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, $\frac{p-1}{4} = k + \frac{1}{2}$, $\frac{p-1}{2} = 2k + 1$ and $n(p)$ is the number of s with $k + 1 \leq s \leq 2k + 1$. So, $n(p) = k + 1$. Therefore,

$$n(p) \text{ is even } \Leftrightarrow k \text{ is odd } \Leftrightarrow p = 4(2m + 1) + 3 = 8m + 7$$
$$n(p) \text{ is odd } \Leftrightarrow k \text{ is even } \Leftrightarrow p = 4(2m) + 3 = 8m + 3$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

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 $p \equiv 1 \pmod 4$, $4 \mid (p - 1)$. 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 $\left(y^2\right)^2 = y^4 = 1$, so $y^2 = -1$ and so -1 is a square in $\mathbb{Z}_p^*$. ■

E20) Prove Lemma 5.

E21) If $p = 2^{2^k} + 1$, for some $k \geq 1$ is a prime, show that 3 is a primitive root for $U\left(\mathbb{Z}_p\right)$.

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 (mod$n$);
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

$$7 - 0 + 2 - 1 + 0 - 9 = -1, 7 - 0 + 2 - 1 + 0 - 9 + 1 \equiv 0 \pmod{11}$$

So, the number is divisible by 11.

E2) Adding terms with zero coefficients if necessary, we can assume that

$$n = \sum_{i=0}^{k} a_i 10^k, m = \sum_{i=0}^{n} b_i 10^k, 0 \leq a_i, b_i \leq 9 \text{ for } i = 0, 1, 2, \ldots, k$$

Then

$$n - m = \sum_{i=1}^{k} (a_i - b_i)\, 10^k + (a_0 - b_0) \equiv (a_0 - b_0) \pmod{10} \quad \ldots(65)$$

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 $\overline{a + c} = \overline{b + d}$. We have

$$\begin{aligned} \overline{a + c} &= \psi(a + c) = \psi(a) + \psi(c) \\ &= \psi(b) + \psi(d) \\ &= \psi(b + d) = \overline{b + d} \end{aligned}$$

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 $ad \equiv bd \mod nd$.

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 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 $(-21, -8) = (21, -8) = (-8, 21) = (8, 21) = (21, 8)$. 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 to Step I to find $(1, 0)$.
In Step I, $b = 0$ so $(21, 8) = a = 1$.

E6) i) The computation is given below:

a	b	q	u	v	d
*	*	*	0	1	*
65	25	2	1	–2	15
25	15	1	–1	3	10
15	10	1	2	–5	5
10	5	2			0

From the fourth row, $(65, 25) = 5$, $u = 2$, $v = -5$.

ii) The computation is shown below:

a	b	q	u	v	d
*	*	*	0	1	*
141	93	1	1	–1	48
93	48	1	–1	2	45
48	45	1	2	–3	3
45	3	15			0

From the fourth row, $(141, 93) = 3$, $u = 2$ and $v = -3$.

iii) The computation is given below:

a	b	q	u	v	d
*	*	*	0	1	*
21	8	2	1	–2	5
8	5	1	–1	3	3
5	3	1	2	5	2
3	2	1	–3	8	1

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:

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			0

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:

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
170	25	6	1	–6	20
25	20	1	–1	7	5
20	5	4			0

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:

a	b	q	u	v	d
$*$	$*$	$*$	0	1	$*$
17	3	5	1	–5	2
3	2	1	–1	6	1

We have $(-1)17 + (6)3 = 1$. So, $\bar{3}^{-1} = \bar{6}$. Multiplying both sides of the congruence $3x \equiv 2 \pmod{17}$ by 6, we get, $x \equiv 12 \pmod{17}$.

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 $2x \equiv 3 \pmod{9}$. We proceed as before and find $u = -4$, $v = 1$ satisfying $2u + 9v = 1$. So, $\bar{2}^{-1} = \overline{-4} = \bar{5}$. Multiplying both sides of the congruence $2x \equiv 3 \pmod{9}$ by 5, we get $x \equiv 15 \equiv 6 \pmod{9}$. From Proposition 6, it follows that $6 + 0 \cdot 9 = 6$, $6 + 1 \cdot 9 = 15$ are the solutions to the congruence $4x \equiv 6 \pmod{18}$.

iii) We have $(10, 85) = 5$ and $5 \mid 5$. We consider the congruence $2x \equiv 1 \pmod{17}$. We proceed as before to find $u = 1$, $v = -8$, i.e. $(1)17 + (-8)2 = 1$. So, $\bar{2}^{-1} = \overline{-8}$ in $\mathbb{Z}_{17}$. Multiplying both sides of the congruence $2x \equiv 1 \pmod{17}$ by -8, we get $x \equiv -8 \equiv 9 \pmod{17}$. 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 $7^4 \equiv 1 \pmod{10}$. Since $323 = 4 \cdot 80 + 3$, it follows that $7^{323} = \left(7^4\right)^{80} 7^3 \equiv 7^3 \equiv 3 \pmod{10}$. So, the units digit of 7^{323} is 3.

E9) By Fermat's little theorem, $a^{10} \equiv 1 \pmod{11}$. Since $\mathbb{Z}_{11}$ is a field, the equation $x^2 - 1 = 0$ has only two solutions, Since a^5 is a solution, $a^5 = \pm\bar{1}$, in $\mathbb{Z}_{11}$. So, $11 \mid \left(a^5 - 1\right)\left(a^5 + 1\right)$.

E10) We take $n_1 = 5$, $n_2 = 7$ and $n_3 = 11$. Then

$$N_1 = 77 \equiv 2 \pmod 5 \qquad \overline{2}^{-1} = \overline{3} \text{ in } \mathbb{Z}_5 \qquad N_1' = 3$$
$$N_2 = 55 \equiv 6 \pmod 7 \qquad \overline{6}^{-1} = \overline{6} \text{ in } \mathbb{Z}_7 \qquad N_2' = 6$$
$$N_3 = 35 \equiv 2 \pmod{11} \qquad \overline{6}^{-1} = \overline{6} \text{ in } \mathbb{Z}_7 \qquad N_3' = 6$$

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 $2412 \pmod{385}$ which is 102.

E11) First, we convert the congruences to the standard form. We have $\overline{3}^{-1} = \overline{3}$ in $\mathbb{Z}_4$. So, multiplying both sides of the first congruence by 3 we get $x \equiv 2 \pmod 4$. We have $\overline{8}^{-1} = \overline{8}$ 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

$$x \equiv 2 \pmod 4$$
$$x \equiv 5 \pmod 9$$
$$x \equiv 3 \pmod{11}$$

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 $x = 2 \cdot 99 \cdot 3 + 5 \cdot 44 \cdot 8 + 3 \cdot 36 \cdot 4 = 2786$. 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

$$ab = (a_1, a_2, \ldots, a_k)\,(b_1, b_2, \ldots, b_k \in R) = \underbrace{(1, 1, \ldots, 1)}_{\text{k times}}$$

Therefore, we have

$$(a_1b_1, a_2b_2, \ldots, a_kb_k) = \underbrace{(1, 1, \ldots, 1)}_{\text{k times}}$$

or $a_ib_1 = 1$ for $i = 1, 2, \cdots, k$. 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, $e_1 = 1$, $e_2 = 1$, $e_3 = 1$.

Let us first check if 2 is a primitive. So, we take g = 2 and calculate $g_1 = 2^{n_1} = 2^{21} \pmod{43}$. We have

$$21 = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4.$$

So,

$$2^{21} = 2 \cdot 2^{2^2} \cdot 2^{2^4} = 2 \cdot 2^4 \cdot 2^{16}.$$

Note that
$41 \equiv -2 \pmod{43}$.

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

$$2^{21} = 2 \cdot 2^4 \cdot 2^{16} \equiv 2 \cdot 16 \cdot 4 \equiv 42 \equiv -1 \pmod{43}.$$

So, $g_1^{p_1^{e_1-1}} = (-1)^{2^0} = -1 \neq 1 \pmod{43}$. We have

$$g_2 = 2^{n_2} = 2^{14} = 2^2 \cdot 2^4 2^8 \equiv 4 \cdot 16 \cdot (-2) \equiv 1 \pmod{43}.$$

So, $g_2^{p_2^{e_2-1}} = g_2 \equiv 1 \pmod{43}$. 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

$$g_1 = 3^{21} \equiv 3 \cdot (-5) \cdot 23 \equiv 42 \pmod{43}.$$

$$g_1^{p_1^{e_1-1}} \equiv 42 \not\equiv 1 \pmod{43}$$

Computing as before, We have

$$g_2 = g^{n_2} = 3^{14} \equiv 36 \pmod{43},\ g_2^{p_2^{e_2-1}} = g_2 \equiv 36 \neq 1 \pmod{43}$$

We have $g_3 = 3^6 \equiv 41$, $g_3^{p_3^{e_3-1}} = g_3 \neq 1 \pmod{43}$. Therefore, 3 is a primitive root $\pmod{43}$.

E15) Suppose a is a primitive root (mod p) and –a is not a primitive root (mod p). Then $(-a)^k = 1$ for some $k \in \mathbb{N}$, $k < p - 1$. It follows that $(-1)^k a^k = 1$. 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 $U(\mathbb{Z}_8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

E17) Let $K = \left\{ x \in G \,\middle|\, x^d = 1 \right\}$. 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

$$\left(\frac{109}{347}\right) = (-1)^{\frac{109-1}{2}\frac{347-1}{2}} \left(\frac{347}{109}\right) = \left(\frac{20}{109}\right) = \left(\frac{4}{109}\right)\left(\frac{5}{109}\right) = \left(\frac{5}{109}\right)$$

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

$$\left(\frac{71}{107}\right) = (-1)^{\frac{71-1}{2}\frac{107-1}{2}} \left(\frac{107}{71}\right) = -\left(\frac{36}{71}\right) = -1$$

since $\left(\frac{36}{71}\right) = 1$.

iii) We have

$$\left(\frac{41}{61}\right) = (-1)^{\frac{41-1}{2}\frac{61-1}{2}} \left(\frac{61}{41}\right) = \left(\frac{20}{41}\right) = \left(\frac{4}{41}\right)\left(\frac{5}{41}\right)$$
$$= \left(\frac{5}{41}\right) = (-1)^{\frac{41-1}{2}\frac{5-1}{2}} \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1$$

iv) We have

$$\left(\frac{97}{239}\right) = (-1)^{\frac{231-1}{2}\frac{97-1}{2}}\left(\frac{239}{97}\right) = \left(\frac{239}{97}\right) = \left(\frac{45}{97}\right)$$
$$= \left(\frac{9}{97}\right)\left(\frac{5}{97}\right) = \left(\frac{5}{97}\right) = (-1)^{\frac{5-1}{2}\frac{97-1}{2}}\left(\frac{97}{5}\right)$$
$$= \left(\frac{2}{5}\right) = 2^2 = 4 \equiv -1 \pmod 5.$$

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

$$x^{2k+1} - \frac{1}{x^{2k+1}} = \left(x - \frac{1}{x}\right)^{2k+1} + \sum_{i=0}^{k-1} a_{i,k}\left(x - \frac{1}{x}\right)^{2i+1} \quad \ldots(66)$$

where $a_{i,k} \in \mathbb{Z}$.

$$\left(x - \frac{1}{x}\right)^{2n+1} = x^{2n+1} + \sum_{i=1}^{n}(-1)^i C(2n+1, i)x^{2n+1-i}\frac{1}{x^{-i}}$$
$$+ \sum_{i=n+1}^{2n}(-1)^i C(2n+1, i)x^{2n+1-i}\frac{1}{x^{-i}} - \frac{1}{x^{2n+1}}$$
$$\therefore x^{2n+1} - \frac{1}{x^{2n+1}} = \left(x - \frac{1}{x}\right)^{2n+1} - \sum_{i=1}^{n}(-1)^i C(2n+1, i)x^{2n+1-2i}$$
$$- \sum_{i=n+1}^{2n}(-1)^i C(2n+1, i)x^{2n+1-2i} \quad \ldots(67)$$

To complete the proof, we have to show that

$$\sum_{i=1}^{n}(-1)^i C(2n+1, i)x^{2n+1-2i} + \sum_{i=n+1}^{2n}(-1)^i C(2n+1, i)x^{2n+1-2i} \quad \ldots(68)$$

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

$$\begin{aligned}(-1)^{2n}C(2n+1,2n)x^{-(2n-1)} &= C(2n+1,2n)x^{-(2n-1)}\\ &= C(2n+1,1)x^{-(2n-1)}\end{aligned}$$

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

$$(-1)^m C(2n+1,m)x^{2(n-m)+1} \quad \ldots(69)$$

The sum corresponding to i = 2n – (m – 1) is the second term is

$$\begin{aligned}&(-1)^{2n-m+1}C(2n+1,2n-m+1)x^{2n+1-(2n-m+1)}\frac{1}{x^{2n-m+1}}\\ &= -(-1)^m C(2n+1,2n-m+1)x^{2n+1-(2n-m+1)-(2n-m+1)}\\ &= -(-1)^m C(2n+1,m)x^{-(2(n-m)+1)} \quad \ldots(70)\end{aligned}$$

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

$$\sum_{i=1}^{n}(-1)^i C(2n+1,i)\left(x^{2(n-i)+1} - x^{-(2(n-i)+1)}\right) \quad \ldots(71)$$

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 $\left|U\left(\mathbb{Z}_p\right)\right| = 2^{2^k}$ so, if g is any primitive root for $U\left(\mathbb{Z}_p\right)$, 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

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{2^{2^k}}{2}} \left(\frac{p}{3}\right) = \left(\frac{2^{2^k}+1}{3}\right)$$

If $k = 1$, we have $2^2 = 4 \equiv 1 \pmod 3$, so $2^2 + 1 \equiv 2 \pmod 3$ and $\left(\frac{2^2+1}{3}\right) = -1$. For $k > 1$, we have

$$2^{2^k} + 1 = \left(2^2\right)^{2^{k-1}} + 1 = (4)^{2^{k-1}} + 1 \equiv 2 \pmod 3$$

and we are done.

E22) We have $\left|U\left(\mathbb{Z}_p\right)\right| = 2q$ 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 $\left|U\left(\mathbb{Z}_p\right)\right|$. We have $2^2 = 4 \not\equiv 1 \pmod 3$ because $4 - 1 = 3 < p$.

Let us now consider 2^q. We have $2^q = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right)$. Since $p \equiv 3 \pmod 8$, it follows that $\left(\frac{2}{p}\right) = -1$, so $2^q \equiv -1 \pmod p$.