DR. BHUPENDRANATH DUTTA SMRITI MAHAVIDYALAYA

PROJECT WORK

CONGRUENCE AND ITS APPLICATIONS

Name → SANTU GARAI.

Department → MATHEMATICS.

Semester → 6th SEMESTER.

Course → BMH6PW01.

Roll No. → 200312400021

Registration No. → 202001016222 of 2020-21

Certificate

This is to certify that the project work in course **Project Work** (Course Code **BMH6PW01**) entitled **"Congruence and Its Applications"** submitted by **Santu Garai**, Roll No.- **200312400021**, Registration No.- **202001016222 of 2020-21** who took admission in **Dr. Bhupendra Nath Dutta Smriti Mahavidyalaya** under **The University of Burdwan** has successfully completed the project work under my supervision and guidance. Neither the project work nor any part of the project work has been submitted for either any degree or diploma or any other academic award anywhere before.

…………………………………

(Signature of the Supervisor)

Declaration

I hereby declare that the project work in course **BMH6PW01** entitled **“Congruence and Its Applications”** submitted by me for partial fulfilment of Bachelor of Science (B.Sc.) degree to **The University of Burdwan** is my original work and has not been submitted earlier to any other institution for the fulfilment of my course of study. I also declare that no section of this manuscript in whole or in part is lifted and incorporated in this report from any work done earlier, either by others or by me.

………………………………..

(Signature of the Student)

Acknowledgement

I would like to express my special thanks of gratitude of my teacher **Dr. Tapas Kumar Mondal** as well as our principal **Dr. Amal Kumar Ghosh** who gave me the golden opportunity to do this wonderful project on the topic **“Congruence and Its Applications”**, which also helped me in doing a lot of Research and I came to know about so many new things. I am really thankful to them.

Congruence and Its Applications

Santu Garai

August 13, 2023

1 Introduction

Karl Friedrich Gauss(1777-1855), a celebrated German mathematician, introduced the concept of congruence which which laid the foundation of modern theory of numbers.In abstract algebra a congruence relation(or simply congruence) is an equivalence relation on an algebraic structure (such as a group, ring,or vectors space)that is compatible with the structure in the sense that algebraic operations done with equivalent elements will yield equivalent elements.Every congruence relation has corresponding quotient structure whose elements are the equivalence classes (or congruence classes) for the relation.

In geometry,two figures or objects are congruent if they have the same shape and size,if one has the same shape and size as the mirror image of the other.congruence permits alteration of some properties, such as location and orientation, but leaves others unchanged, like distances and angles the unchanged properties are called invariants. More formally two sets of points are called congruent if and only if, one can be transformed into the others by an isometry, i.e., a combination of rigid motions, namely a translation, a rotation, and a reflection. This means that either object can be repositioned and reflected(but not resized)so as to coincide precisely with the others object.

Therefore two distinct plane figures on a piece of paper are congruent if they can be cut out and then matched up completely. Turning then paper over is permitted.

2 Congruence

If a and b are integers and m is a positive integer, we say that a is congruent to b modulo m when m divides $a - b$. If a is congruent to b modulo m, we write $a \equiv b(\text{mod } m)$. If $a - b$ is not divisible by m, then we write $a \not\equiv b$ (mod

m) and we say that is not congruent to b modulo m.

Example 2.1 *We have* $19 \equiv 5$*(mod* 7*). Similarly for any* $k \in \mathbb{Z}, 2k+1 \equiv 1$*(mod* 2*), which means every odd number is congruence modulo* 2*. But* $11-3$ *is not divisible by* 5*. Hence* $11 \not\equiv 3$*(mod* 5*)*

2.1 Properties of congruence

There are many common properties between equations and congruences. some properties are listed in following theorem.

Theorem 2.2 *Let a,b,c and d denote integers. Let m be a positive integers. Then one has*

1. *If* $a \equiv b$*(mod m),then* $b \equiv a$*(mod m).*
2. *If* $a \equiv b$*(mod m) and* $b \equiv c$ *(mod m),then* $a \equiv c$*(mod m).*
3. *If* $a \equiv b$*(mod m), then a+c* $\equiv$ *b+c(mod m).*
4. *If* $a \equiv b$*(mod m),then a - c* $\equiv$ *b - c(mod m).*
5. $a \equiv b$*(mod m), then ac* $\equiv$ *bc(mod m).*
6. *If* $a \equiv b$*(mod m), then ac* $\equiv$ *bc(mod mc),for c > 0.*
7. *If* $a \equiv b$*(mod m) and* $c \equiv d$*(mod m) then a+c* $\equiv$ *b+d(mod m).*
8. *If* $a \equiv b$*(mod m) and* $c \equiv d$*(mod m) then a - c* $\equiv$ *b - d(mod m).*
9. *If* $a \equiv b$*(mod m) and* $c \equiv d$*(mod m) then ac* $\equiv$ *bd(mod m).*

Proof:

1. *Suppose* $a \equiv b$ *(mod m). Then m divides a - b . Hence m divides b - a . So we find that* $b \equiv a$*(mod m).*
2. *Suppose* $a \equiv b$ *(mod m) and* $b \equiv c$ *(mod m) . then m divides a - b and b - c . Hence there exist integers r and t such that a - b = mr and b - c = mt, then a - c =(a - b) + (b - c) = m(r+t).*
   This show that m divides a - c. Hence $a \equiv c$ *(mod m).*
3. *If* $a \equiv b$ *(mod m) and* $c \equiv c$ *(mod m) ,then a+c* $\equiv$ *b+c(mod m).*

4. *Suppose a $\equiv$ b (mod m) .Then from (3), a + (- c) $\equiv$ b +(- c) (mod m). i.e., a - c $\equiv$ b - c (mod m).*

5. *Suppose a $\equiv$ b (mod m) then m $|$(a-b).Thus there exists integer k such that a - b = mk and as result ac - bc =m(kc).Thus m $|$ (ac - bc) and hence ac $\equiv$ bc (mod m).*

6. *If a $\equiv$ b (mod m) then m $|$(a-b).Thus there exists integer k such that a - b = mk and as result ac - bc = mc (k).*
   Thus mc $|$ (ac - bc)
   and hence ac $\equiv$ bc (mod mc).

7. *Since a a $\equiv$ b (mod m) then m $|$(a-b). Also c $\equiv$ d (mod m), then . m $|$ (c - d) As a result ,there exits two integers k and l such that a - b = mk and c - d = ml. Note that (a - b)+ (c - d) = (a + C) - (b + d) = m(k + l).*
   As a result m $|$ ((a + c) - (b + d)).
   Hence a + c $\equiv$ b + d (mod m).

8. *If a = b + mk and c = d + ml where k and l are integers, then*
   (a - b)- (c - d) = (a - c) - (b - d) = m(k - l)
   As a result m $|$ ((a - c) - (b - d))
   hence a - c $\equiv$ b - d (mod m).

9. *There exit two integers k ande l such that a - b = mk and c - d = ml and thus ca - cb = m (ck) and bc - bd = m(bl).Note that (ca - cb) + (bc - bd) = ac - bd = m (ck + bl).*
   As a result m mid (ac - bd)
   Hence ac $\equiv$ bd (mod m).

Theorem 2.3 *let a,b,c be integers and m a positive integer.*

ab $\equiv$ ac if and only if b $\equiv$ c $\left(\frac{m}{gcd(a,m)} \right)$

2. *If ab $\equiv$ ac (mod m)and gcd(a,m)=1, then b $\equiv$ c (mod m)*

Proof:

1. *Let d = gcd(a,m). Since $m > 0, d \neq 0$, there exist integers r and t such that gcd(t, r) = 1 and $a = dr, m = dt$. Now ab $\equiv$ ac (mod m)implies that m divides $ab - ac$,i.e, dt divides $drb - drc$ i.e., t divides $r(b - c)$. Since t and r are relatively prime,it follows that t divides $b - c$.*

Hence $b \equiv c(modm)$ *i.e,* $b \equiv c\left(\mod \frac{m}{d}\right)$.

Conversely, assume that $b \equiv c\left(\mod \frac{m}{d}\right)$. *Then* $b - c = k\frac{m}{d}$ *for some integer* k. *Hence*

$$ab - ac = k\tfrac{m}{d}a = km\tfrac{a}{d} = kmr = mkr.$$

So, we find that m divides ab - ac i.e, $ab \equiv ac$ *(mod m).*

2. *Follows from (i). We can prove the following theorem.*
   It follows from previous.

Theorem 2.4 *If* $f(x)=a_ix^n+a_{n-1}x^{n-1}$ $+\ldots+a_1x+a_0$ *is a polynomial with integral coefficients and if a,b,m are integers with m>0,* $a \equiv b$ *(mod m), then* $f(a) \equiv f(b)(mod\ m)$.

Proof: *Since* $a \equiv b$ *(mod m),it follows from previous theorem that* $a^i \equiv b^i$ *(mod m) and* $a_ia^i \equiv b_i\ b^i$ *(mod m).Then* $a_na^n+a_{n-1}a^n - 1+\ldots+a_1a+a_0 \equiv a_nb^n+a_{n-1}b^{n-1}+\ldots+a_1b+a_0$ *(mod m). Hence* $f(a) \equiv f(b)(mod\ m)$.

Example 2.5 *Let a,b be integers and m a positive integer. Prove that* $a \equiv b(mod\ m)$ *if and only if* $a = km$ *for some integer k. i.e,* $a = km + b$ *for some integer k.*

Solution: *Suppose* $a \equiv b$ *(mod m). Then m divides* $a - b$. *Hence a - b* $= km + b$ *for some integer k.Then a-b = km.Hence m divides a-b i.e.*$a \equiv b$ *(mod m).*

Example 2.6 *Let a,b,c,d be integers and m be a positive integer .If* $a \equiv b(mod\ m)$ *and* $c \equiv d(mod\ m)$,*then prove that*
$ax+cy \equiv bx+dy$ *(mod m).*

Solution: *Suppose* $a \equiv b(mod\ m)$. *Then m divides* $a - b$. *Hence m divides* $(a-b)x$ *i.e.,m divides* $ax - bx$. *Let* $c \equiv d$ *(mod m).Then m divides* $c - d$. *Hence m divides* $cy - dy$.*So we find that m divides* $(ax - bx) + (cy - dy)$ *i.e.,m divides* $(ax + cy)-(bx + dy)$. *Hence* $ax + cy \equiv bx + dy$ *(mod m).*

Example 2.7 *What is the remainder when* 7^{30} *is divided by* 4 *?*

Solution: *Let r be the required remainder .Then 0$\leq$ r¡* 4 *and* 7^{30} *- r is divisible by* 4.
Hence ,$7^{30} \equiv r$ *(mod* 4*).*
Now ,$7 \equiv 3$*(mod* 4*). Hence* $7^2 \equiv 3^2$ *(mod m). But* $3^2 \equiv 1$ *(mod* 4*). Hence* ,$7^2 \equiv 1$ *(mod* 4*).*
This implies $(7^2)^{15} \equiv 1^{15}$ *(mod* 4*). i.e.,* $7^{30} \equiv 1$ *(mod* 4*). Hence the remainder is* 1.

Example 2.8 *what is the remainder when* $6 \cdot 7^{32} + 7 \cdot 9^{45}$ *is divided by* 4 ?

Solution: $7^2 \equiv 1$ *(mod* 4*).Hence* $(7^2)^{16} \equiv 1^{16}$ *(mod* 4*), i.e,* $7^{32} \equiv 1$*(mod* 4*).Then* $6 \cdot 7^{32} \equiv 6$ *(mod* 4*). Again* $9 \equiv 1$ *(mod* 4*). Hence* $9^{45} \equiv 1$*(mod* 4*). Then* $79^{45} \equiv 7$ *(mod* 4*).So it follows that*

$$\cdot 7^{32} + 7 \cdot 9^{45} \equiv 6 + 7 \ (mod\ 4)$$
$$i.e.,6 \cdot 7^{32} + 7 \cdot 9^{45} \equiv 13 \ (mod\ 4).$$

But $13 \equiv 1$ *(mod* 4*).Hence* $6 \cdot 7^{32} + 7 \cdot 9^{45} \equiv 1$ *(mod* 4*). Therefore the remainder is* 1.

Example 2.9 *(a)Find all the integers* $k \geq 3$ *such that* $5 \equiv k^2$ *(mod k).*
(b) Find all the integers $k \geq 3$ *such that* $5 \equiv k$ *(mod k).*

Solution: *(a) Given* $5 \equiv k^2$ *(mod k). Then k divides* $5 - k^2$*. Hence k divides* 5*. Since* $k \geq 3$*, we find that* $k = 5$ *.*
(b)Given $5 \equiv k$*(mod* k^2*). Then* k^2 *divides* $5 - k$ *. Hence there exists an integer t such that* $5 - k = k^2 t$*.Then* $5 = k + k^2 t = k(1 + kt)$*.So we find that k divides* 5*. But* $k \geq 3$*. Hence* $k = 5$ *.*

Theorem 2.10 *What is the remainder when* $1! + 2! + 3! + \cdots + 99! + 100!$ *is divided by* 15 ?

Proof: *We have to find an integer r such that* $0 \leq r < 15$ *and* $1! + 2! + 3! + \cdots + 99! + 100!$ *(mod* 15*). Now ,* $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ *.Hence* 15 *divides* 5!*. This shows that* $5! \equiv 0$ *(mod* 15*). Then* $k \cdot 5! \equiv 0$ *(mod* 15*).Since for any* $n \geq 5$*,n! is a multiple of* 5!*, it follows that* $n! \equiv 0$*(mod 15) for any* $n \geq 5$ *. Now,*

$$
\begin{gathered}
1! \equiv 1 \ (mod\ 15), \\
2! \equiv 2 \ (mod\ 15), \\
3! \equiv 6 \ (mod\ 15), \\
4! \equiv 9 \ (mod\ 15), \\
\text{and } n! \equiv 0 \ (mod\ 15) \text{ for } n \geq 5 \ .
\end{gathered}
$$

Hence $1! + 2! + 3! + \cdots + 99! + 100! \equiv 18 \ (mod\ 15)$.

But $18 \equiv 3 \ (mod\ 15)$.

Hence , $1! + 2! + 34! + \cdots + 99! + 100! \equiv 3 \ (mod\ 15)$.*So* , *the remainder is* 3 .

3 Congruence Classes

Definition 3.1 *let* m *be a positive integer and* a *an integer then the subset* $\{b \in z \mid b \equiv a \ (mod\ m)\}$ *is called the congruence class modulo* m *of the integer* a. *We denote this congruence class by* $[\ a\ ]$.

Example 3.2 *let* $m = 6$ *and* $a = 4$, *then the congruence class modulo* 6 *of* 4 *is the subset*

$$
\begin{aligned}
[\ 4\ ] &= \{\ b \in z \mid b \equiv 4 \ (mod\ 6)\ \} \\
&= \{\ b \in z \mid 6 \text{ divides } b - 4\ \} \\
&= \{\ b \in z \mid b - 4 = 6k \text{ for some integer } k\ \} \\
&= \{\ b \in z \mid b = 4 + 6k \text{ for some integer } k\ \} \\
&= \{\ \cdots -14, -8, -2, 4, 10, 16, 22, \cdots\ \}
\end{aligned}
$$

3.1 Properties

Theorem 3.3 *Let* m *be a positive integer. The congruence classes modulo* m *satisfy the following:*

(i) $[\ a\ ] \neq \phi$, *for all integers* a.

(ii) If $b \in [\ a\ ]$, *then* $[\ b\ ] = [\ a\ ]$ *for all integers a,b.*

(iii) For all integers a,b either $[\ a\ ] \cap [\ b\ ] = \phi$ *or* $[\ a\ ] = [\ b\ ]$.

Proof 3.4

(i) It is obvious.

(ii) Let $b \in [\ a\ ]$.Then $b \equiv a$ (mod m).Suppose $x \in [\ b\ ]$. This implies that $x \equiv b$ (mod m). Hence it follows that $x \equiv a$ (mod m). As a result , $x \in [\ a\ ]$.Hence $[\ b\ ] \subseteq [\ a\ ]$.
Now, assume that $x \in [\ a\ ]$. Then $x \equiv a$ (mod m). since $b \equiv a$ (mod m), we find that $a \equiv b$ (mod m). Hence $x \equiv a$ (mod m).and $a \equiv b$ (mod m)together imply that $x \equiv b$ (mod m) and shows that $x \in [\ b\ ]$. Therefore $[\ a\ ] \subseteq [\ b\ ]$.Consequently, $[\ a\ ] = [\ b\ ]$.

(iii) Let a and b be two integers .Suppose $[\ a\ ] \cap [\ b\ ] \neq \phi$. Then there exists $u \in [\ a\ ] \cap [\ b\ ]$.Thus $u \in [\ a\ ]$ and $u \in [\ b\ ]$. Hence $u \equiv a$ (mod m) and $u \equiv b$ (mod m). Now $u \equiv b$ (mod m) implies that $b \equiv u$ (mod m). Then $b \equiv u$ (mod m)and $u \equiv a$ (mod m) imply that $b \equiv a$ (mod m). This shows that $b \in [\ a\ ]$. Hence from (ii) implies that $[\ b\ ] = [\ a\ ]$.

Example 3.5 *Consider the positive integer 6 and consider the congruence classes modulo 6. Now $8 \equiv 2$(mod 6).Hence $8 \in [\ 2\ ]$.This implies that $[\ 8\ ] = [\ 2\ ]$. Likewise $[\ 1\ ] = [\ 7\ ]$,$[\ 3\ ] = [\ 9\ ]$, $[\ 4\ ] = [\ 10\ ]$ etc.*

Theorem 3.6 *For any positive number m, let Z_m denote the set of all congruence classes modulo m.then the number of elements of Z_m is finite and this number is m.*

Proof 3.7 *Let k be any integer .By division algorithm there exist integers q and r such that $k = qm + r$ where $0 \leq r \leq m - 1$.*
Hence ,m divides $k - r$.This implies $k \equiv r$ (mod m), i.e, $[\ k\ ] = [\ r\ ]$.So, we find that for any integer k there exists an integer $0 \leq r \leq m - 1$ such that $[\ k] = [\ r\ ]$.Hence the number of congruence classes $[\ k\ ]$ modulo m is less than or equal to m.
Now,let $[\ r\ ]$ and $[\ t\ ]$ be two congruence classes modulo m such that $0 \leq r \leq m - 1$. Then

$$-(m - 1) \leq r - t \leq (m - 1).$$

Hence $[\ r\ ] = [\ t\ ]$ if and only if $r - t = 0$ i.e, if and only if $r = t$. It follows that$[\ 0]$,$[\ 1\ ]$, $[\ 2\ ]$, $\cdots$, $[\ m - 1\ ]$ are the m distinct congruence classes and any congruence class $[\ k\ ]$ equals to one of these. Hence the theorem.

Definition 3.8 *An element $[\ b\ ] \in Z_n$ is called an inverse of an element $[\ a\ ] \in Z_n$ if $[\ a\ ]\ [\ b\ ] = [\ 1\ ]$ in Z_n.*

4 :: MORE EXAMPLES ::

(1) Find the inverse of [15] in Z_{19} and use it to solve $[\ 15\ ]x = [16]$

Solution 4.1 *Because gcd (15,19) = 1, the inverse of [15] exists in Z_{19}. From the Euclidean algorithm we find that*

$$19 = 15{\cdot}1 + 4$$
$$15 = 4{\cdot}3 + 3$$
$$4 = 3{\cdot}1 + 1$$

Hence

$$\begin{aligned} 1 = 4 - 3{\cdot}1 &= (15 - 4{\cdot}3){\cdot}1 \\ &= (4 + 4{\cdot}3) - 15 \\ &= 4{\cdot}4 - 15 \\ &= (19 - 15{\cdot}1){\cdot}4 - 15 \\ &= 19{\cdot}4 - 15(4 + 1) \\ &= 19{\cdot}4 + 15(-5) \end{aligned}$$

This implies that

$$[1] = [19]\ [4] + [15]\ [-5]$$
$$= [0]\ [4] + [15]\ [14]\ \{because\ 14 \equiv -5\ (mod\ 19)\}$$
$$= [15]\ [14]$$

Hence the inverse of [15] *is* [14].

$$Now\ [15]\ [14]x = [14]\ [16]$$
$$implies\ that\ x = [14]\ [16] = [\ -5]\ [\ -3]$$
$$= [15].$$

2). Find all unit elements of Z_{10}.

Solution 4.2 *We know*

$$Z_{10} = \{\ [0],[1],[2],\cdots,[8],[9]\ \}.$$

now $gcd\ (1{,}10) = gcd(3{,}10) = gcd(7{,}10) = gcd\ (9{,}10) = 1.$

Hence,[1],[3],[7],[9] *are the only unit element of* Z_{10}.

Corollary 4.3 *For any positive integer n,Zn (or U(n)) denotes the set of all unit elements of Zn.For example* $Z_{10} = \{\ [1],[3],[7],[9]\ \}$

5 Linear Congruence

Let m be a positive integer and a,b be two integers.If there exists an integer u such that au $\equiv$ b (mod m) then we say that u satisfies the congruence

$$\text{a}x \equiv \text{b (mod m), where } x \text{ is an unknown integer.}$$

Definition 5.1 *A congruence of the form*

$$ax \equiv b \ (mod\ m),$$

where a,b are integer m is a positive integer and x is an unknown integer, is called a linear congruence in one variable x. An integer x_0 is called a solution of $ax \equiv b$ (mod m), if $ax_0 \equiv b$ (mod m).

Example 5.2 $2x \equiv 1$ *(mod 5) is a linear congruence in one variable. Since* $2{\cdot}3 \equiv 1$ *(mod 5) we find that 3 is a solution of this congruence. Now* $8 \equiv 3$ *(mod 5). We find that 8 is a solution of* $2x \equiv 1$ *(mod 5). In fact we can show that if x_0 is an integer such that $x_0 \equiv 3$ (mod 5), i.e, x_0 is a member of the congruence class [3] modulo 5, then x_0 is a solution of the congruence.*

5.1 Properties

Theorem 5.3 *Let a,b and m be integer with m > 0 and gcd(a,m) = 1. Then the congruence $ax \equiv b$ (mod m) has a unique solution. Here **Unique Solution** means one congruence class modulo m.it does not mean one integer.*

Proof 5.4 *Since gcd (a,m) = 1, there exists integers u and t such that au + mt = 1. then aub + mtb =. Hence aub − b = m(−tb).So, we find that*

$$a(ub) \equiv b \ (mod\ m).$$

Hence $x_0 = ub$ is a solution of $ax \equiv b$ (mod m).
Let y_0 be another solution of $ax \equiv b$ (mod m). Then $ay_0 \equiv b$ (mod m).
Now $ax_0 \equiv b$ (mod m) and $ay_0 \equiv b$ (mod m), i.e,$ax_0 \equiv b$ (mod m) and
$b \equiv ay_0$ (mod m).Hence $ax_0 \equiv ay_0$ (mod m).Since gcd(a,m) = 1, it now follows that $x_0 \equiv y_0$ (mod m). Thus we find that any solutions y_0 of $ax \equiv b$ (mod m) is congruent to x_0 (mod m).

Example 5.5 *: Consider the congruence* $12x \equiv 5$ *(mod 7).*

$\Rightarrow$ *since gcd (12,7) = 1, this congruence has a unique solution.*
Here $x = 1$ is a solution.

Supoose now $x = x_0$ is a solution of $12x \equiv 5$ (mod 7).
But $12{\cdot}1 = 5$ (mod 7). Hence $12x_0 \equiv 12{\cdot}1$ (mod 7).
Since gcd (124,7) = 1, it follows that $x_0 \equiv 1$ (mod 7).
So we find that $x = 1$ is a solution of $12x \equiv 5$ (mod 7) and any solution $x = x_0$ of this congruence is congruent to 1 (modulo 7). Hence the solution of the given congruence is $x = 1 + 7k$ where k is any integer ,
i.e, $x \equiv 1$ (mod 7).

Definition 5.6 ***L****et m be a positive integer.For an integer a with gcd(a,m) = 1, an integer b is called an inverse of a modulo m if*

$$ab \equiv 1 \ (mod\ m).$$

From this definition it follows that b is an inverse of a modulo m if and only if b is a solution of the congruence $ax \equiv 1$ (mod m).

Example 5.7 5 *is an inverse of* 9 *modulo* 11,*because* $5{\cdot}9 \equiv 1$ *(mod* 11*).*

6 MORE EXAMPLES

(1) Find all solutions of the congruence $4x \equiv 6$ (mod 4).
Solution 6.1 *Let*

$$4x \equiv 6 \ (mod\ 4). \cdots \ \cdots \ \cdots \ (1)$$

Here gcd(4,4) = 4 and 4 does not divide 6. Hence (1) has no solution.

(2) Find all the (so4) $\cdots \ \cdots \ \cdots$ (1)

Solution 6.2 *Here gcd(3,4) = 1. Hence (1) has a unique solution.*
Now $3{\cdot}(-1) + 4(1) = 1$. Hence $3(-7) + 4(7) = 7$. This shows that

$$3(-7) \equiv 7 \ (mod\ 4).$$

This shows that (-7) is a solution of (1). Now $-7 \equiv 1$ (mod 4). Therefore the given congruence has the solution $x \equiv 1$ (mod 4).

3). Find all solutions of $7x \equiv 4$ (mod 18).

Solution 6.3 *Let*

$$7x \equiv 4 \ (mod\ 18) \cdots \ \cdots \ \cdots \ (1)$$

Here gcd(7,18) = 1. Hence (1) has a unique solution .
Now,

$$
\begin{aligned}
18 &= 7\cdot 2 + 4\\
7 &= 4\cdot 1 + 3\\
4 &= 3\cdot 1 + 1\\
1 &= 4 - 3\cdot 1\\
&= 4 - (7 - 4\cdot 1)\cdot 1\\
&= 4\cdot 2 - 7\\
&= (18 - 7\cdot 2)\cdot 2 - 7\\
&= (18\cdot 2 + 7\cdot(-5).
\end{aligned}
$$

Hence $4 = 18\cdot 8 + 7(-20)$*.This implies*

$$7(-20) \equiv 4 \ (mod\ 18).$$

Hence $x_0 = -20$ *is a solution of (1).*
Now, $-20 \equiv 16$ *(mod* 18*).*
Therefore, the given congruence has the solution $x \equiv 16$ *(mod* 18*).*

4). Find an inverse of 12 modulo 17,if exists.

Solution 6.4 *Consider the congruence* $12x \equiv 1$ *(mod* 17*).*
Since gcd(12,17) = 1, it follows that the congruence $12x \equiv 1$ *(mod* 17*) has a solution.*
Hence there exist an inverse of 12 *modulo* 17*.*
Now,

$$
\begin{aligned}
17 &= 12\cdot 1 + 5\\
12 &= 5\cdot 2 + 2\\
5 &= 2\cdot 2 + 1
\end{aligned}
$$

Hence,

$$
\begin{aligned}
1 &= 5 - 2\cdot 2 = 5 - 2(12 - 5\cdot 2)\\
&= 5 - 2\cdot 12 + 5\cdot 4\\
&= 5\cdot 5 - 2\cdot 12 = 5\cdot(17\text{-}12\cdot 1) - 2\cdot 12\\
&= 5\cdot 17 - 5\cdot 12 - 2\cdot 12\\
&= 12(-7) + 17\cdot 5
\end{aligned}
$$

It implies that $12(-7) \equiv 1$ *(mod* 17*).*
So we find that -7 *is a solution of* $12x \equiv 1$ *(mod* 17*).*

This shows that -7 *is an inverse of* 12 *modulo* 17*.*

5). Solve the congruence $12x \equiv 9$ (mod 15).

Solution 6.5 *Since gcd* $(12,15) = 3$ *and* 3 *divides* 9, *the congruence*

$$12x \equiv 9 \ (mod\ 15) \cdots \ \cdots \ \cdots (1)$$

has exactly three solutions.
Now, $3 = 12(-1) + 15(1)$. *Then* $9 = 12(-3) + 15(3)$.
Accordingly, we have $12(-3) \equiv 9$ *(mod* 15*), and hence* $x_0 = -3$ *is a solution of* $12x \equiv 9$ *(mod* 15*).*
Therefore the three solutions of the congruence (1) are given by

$$x \equiv -3 + \left(\frac{15}{3} \right) i \ (mod\ 15), \ where\ i = 0,1 \ and\ 2$$
$$i.e,\ x \equiv -3 + 5i \ (mod\ 15),\ i = 0,1 \ and\ 2.$$

6). Solve the congruence $72x \equiv 18$ (mod 42).

Solution 6.6 *Since gcd*$(72,42) = 6$ *and* 6 *divides* 18, *the congruence*

$$72x \equiv 18 \ (mod\ 42) \cdots \ \cdots \ \cdots \ (1)$$

has exactly six solutions.
We now find a solution of (1). To find a solution of (1), we may consider the following congruence and find a solution of it

$$12x \equiv 3 \ (mod\ 7) \cdots \ \cdots \ \cdots \ (2)$$

Now, gcd$(12,7) = 1$ *and* $12 = 7{\cdot}1 + 5,\ 7 = 1{\cdot}5 + 2, 5 = 2{\cdot}2 + 1$.
Hence

$$1 = 5 + 2(-2) = 5 + (7 - 5)(-2) = 7(-2) + 5{\cdot}3$$
$$= 7(-2) + (12 - 7{\cdot}1)3 = 12{\cdot}3 + 7(-5).$$

Accordingly $3 = 12{\cdot}9 + 7(-15)$. *Hence* $12{\cdot}9 \equiv 3$ *(mod* 7*). So, we find that* $x_0 = 9$ *is a solution of (2).Hence* $x_0 = 9$ *is a solution of (1).*
Therefore the six solutions of (1) are given by

$$x \equiv 9 + \frac{42}{6} i \ (mod\ 42), i = 0,1,2,3,4,5.$$
$$i.e,\ x \equiv 9 + 7i \ (mod\ 42), i = 0,1,2,3,4,5.$$

$10x \equiv 6$ *(mod* $34)$ $\cdots$ $\cdots$ $\cdots$ *(1)*

Here gcd($10,34$*)* $= 2$ *and* 2 *divides* 6*. Hence (1) has two solutions. Now from (1),*

$$\frac{10}{2} \equiv \frac{6}{2} \left(mod\ \frac{34}{2} \right)$$
$$i.e,\ 5x = 20\ (mod\ 17) \cdots \cdots \cdots\ (2)$$

Now $3 \equiv 20$ *(mod* 17*). Hence from (2)*

$$5x \equiv 20\ (mod\ 17) \cdots \cdots \cdots\ (3)$$

Now gcd($5,17$*)* $= 1$ *.Hence from (3)*

$$\frac{5}{5} \equiv \frac{20}{5}\ (mod\ 17)$$
$$i.e,\ x \equiv 4\ (mod\ 17).$$

Thus $x_0 = 4$ *is a solution ,So the solutions of (1) are given by*

$$x \equiv 4 + 17i\ (mod\ 34),\ i = 0,1.$$

7 Application of Congruences

7.1 Divisibility Tests :

In this section we like to describe some criteria under which a given integer is divisible by anoyher integer. This will be done with the help of congruence. Let m be a positive integer. Then m can be written uniquely as

$$m = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$
$$= (a_k\ a_{k-1} \cdots a_1\ a_0)$$

where a_0,a_1,$\cdots$,a_k are integers such that

$$a_k \neq 0 \text{ and } 0 \leq a_i < 10 \text{ for i} = 0,1,2, \cdots, k.$$

We first develop tests for divisibility by powers of 2.
Let

$$\text{f}(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

Then f(10) = m and f(0) = a_0.

We observe that $10 \equiv 0 \pmod 2$. Hence $f(10) \equiv f(0) \pmod 2$.This shows that m $\equiv a_0 \pmod 2$. It follows that m is divisible by 2 if and only if a_0 is divisible by 2.

Next we observe that $10^i \equiv 0 \pmod 4$ for all i $\geq$ 2. Hence

$$a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 \equiv 0 \pmod{2^2},$$
$$\text{and } a_1 10 + a_0 \equiv a_1 10 + a_0 \pmod{2^2}.$$

From these two congruences it follows that

$$a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$
$$\equiv a_1 10 + a_0 \pmod{2^2}$$
$$\text{or, } m \equiv a_1 10 + a_0 \pmod{2^2}$$
$$\text{i.e, } m \equiv (a_1 a_0)_{10} \pmod{2^2}$$

Hence m is divisible by 2^2 if and only if the number $a_1 a_0$ is divisible by 2^2. Likewise we can prove that m is divisible by 2^3 if and only if the number, a_2, a_1, a_0 is divisible by 8.

7.1.1 Properties:

Theorem 7.1 *Let* $m = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ *, where* a_0,a_1,$\cdots$,a_k *are integers such that* $a_k \neq 0$ *and* $0 \leq a_i < 10$ *for* $i =$ 0,1,2, $\cdots$, k. *Let*

$$S = a_0 + a_1 + \cdots + a_k$$
$$\textit{and } T = a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$$

***T**hen*
(i) m is divisible by 3 *if and only if S is divisible by* 3.
(ii m is divisible by 9 *if and only if S is divisible by* 9.
(iii) m is divisible by 11 *if and only if T is divisible by* 11.

Proof 7.2 *(i)Let*

$$f(x) = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 .$$

Now $f(10) = m$ *and* $f(1) = S$.
since $10 \equiv 1 \pmod 3$*, it follows from that* $f(10) \equiv f(1) \pmod 3$*, i.e,* $m \equiv S \pmod 3$*. Hence m is divisible by* 3 *if and only if S is divisible by* 3.

(ii)$10 \equiv 1 \pmod 9$*. Hence*

$$f(10) \equiv f(1) \ (mod\ 9),\ i.e,\ m \equiv S\ (mod\ 9).$$

It follows that m *is divisible by* 9 *if and if* S *is divisible by* 9.

(iii) $10 \equiv -1$ *(mod* 11*). Hence*

$$f(10) \equiv f(-1)\ (mod\ 11),\ i.e,\ m \equiv T\ (mod\ 11).$$

Consequently m *is divisible by* 11 *if and only if* T *is divisible by* 11.

Example 7.3 *Consider the integer* $m = 71932$.
Here

$$S = 7{+}1{+}9{+}3{+}2{+}5 = 22.$$

since 3 *does not divide* 22, *it follows that* 3 *does not divide* m.*It follows that* 9 *also does not divide* m.

Let $m = 719325$**.**
Then

$$S = 7 + 1 + 9 + 3 + 2 + 5 = 27.$$

Now 3 *divides* 27.
Hence 3 *divides* m. *Also* 9 *divides* 27. *Hence* 9 *divides* m.

L*et* $m = 7175839$.
Now

$$T = 9 - 3 + 8 - 5 + 7 - 1 + 7 = 22$$

Hence 11 *divides* T. *This implies that* 11 *divides* m.

Theorem 7.4 *Let* $m = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0$, *where* $a_0, a_1, \cdots, a_k$ *are integers such that* $a_k \neq 0$ *and* $0 \leq a_i \leq 9$ *for* $i = 0,1,2, \cdots, k$. *Let*

$$t = (a_2a_1a_0)10 - (a5a_4a_3)10 + (a8a_7a_6)_{10} - \cdots .$$

T*hen*
(i) m *is divisible by* 7 *if and only if* t *is divisible by* 7.
(ii) m *is divisible by* 13 *if and only if* t *is divisible by* 13.

Example 7.5 *Let* $m = 11953861057112$.

Then

$m = 1\cdot 10^{13} + 1\cdot 10^{12} + 9\cdot 10^{11} + 5\cdot 10^{10} + 3\cdot 10^{9} + 8\cdot 10^{8} + 6\cdot 10^{7} + 1\cdot 10^{6} + 0\cdot 10^{5} + 5\cdot 10^{4} + 7\cdot 10^{3} + 1\cdot 10^{2} + 1\cdot 10^{1} + 2$

$= (1\cdot 10^2 + 1\cdot 10^1 + 2) + 10^3(0\cdot 10^2 + 5\cdot 10 + 7) + 10^6(8\cdot 10^2 + 6\cdot 10 + 1) + 10^9(9\cdot 10^2 + 5\cdot 10 + 3) + 10^{12}(1\cdot 10 + 1)$.
$= 112 + 10^3\cdot 57 + 10^6\cdot 861 + 10^9\cdot 953 + 10^{12}\cdot 11$.
Now

$$10^3 \equiv -1 \pmod 7,$$
$$10^6 \equiv 1 \pmod 7,$$
$$10^9 \equiv -1 \pmod 7,$$
$$10^{12} \equiv 1 \pmod 7. \text{ Hence}$$

$$m \equiv 112 - 57 + 861 - 953 + 11 \pmod 7$$
$$\text{i.e, } m \equiv -26 \pmod 7.$$

This implies that m *is divisible by* 7 *if and only if* -26 *is divisible by* 7*. But* 7 *does not divide* -26*.Hence the integer* m *is not divisible by* 7*.*

Again,

$$10^3 \equiv -1 \pmod{13},$$
$$10^6 \equiv 1 \pmod{13},$$
$$10^9 \equiv -1 \pmod{13},$$
$$10^{12} \equiv 1 \pmod{13}.$$

Then

$$m = 112 - 57 + 861 - 953 + 11 \pmod{13}$$
$$\text{i.e, } m \equiv -26 \pmod{13}.$$

This shows that m *is divisible by* 13 *if and only if* -26 *is divisible by* 13 *. Since* 13 *divides* -26*, it follows that* 13 *divides* m*.*

8 MORE EXAMPLES

1. Without performing the long divisions, determine whether the integers 761215122 and 51956124 are divisible by 9 or 11 or 3.

Solution 8.1 *Let* $m = 761215122$

$$S = 7 + 6 + 1 + 2 + 1 + 5 + 1 + 2 + 2 = 27.$$

Since 9 *divides* 27 *, it follows that* 9 *divides* m*. Hence* 3 *also divides* m*. Again for* m*,*

$$T = 2–2\ +1\ -\ 5\ +1\ -\ 2\ +1\ -\ 6\ +7 = -3.$$

Since 11 *does not divide* -3 *, it follows that* 11 *does not divide* m*.*

Let n= 51956124*.*
For this n*,*

$$S = 5\ +1\ +9\ +5\ +6\ +1\ +2\ +4 = 33.$$

Since 3 *divides* 33 *and* 9 *does not divide* 33*. It follows that* 3 *divides* n *but* 9 *does not.*

Again,

$$T = 4\ \text{-}\ 2\ +1\ \text{-}\ 6\ +5\ \text{-}\ 9\ +1\ \text{-}\ 5 = -11$$

which is divisible by 11*. So,It follows that* 11 *divides* n*.*

2. Which of the following integers are divisible by 13? (a)501121301 (b)2711111120201

Solution 8.2 *(a) Let* $m = 501121301$*. For this integer*

$$t = 301\ \text{-}\ 121\ +501 = 681.$$

Now 13 *does not divide* 681*. Hence* 13 *does not divide* m*.*

(b) Let $n = 27111111202201$*. for this integer*

$$t = 201\ \text{-}\ 202\ +111\ \text{-}\ 111\ +27 = 26.$$

Since 13 *divides* 26*, it follows that* 13 *divides* n*.*

9 Credit Card Check Digit

In this section we discuss the use of check digit in credit cards : Master card and VISA.Generally a check digit is used in a credit card number to determine if a person has keyed in a number incorrectly .

When dealing with credit cards it is important to relaize that the identification numbers of different cards have different lengths and different prefixes.

In a Master Card the identification number consists of 16 digits and the number starts with 51,or 52, or 53, or 54 or 55.A VISA number is of length 13 or 16 and the identification number starts with the digit 4.

All the above credit cards use congruence mod 10 to detrermine check digit, and in all cases the check digit is the right most digit in the number .Consider a credit card with the following identification number

5548 3742 7983 0696

Here the first two digit indicate that this credit card is a Master card.
In a Master card digits from 2nd place to 3rd place, digits from 2nd place to 4th place , 2nd place to 5th or digits from 2nd place to 6th place from the bank number depending on whether the second digit is 1,2,3 or other.

For example in the above Master card the second digit is 5 . Hence digits from 2nd place to 6th place from the Bank number. For the above card the Bank number is 54837.

The digits after the bank number up to 15th place from the account number of the card holder. for the above card the account number of the card holder is 42 7983 069

Finally the digit in the 16th place is the check digit . In the case of VISA , digits from 2nd place to 6th place from the identification number of the bank and digits from 7th place to 12th place or 7th place to 15th place from the account number, and the digit in the 13th or 16th place is the check digit. The check digit a_k of the identification number $a_1\ a_2\ \cdots\ a_{k-1}\ a_k$ of a Master card or a Visa is obtained from the following algorithm. This algorithm was created by IBM scientist Hans Peter Luhn.

References

[1] Sen, M.K., Chakraborty, B.C.: Introduction to Discrete Mathematics, Books and Allied Ltd.

[2] Mapa, S.K.: Higher Algebra Abstract and Linear, Levant Books.

[3] Dossey, J.A, Albert, D. Otto, Spence, L.E. and Eynden, C.V.(1993): Discrete Mathematics, Harper Collins College publishers.

[4] Johnsonbaugh, R.(1994): Discrete and Combinatorial Mathematics, prentice - Hall.