integer is divisible by 3, then the original integer is divisible by 3.

Also, congruences have their own restrictions. For instance, knowing the number of minutes past the hour is useful but knowing the hour the minutes are past is often more useful. So congruences discard absolute information. Also, if $a \equiv b(\text{mod } n)$ and $c \equiv d(\text{mod } n)$, then it follows that $a^x \equiv b^x(\text{mod } n)$, but not usually $x^c \equiv x^d(\text{mod } n)$ or $a^c \equiv b^d(\text{mod } n)$.

4.2 Congruences

The language of congruences was developed at the beginning of the nineteenth century by famous Mathematician Gauss. The language of congruence is extremely useful in number theory.

Definition 4.2.1. *If a and b are integers, we say that a is congruent to b modulo m if $m|(a-b)$, symbolically denoted by $a \equiv b(\text{mod } m)$. If a and b are incongruent modulo m, then $m \nmid (a-b)$ and is denoted by $a \not\equiv b(\text{mod } m)$.*

Example 4.2.1. *Since $6|(20-2) = 18$, therefore, $20 \equiv 2(\text{mod } 6)$. Similarly, $4 \equiv -5(\text{mod } 9)$ and $300 \equiv 6(\text{mod } 7)$.*

In working with congruences, the following proposition is needed.

Proposition 4.2.1. *If a and b are integers, then $a \equiv b(\text{mod } m)$ if and only if there is an integer l such that $a = b + lm$.*

Proof. Let $a \equiv b(\text{mod } m)$ hold. Then $m|(a-b)$ implies there exists an integer l such that $a = b+lm$. Conversely, if there exists an integer l such that $a = b+lm$ holds, then $a - b = lm$ implies $l|(a-b)$ implies $a \equiv b(\text{mod } m)$. □

Here we have given an example to understand the above theorem lucidly.

Example 4.2.2. *Let us consider $16 \equiv 2(\text{mod } 7)$. Then $16 - 2 = 14$ is divisible by 7 and also we can write 16 as $16 = 2 + 2 \times 7$.*

In the following theorem, we have shown some standard properties related to congruence relation which depicts how an algebraic operations(addition, subtraction, or multiplication) to both sides of a congruence preserves the congruence.

Theorem 4.2.1. *If a, b, c, d and m are integers with $m > 0$ satisfying $a \equiv b($ mod $m)$ and $c \equiv d(\text{mod } m)$, then*

1. $a \pm c \equiv b \pm d(\text{mod } m)$
2. $ac \equiv bd(\text{mod } m)$

3. $a \pm c \equiv b \pm c (\text{mod } m)$

4. $ac \equiv bc (\text{mod } m)$

5. $a (\text{mod } m) \equiv b (\text{mod } m)$.

Proof. 1. Here $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ implies $m|(a-b)$ and $m|(c-d)$, which further implies there exists integers k and l satisfying $a - b = km$ and $c - d = lm$. From the identity $(a \pm c) - (b \pm d) = (a-b) \pm (c-d) = km \pm lm = m(k \pm l)$, we see both $m|\big((a+c) - (b+d)\big)$ and $m|\big((a-c) - (b-d)\big)$ as $k + l$, $k - l$ both are integers. Therefore $a \pm c \equiv b \pm d (\text{mod } m)$.

2. Here $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ implies $m|(a-b)$ and $m|(c-d)$, this again implies that $(c-d)b$, $(a-b)c$ both are divisible by m. Thus, $(a-b)c + (c-d)b = (ac - bd)$ is divisible by m. Therefore $ac \equiv bd (\text{mod } m)$.

3. Since $a \equiv b (\text{mod } m)$, therefore $m|(a-b)$. Now $(a \pm c) - (b \pm c) = a - b$ is divisible by m. Therefore $a \pm c \equiv b \pm c (\text{mod } m)$.

4. Note that $a \equiv b (\text{mod } m) \Rightarrow m|(a-b)$. Now $(a-b)c = ac - bc$ is divisible by m. Therefore $ac \equiv bc (\text{mod } m)$.

5. As $a \equiv b (\text{mod } m)$, then for some integer k we have $a - b = km$. Now k can be written as $k = k_1 - k_2$ where k_1, k_2 are integers. Again, $a - b = (k_1 - k_2)m = k_1 m - k_2 m \Rightarrow a - k_1 m = b - k_2 m = r$. Therefore $r \equiv a (\text{mod } m)$, $r \equiv b (\text{mod } m) \Rightarrow a (\text{mod } m) \equiv b (\text{mod } m)$.

□

Example 4.2.3. *Since* $18 \equiv 3 (\text{mod } 5)$ *and* $22 \equiv 2 (\text{mod } 5)$*, using Theorem (4.2.1) we see that* $40 = 18 + 22 \equiv 3 + 2 \equiv 0 (\text{mod } 5), -4 = 18 - 22 \equiv 3 - 2 \equiv 1 (\text{mod } 5)$ *and* $396 = 18 \cdot 22 \equiv 3 \cdot 2 \equiv 6 (\text{mod } 5)$.

Example 4.2.4. *Since* $27 \equiv 3 (\text{mod } 8)$*, it follows* $34 = 27 + 7 \equiv 3 + 7 \equiv 10 (\text{mod } 8), 23 = 27 - 4 \equiv 3 - 4 \equiv -1 (\text{mod } 8)$*, and* $25 = 27 - 2 \equiv 3 - 2 \equiv 1 (\text{mod } 8)$.

Next before proceeding further, the following example reflects the fact that a congruence is not necessarily retained when divided both sides by an integer.

Example 4.2.5. *We have* $20 = 10 \cdot 2 \equiv 4 \cdot 2 = 8 (\text{mod } 6)$. *But* $5 \not\equiv 2 (\text{mod } 6)$.

However, the next theorem provides us with a well-founded congruence when both sides of a congruence are divided by the same integer.

Theorem 4.2.2. *If a, b, c and m are integers such that $m > 0, d = \gcd(c, m)$ and $ac \equiv bc(\mathrm{mod}\ m)$, then $a \equiv b\big(\mathrm{mod}\ \frac{m}{d}\big)$.*

Proof. Here $ac \equiv bc(\mathrm{mod}\ m)$ implies $m|(ac-bc) = c(a-b)$, which further implies there exists an integer k satisfying $c(a-b) = km$. Dividing both sides by d, we have $\frac{c}{d}(a-b) = \frac{km}{d}$. Since $\gcd\big(\frac{c}{d}, \frac{m}{d}\big) = 1$, it follows $\frac{m}{d}|(a-b) \Rightarrow a \equiv b\big(\mathrm{mod}\ \frac{m}{d}\big)$. □

Theorem(4.2.2) has a corollary that is worth a separate statement.

Corollary 4.2.1. *For any arbitrary positive integers a and b, $lcm(a, b) = ab$ if and only if $\gcd(a, b) = 1$.*

Proof. Obvious. □

Example 4.2.6. *Since $15 = 5(\mathrm{mod}\ 10)$ and $\gcd(5, 10) = 5$, we see that $\frac{15}{5} \equiv \frac{5}{5}\big(\mathrm{mod}\ \frac{10}{5}\big)$ or $3 \equiv 1(\mathrm{mod}\ 2)$.*

Example 4.2.7. *Since $42 \equiv 7(\mathrm{mod}\ 5)$ and $\gcd(5, 7) = 1$, we can conclude that $\frac{42}{7} = \frac{7}{7}\big(\mathrm{mod}\ 5\big)$, or that $6 \equiv 1(\mathrm{mod}\ 5)$.*

In our next theorem using the principle of mathematical induction we have shown that if we increase the exponential power of elements of both sides of a congruence then the congruence relation is preserved.

Proposition 4.2.2. *Let a, b be any two integers. For some integer $m > 0$, if $a \equiv b(\mathrm{mod}\ m)$ holds then for any positive integer n, $a^n \equiv b^n(\mathrm{mod}\ m)$ is also true.*

Proof. We are going to prove this theorem by the principle of mathematical induction. As $a \equiv b(\mathrm{mod}\ m)$ then the result is obviously true for $n = 1$. Let us assume the result is true for $n = k$. Then $a^k \equiv b^k(\mathrm{mod}\ m)$ holds. Now using the property(2) of Theorem (4.2.1)we have $a^{k+1} \equiv b^{k+1}(\mathrm{mod}\ m)$. Thus the result is true for $n = k + 1$. Therefore from the principle of mathematical induction the result is true for all n. □

Example 4.2.8. *Here in this example we have tried to clarify the above proposition by an example. For that let us choose $8 \equiv 3(\mathrm{mod}\ 5)$ then for $n = 3$ we see that $8^3 = 512 \equiv 27 = 3^3(\mathrm{mod}\ 5)$.*

In our following theorem we have shown the way to combine congruences of two same numbers with different congruent moduli. To prove this theorem, first we need to prove the following result.

Result 4.2.1. *Let a be any integer and n_1, n_2 be two positive integers with $n_1|a$, $n_2|a$. Then $lcm(n_1, n_2)|a$.*

Proof. Let l be the least common multiple of n_1 and n_2. If $l \nmid a$, then the division algorithm yields $m = lq + r$ for some integers q and r where $0 \leq r < l$. Then $r = m - lq$. As l and m are multiples of a and b, then there exists integers $t_1, t_2 t_1', t_2'$ such that $m = at_1 = bt_1'$, $l = at_2 = bt_2'$. Therefore $r = at_1 - at_2 q = a(t_1 - t_2 q)$ and $r = bt_1' - bt_2' q = b(t_1' - t_2' q)$. This shows that r is a multiple of both a and b. As l is least, then $r \geq l$. This contradicts the fact $0 < r < l$. Therefore $m = lq \Rightarrow l|m$. □

Now the proof of the main theorem as follows.

Theorem 4.2.3. *For any integers a and b with positive integers $t_1, t_2, \cdots t_k$ if $a \equiv b(\mathrm{mod}\ t_1), a \equiv b(\mathrm{mod}\ t_2), \cdots, a \equiv b(\mathrm{mod}\ t_k)$ then $a \equiv b(\mathrm{mod}\ lcm(t_1, t_2, \cdots, t_k))$.*

Proof. Since $a \equiv b(\mathrm{mod}\ t_1), a \equiv b(\mathrm{mod}\ t_2), \cdots, a \equiv b(\mathrm{mod}\ t_k)$ then we have, $t_1|(a-b)$, $t_2|(a-b), \cdots t_k|(a-b)$. Now by above result we can say that $lcm(t_1, t_2, \cdots, t_k)|(a-b)$. This implies $a \equiv b(\mathrm{mod}\ lcm(t_1, t_2, \cdots, t_k))$. □

In next corollary, we are going to describe an useful consequence of the above theorem.

Corollary 4.2.2. *For any integers a and b with positive relatively prime integers $t_1, t_2, \cdots t_k$ if $a \equiv b(\mathrm{mod}\ t_1), a \equiv b(\mathrm{mod}\ t_2), \cdots, a \equiv b(\mathrm{mod}\ t_k)$ then $a \equiv b($ mod $(t_1 t_2 \cdots t_k))$.*

Proof. Since $a \equiv b(\mathrm{mod}\ t_1), a \equiv b(\mathrm{mod}\ t_2), \cdots, a \equiv b(\mathrm{mod}\ t_k)$, therefore $t_1|(a-b)$, $t_2|(a-b), \cdots t_k|(a-b)$. As $t_1, t_2, \cdots t_k$ are relatively prime integers, therefore $lcm(t_1, t_2, \cdots, t_k) = t_1 t_2 \cdots t_k$. Then Theorem 4.2.3 gives $a \equiv b(\mathrm{mod}\ (t_1 t_2 \cdots t_k))$. □

In the following proposition we have seen that the congruence relation is nothing but an equivalence relation.

Proposition 4.2.3. *Let m be any non-zero integer. Define a relation '$\equiv \mathrm{mod}\ m$' on set of integers $\mathbb{Z}$ by $a \equiv b(\mathrm{mod}\ m)$ if and only if $m|(a-b)$. The relation '$\equiv \mathrm{mod}\ m$' is an equivalence relation.*

Proof. A relation on a set is said to be equivalence if it is reflexive, symmetric and transitive.

1. Reflexivity: Since $m|(a-a)$, we see that $a \equiv a(\mathrm{mod}\ m)$.

2. Symmetricity: If $a \equiv b(\text{mod } m)$, then $m|(a-b)$. Hence there exists an integer l such that $a-b=lm$. This shows that $(-l)m = b-a \Rightarrow m|(b-a)$. Consequently, $b \equiv a(\text{mod } m)$.

3. Transitivity: Let $a \equiv b(\text{mod } m)$ and $b \equiv c(\text{mod } m)$. Then $m|(a-b)$ and $m|(b-c)$ holds. Hence there exists integers k and l such that $a-b=km$ and $b-c=lm$. Therefore $a-c=(a-b)+(b-c)=km+lm=(k+l)m$. Consequently, $m|(a-c)$ implies $a \equiv c(\text{mod } m)$.

□

Infact this equivalence relation is also called congruence relation. From the basic concept of algebra we can say that this equivalence relation always forms an equivalence class. In this case this is called congruence class. For example if we choose a positive integer 5 which leaves the remainder $0, 1, 2, 3, 4$ when divides any integer. Here if we choose remainder as 1 then we have the set of integers $\{6, 11, 16, \cdots\}$ whose all the elements have remainder 1 when divided by 5. For that the above set can be written as [1] which is a congruence class modulo 5. Thus the definition of congruence class as follows.

Definition 4.2.2. *Let m be a positive integer and a be any integer then set of integers, $\{b : b \equiv a(\text{mod } m)\}$ is called congruence class modulo m and denoted by $[a]$.*

From the above definition of congruence class another important fact we can discuss on integers. If we choose a set of integers say, $\{5, 21, -2, 62, 34\}$ then for congruent modulo 5 we have, $5 \equiv 0(\text{mod } 5)$, $21 \equiv 1(\text{mod } 5)$, $62 \equiv 2(\text{mod } 5)$, $-2 \equiv 3(\text{mod } 5)$, $34 \equiv 4(\text{mod } 5)$. Here we see that each of the elements of the above set are congruent modulo 5 with exactly one of the set $\{0, 1, 2, 3, 4\}$. Then this arbitrary set $\{5, 21, -2, 62, 34\}$ is said to be a complete set of residue modulo 5. Now we are in the position to define that arbitrary set.

Definition 4.2.3. *An arbitrary set of m integers $\{a_1, a_2, \cdots, a_m\}$ is said to be a complete set of residue modulo m or CRS$(\text{mod } m)$ if every integer of the set is congruent modulo m to exactly one of $a_1, a_2, \cdots, a_m$. More specifically if,*

1. *$a_i \not\equiv a_j(\text{mod } m)$, $\forall i \neq j$, $i, j = 1, 2, \cdots m$*

2. *For each integer n, there exists a unique integer a_j such that $n \equiv a_j(\text{mod } m)$, $j = 1, 2, \cdots m$.*

Obviously the set $\{0, 1, 2, \cdots, m-1\}$ forms a CRS$(\text{mod } m)$. It is called trivial CRS$(\text{mod } m)$. For an example if we choose $m = 5$ then the set $\{0, 1, 2, 3, 4\}$ is the trivial CRS$(\text{mod } 5)$.

Now in the following theorems we have shown here that addition and multiplication of any arbitrary element with all the elements of a complete residue system under some conditions preserves the properties of complete residue system.

Theorem 4.2.4. *If* $\{a_1, a_2, \cdots, a_m\}$ *is a set of complete residue system modulo* m *and* c *be any integer then* $\{a_1 + c, a_2 + c, \cdots, a_m + c\}$ *is also a set of complete residue system modulo* m.

Proof. It's suffices to show that all the elements of $\{a_1 + c, a_2 + c, \cdots, a_m + c\}$ are distinct under congruent modulo m. Since $\{a_1, a_2, \cdots, a_m\}$ is a set of complete residue system modulo m then $a_i \not\equiv a_j$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. Thus $a_i - a_j$ is not divisible by m. Also, $(a_i + c) - (a_j + c) = a_i - a_j$ which follows that $(a_i + c) - (a_j + c)$ is not divisible by m. Therefore $a_i + c \not\equiv a_j + c (\text{mod } m)$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. This proves the theorem. □

Theorem 4.2.5. *If* $\{a_1, a_2, \cdots, a_m\}$ *is a set of complete residue system modulo* m *and* c *be any integer prime to* m, *then* $\{ca_1, ca_2, \cdots, ca_m\}$ *is also a set of complete residue system modulo* m.

Proof. Again here to prove this theorem we are to show all the elements of $\{ca_1, ca_2, \cdots, ca_m\}$ are distinct under congruent modulo m. Since $\{a_1, a_2, \cdots, a_m\}$ is a set of complete residue system modulo m then $a_i \not\equiv a_j$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. Thus $a_i - a_j$ is not divisible by m. Also we have $ca_i - ca_j = c(a_i - a_j)$. Now c is prime to m implies $\gcd(c, m) = 1$ and $a_i - a_j$ is not divisible by m. Combining these two concepts we can conclude that $ca_i - ca_j$ is not divisible by m. Therefore $ca_i \not\equiv ca_j (\text{mod } m)$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. This proves the assertion of this theorem. □

Combining the above two theorems, lead us to the following straightforward corollary:

Corollary 4.2.3. *If* $\{a_1, a_2, \cdots, a_m\}$ *is a set of complete residue system modulo* m *and* c *be any integer prime to* m, *then* $\{ca_1 + d, ca_2 + d, \cdots, ca_m + d\}$ *is also a set of complete residue system modulo* m *for any integer* d.

4.3 Worked out Exercises

Problem 4.3.1. *Give an example to show that* $a^2 = b^2 (\text{mod } n)$ *need not imply that* $a \equiv b (\text{mod } n)$.

Solution 4.3.1. *Let us consider* $a = 5, b = 4, m = 3$. *Since* $3\big|(25 - 16) = 9$, *therefore* $5^2 \equiv 4^2 (\mathrm{mod}\ 3)$. *But* $5 \not\equiv 4 (\mathrm{mod}\ 3)$.

Problem 4.3.2. *What is the remainder when the sum* $1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$ *is divided by* 4*?*

Solution 4.3.2. *Here*

$$\begin{aligned} 1^5 &\equiv 1(\ \mathrm{mod}\ 4) & 1 \equiv 5 \equiv 9 \ldots (\ \mathrm{mod}\ 4) \\ 32 = 2^5 &\equiv 0(\ \mathrm{mod}\ 4) & 2 \equiv 6 \equiv 10 \ldots (\ \mathrm{mod}\ 4) \\ 243 = 3^5 &\equiv 3(\ \mathrm{mod}\ 4) & 3 \equiv 7 \equiv 11 \ldots (\ \mathrm{mod}\ 4) \\ 4^5 &\equiv 0(\ \mathrm{mod}\ 4) & 4 \equiv 8 \equiv 12 \ldots (\ \mathrm{mod}\ 4). \end{aligned}$$

Each block of four numbers will have same remainder sum. Since $1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 0 + 3 + 0 \equiv 4 \equiv 0 (\mathrm{mod}\ 4)$, *therefore* 25 *blocks will all have remainder* 0 *implies entire remainder is* 0.

Problem 4.3.3. *For* $n \geq 1$, *use congruence theory to establish* $27\big|(25^{n+1} + 5^{n+2})$.

Solution 4.3.3. *Here* $32 \equiv 5 (\mathrm{mod}\ 27) \Rightarrow 2^5 \equiv 5 (\mathrm{mod}\ 27)$. *Now*

$$\begin{aligned} 2^{5n} &\equiv 5^n(\ \mathrm{mod}\ 27) \\ 2 \cdot 2^{5n} &\equiv 2 \cdot 5^n(\ \mathrm{mod}\ 27). \\ \therefore\ 2^{5n+1} + 2^{5n+2} &\equiv 2 \cdot 5^n + 5^{n+2}(\ \mathrm{mod}\ 27) \\ &\equiv 5^n(5 + 25)(\ \mathrm{mod}\ 27) \\ &\equiv 5^n \cdot 27(\ \mathrm{mod}\ 27) \\ &\equiv 0(\ \mathrm{mod}\ 27). \end{aligned}$$

Problem 4.3.4. *Find the remainder when the sum* $1! + 2! + 3! + \ldots + 100!$ *is divided by* 18.

Solution 4.3.4. *Note that* $6! \equiv 0 (\mathrm{mod}\ 18) \Rightarrow (6 + n)! \equiv 0 (\mathrm{mod}\ 18)$ *for* $n \in \mathbb{Z}$. *Then*

$$\begin{aligned} 1! + 2! + 3! + \cdots + 100! &\equiv (1! + 2! + 3! + 4! + 5!)(\ \mathrm{mod}\ 18) \\ &\equiv 153(\ \mathrm{mod}\ 18) \\ &\equiv 9(\ \mathrm{mod}\ 18). \end{aligned}$$

Therefore the remainder is 9.

Problem 4.3.5. *Prove for any integer* a, $a^3 \equiv 0, 1,$ *or* $6 (\mathrm{mod}\ 7)$.

Solution 4.3.5. *By division Algorithm, we have* $a = 7k + r,\ 0 \leq r < 7$. *Now*

$$\begin{aligned} a = 7k : a^3 &= (7k)^3 = 7 \cdot 7^2k^3 \Rightarrow a^3 \equiv 0(\mod 7). \\ a = 7k+1 : a^3 &= (7k+1)^3 = (7k)^3 + 3\cdot(7k)^2 + 3\cdot 7k + 1. \\ &\therefore\ a^3 - 1 = 7[7^2k^3 + 3\cdot 7k^2 + 3\cdot k] \Rightarrow a^3 \equiv 1(\mod 7) \end{aligned}$$

By similar way, $a = 7k+2 : a^3 \equiv 1(\mod 7)$

$$\begin{aligned} a = 7k+3 &: a^3 \equiv 6(\mod 7) \\ a = 7k+4 &: a^3 \equiv 1(\mod 7) \\ a = 7k+5 &: a^3 \equiv 6(\mod 7) \\ a = 7k+6 &: a^3 \equiv 1(\mod 7). \end{aligned}$$

Problem 4.3.6. *If* $\{a_1, a_2, \ldots, a_n\}$ *is a complete set of residues modulo* n *and* $\gcd(a, n) = 1$, *prove that* $\{aa_1, aa_2, \ldots, aa_n\}$ *is also a complete set of residues modulo* n.

Solution 4.3.6. *Consider* aa_i *and* aa_j *with* $i \neq j,\ 1 \leq i < j \leq n$. *If* aa_i *and* aa_j *are congruent moduli* n, *then* $aa_i - aa_j = kn \Rightarrow a(a_i - a_j) = kn$ *for some* k. *Since* $\gcd(a, n) = 1$, *Euclid's Lemma gives* $n \big| (a_i - a_j)$, *contradicting the fact* $a_i \not\equiv a_j$. *Therefore* $aa_i \equiv aa_j$. *Hence by Proposition 4.2.1, the statement follows.*

Problem 4.3.7. *Find the remainder when* 10^{515} *is divided by* 7.

Solution 4.3.7. *Here* $515 = 85 \times 6 + 5 \Rightarrow 10^{515} = (10^6)^{85} \cdot 10^5$. *Further,*

$$\begin{aligned} & 10^2 \equiv 2(\mod 7) \\ \Rightarrow\ & 10^6 \equiv 2^3 \equiv 1(\mod 7) \\ \Rightarrow\ & (10^6)^{85} \equiv 1(\mod 7) \\ \Rightarrow\ & 10^{515}(10^6)^{85} \cdot 10^5 \equiv 1 \cdot 5 \equiv 5(\mod 7). \end{aligned}$$

So the desired remainder is 5.

Problem 4.3.8. *Verify that if* $a \equiv b(\mod n_1)$ *and* $a \equiv b(\mod n_2)$, *then* $a \equiv b(\mod n)$, *where the integer* $n = lcm(n_1, n_2)$. *Hence whenever* n_1 & n_2 *are relatively prime,* $a \equiv b(\mod n_1 n_2)$.

Solution 4.3.8. *Let* $k_1, k_2 \in \mathbb{Z}$ *be such that* $a - b = k_1 n_1$, & $a - b = k_2 n_2$. *Let* $d = \gcd(n_1, n_2)$. *Then* $\exists\ r \in \mathbb{Z}$ *such that* $n_1 = dr$.

$$\therefore\ a - b = k_2 n_2 = k_2 n_2 \frac{n_1}{dr} = \frac{k_2}{r}\frac{n_1 n_2}{d}.$$

But $\frac{n_1 n_2}{d} = lcm(n_1, n_2)$*[refer to Theorem 2.5.1].*

$$\therefore\ a - b = \frac{k_2}{r} lcm(n_1, n_2).$$

Finally, our aim is to show $\frac{k_2}{r} \in \mathbb{Z}$*. Let* $s \in \mathbb{Z}$ *be such that* $n_2 = ds$*. Since* $a - b = k_1 n_1 = k_2 n_2$*, then* $k_1 dr = k_2 ds \Rightarrow k_1 r = k_2 s$*. Since* $\gcd(r, s) = 1$*, therefore* r *divides* k_2*. This shows that* $\frac{k_2}{r} \in \mathbb{Z}$*.*

Problem 4.3.9. *Show that* 41 *divides* $2^{40} - 1$*.*

Solution 4.3.9. *Here* $2^{20} = (2^5)^4 = (32)^4$*. This shows that* $2^{20} = (32)^4 \equiv (-9)^4 \equiv (81)^2 (\text{mod } 41)$*. However* $81 \equiv -1 (\text{mod } 41) \Rightarrow 2^{20} \equiv 1 (\text{mod } 41)$*. Hence* $41 \big| (2^{20} - 1)$*.*

Problem 4.3.10. *Justify,* $a^k \equiv b^k (\text{mod } n)$ *and* $k \equiv j (\text{mod } n)$ *need not imply that* $a^j \equiv b^j (\text{mod } n)$*.*

Solution 4.3.10. *Since* $4 \equiv 9 (\text{mod } 5)$*, therefore*

$$2^2 \equiv 3^2 (\text{ mod } 5),$$
$$2 \equiv 7 (\text{ mod } 5),$$
$$2^7 \not\equiv 3^7 (\text{ mod } 5) [\textit{Verify!}].$$

Problem 4.3.11. *If* $\gcd(a, n) = 1$*, then prove that the integers* $c, c + a, c + 2a, c + 3a, \ldots, c + (n-1)a$ *form a complete set of residues modulo* n *for any* c*.*

Solution 4.3.11. *Consider* $c + ra$ & $c + sa$*,* $r \neq s$*,* $0 \leq r, s \leq n - 1$*. Suppose* $s > r$*.*

$$\therefore\ c + sa - (c + ra) = (s - r)a.$$

Note that $s \leq n - 1$*,* $r \leq n - 1$ *together implies* $s - r < n$*. Therefore* $n \nmid (s - r)$*. Since* $\gcd(a, n) = 1$*, therefore* $\nexists\ k \in \mathbb{Z}$ *such that* $(s - r)a = nk \Rightarrow c + sa \not\equiv c + ra$*. This completes the solution.*

Problem 4.3.12. *Find all CRS modulo* 6*.*

Solution 4.3.12. *Here the set* $\{0, 1, 2, 3, 4, 5\}$ *forms trivial CRS modulo* 6*. By virtue of Theorem(4.2.4)and Theorem(4.2.5), we conclude that* $\{k, k + a, k + 2a, k + 3a, k + 4a, k + 5a\}$ *forms a CRS modulo* 6*, where* k *is any arbitrary integer and* a *is an integer prime to* 6*.*

Problem 4.3.13. *Prove that the integer* $53^{103} + 103^{53}$ *is divisible by* 39*.*

Solution 4.3.13. *Note that* $39 = 3{\cdot}13,\ 53 = 3{\cdot}17{+}2 = 3{\cdot}18{-}1,\ 103 = 34{\cdot}3{+}1$. *Now*

$$\begin{aligned} 53 &\equiv -1(\bmod 3) & 53 &\equiv 1(\bmod 13) \\ 53^{103} &\equiv (-1)^{103}(\bmod 3) & 53^{103} &\equiv 1(\bmod 13). \end{aligned}$$

Furthermore,

$$\begin{aligned} 103 &\equiv 1(\bmod 3) & 103 &\equiv -1(\bmod 13) \\ 103^{53} &\equiv 1^{53}(\bmod 3) & 103^{53} &\equiv -1(\bmod 13). \end{aligned}$$

Adding those congruences with respect to modulo 3 *and modulo* 13 *we get,* $53^{103} + 103^{53} \equiv 0(\bmod 3)$ *and* $53^{103} + 103^{53} \equiv 0(\bmod 13)$ *respectively. This yields* $3\big|(53^{103} + 103^{53}),\ 13\big|(53^{103} + 103^{53})$. *Since* $\gcd(3, 13) = 1$, *therefore* $3 \cdot 13 = 39\big|(53^{103} + 103^{53})$.

4.4 Linear Congruences

The present section deals with the notion of linear equation in the sense of congruence relation. Consider a linear equation of the form $2x + 3y = 5$ with two unknown integers x and y. Then it can be expressed as $y = \dfrac{5 - 2x}{3}$. If we consider $\dfrac{5 - 2x}{3}$ as an integer then the above linear equation can be written as $2x \equiv 5(\bmod y)$. The foregoing congruence relation with unknown integer x is said to be linear congruence equation, whose definition is as follows:

Definition 4.4.1. *A congruence of the form* $ax \equiv b(\bmod m)$ *where* a, b, m *are integers with* $m > 0$ *and* x *an unknown integer, is called linear congruence in one variable.*

Here we have dealt with the various aspects of linear congruences. In the beginning, we have tried to relate linear congruences with the linear Diophantine equation of two variables x and y. Our following theorem is based on that.

Theorem 4.4.1. *Let* (x_0, y_0) *be an integral solution of* $ax + by = c$ *for some integers* a, b, c *where* a, b *are non zero integers then* x_0 *is the solution of* $ax \equiv c(\bmod m)$ *considering* $m = |b|$. *Conversely, if* x_0 *is a solution of the above congruence then there is an integer* y_0 *for which* (x_0, y_0) *is a solution of* $ax{+}by = c$.

Proof. Since (x_0, y_0) satisfies $ax + by = c$ then we have $by_0 = c - ax_0$. This shows that b divides $ax_0 - c$. Therefore $m = |b|$ divides $ax_0 - c$ and x_0 becomes a solution of $ax \equiv c(\text{mod } m)$.

For the converse part we have x_0 a solution of $ax \equiv c(\text{mod } m)$. Since $m = |b|$ divides $ax_0 - c$ then for some integer y_0 we can write $ax_0 - c = by_0$. This proves that (x_0, y_0) satisfies $ax + by = c$. □

Now we are going to illustrate the above fact by following examples.

Example 4.4.1. Here we have shown that a linear Diophantine equation $221x + 35y = 11$ can be solved using linear congruence. Firstly the equation $221x + 35y = 11$ has been written as $221x \equiv 11(\text{mod } 35)$. Here the solution of this congruence equation is $x \equiv 1(\text{mod } 35)$. Then we have $x = 1 + 35t$ for some integer t. Here $x_0 = 1$ is the particular value of x and $y_0 = \frac{1}{35}[11 - 221 \cdot 1] = -6$ is particular value of y . Therefore $y = -6 - 221t$, $x = 1 + 35t$ is the general solution.

Example 4.4.2. Let us choose the congruence equation $5x \equiv 2(\text{mod } 26)$ and this has been written as $5x - 26y = 2$ for some integer y. Here $\gcd(5, 26) = 1$ can be written as $1 = 26 - 5 \cdot 5$. Thus here the particular value of x is $x_0 = -10$. Then we have $x = -10 - 26t$ for some integer t. Therefore $x \equiv -10 \equiv 16($ mod 26) is the solution of above congruence.

Here in the Example 4.4.1 we have solved the linear Diophantine equation by converting it to linear congruence equation and also from the Example 4.4.2 we have solved the linear congruence equation by converting it to linear Diophantine equation. So from the above two examples we can say that the linear congruences and linear diophantine equations are relatable.

In particular, we have seen that $x = x_0$ is a solution of $ax \equiv b(\text{mod } m)$ then any integer $x_1 \equiv x_0(\text{mod } m)$ is also a solution. Thus if we can find a particular solution x_0 of $ax \equiv b(\text{mod } m)$, then all the elements belonging to the class of x_0, are the solutions of $ax \equiv b(\text{mod } m)$. For instance, choose $4x \equiv ($ mod 5) where $x = 2$ is a solution. Now it's obvious that all the elements of [2] such as $x = 7, 12$ and so on are its solutions. Now the question arises, how many incongruent solutions modulo m do exist?. The following theorem reflects, under which condition it is possible to find a solution of a linear congruence equation and if the solutions exist, how many of them are incongruent modulo m.

Theorem 4.4.2. *Let a, b, m are integers with $m > 0$ then the linear congruence $ax \equiv b(\text{mod } m)$ has a solution if and only if $d|b$, where $d = \gcd(a, m)$. If $d|b$ then it has exactly d numbers of incongruent solutions.*

Proof. Theorem 4.4.1 asserts that any linear congruence $ax \equiv b(\text{mod } m)$ is equivalent to linear Diophantine equation $ax - my = b$, for any integer y. So for particular integer x_0 satisfying $ax_0 \equiv b(\text{mod } m)$ we get an integer y_0 satisfying $ax_0 - my_0 = b$. Again by virtue of Theorem 2.7.1, if $d \nmid b$ then $\nexists$ any solutions. Also, if $d|b$ then the Diophantine equation $ax + mk = b$ have infinite number of solutions given by $x = x_0 + (\frac{m}{d})n,\ k = k_0 - (\frac{a}{d})n$ for some integer n. Here k_0 is a particular value for k. Then comparing both the diophantine equations, yields $y = -k$. Thus, the solutions of $ax - my = b$ are given by

$$x = x_0 + (\frac{m}{d})n,\ -y = -k_0 - (\frac{a}{d})n \Rightarrow y = k_0 + (\frac{a}{d})n.$$

Next, to determine the number of incongruent solutions of $ax \equiv b(\text{mod } m)$, consider $x_1 = x_0 + (\frac{m}{d})n_1$ and $x_2 = x_0 + (\frac{m}{d})n_2$ as two solutions of $ax \equiv b($ mod $m)$ for some integers n_1, n_2. If these two are congruent then,

$$x_0 + (\frac{m}{d})n_1 \equiv x_0 + (\frac{m}{d})n_2(\text{ mod } m).$$
$$\therefore (\frac{m}{d})n_1 \equiv (\frac{m}{d})n_2(\text{ mod } m)$$

Now, $\gcd(m, \frac{m}{d}) = \frac{m}{d}$ and $(\frac{m}{d})|m$. So using Theorem 4.2.2 we obtain $n_1 \equiv n_2($ mod $m)$. This proves that $x = x_0 + (\frac{m}{d})n$ has exactly d numbers of incongruent solutions as n ranges through a complete residue system of residues modulo d. □

In the above theorem, taking a and m as relatively prime integers gives a straightforward corollary:

Corollary 4.4.1. *If a and m are relatively prime then the linear congruence $ax \equiv b(\text{mod } m)$ has a unique solution modulo m.*

Next our aim is to exemplify the foregoing theorem and corresponding corollary by an example:

Example 4.4.3. *Consider the linear congruence $8x \equiv 16(\text{mod } 24)$. Since $\gcd(8, 24) = 8$ and $8|16$, using the last theorem our aim is to show that $\exists$ 8 incongruent solutions modulo 24. Here $x_0 = 2$ is a particular solution. Then $x \equiv 2 + (\frac{24}{8})t \equiv 2 + 3t(\text{mod } 24)$ are the incongruent solutions modulo 24 where $t = 0(1)7$. Thus the solutions are $x \equiv 2, 5, 8, 11, 14, 17, 20, 23(\text{mod } 24)$. Now, if we choose the congruence $8x \equiv 16(\text{mod } 23)$ then $\gcd(8, 23) = 1$. Then by virtue of the last corollary, it has only one incongruent solution modulo 23 which is $x \equiv 2(\text{mod } 23)$.*

Example 4.4.4. *Consider the linear congruence* $8x \equiv 16(\mathrm{mod}\ 24)$. *Since* $\gcd(8, 24) = 8$ *and* $8|16$, *using the last theorem our aim is to show that* $\exists$, 8 *incongruent solutions modulo* 24. *Here* $x_0 = 2$ *is a particular solution. Then* $x \equiv 2+(\frac{24}{8})t \equiv 2 + 3t(\mathrm{mod}\ 24)$ *are the incongruent solutions modulo* 24 *where* $t = 0(1)7$. *Thus the solutions are* $x \equiv 2, 5, 8, 11, 14, 17, 20, 23(\mathrm{mod}\ 24)$. *Now, if we choose the congruence* $8x \equiv 16(\mathrm{mod}\ 23)$ *then* $\gcd(8, 23) = 1$. *Then by virtue of the last corollary, it has only one incongruent solution modulo* 23 *which is* $x \equiv 2(\mathrm{mod}\ 23)$.

After solving a linear congruence equation, we are turning our discussion to solve a simultaneous system of linear congruences. This system actually came from Chinese puzzles as early as the first century A.D. In number theory, the Chinese remainder theorem gives a unique solution to simultaneous linear congruences with coprime moduli. In its basic form, the Chinese remainder theorem will determine a number p that, when divided by some given divisors, leaves given remainders.

The earliest known statement of the theorem is by the Chinese mathematician Sun-tzu Suan-ching in the 3rd century AD, whose original formulation was $x \equiv 2(\mathrm{mod}\ 3) \equiv 3(\mathrm{mod}\ 5) \equiv 2(\mathrm{mod}\ 7)$ with the solution $x = 23 + 105k$ where $k \in \mathbb{Z}$.

The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers.

Theorem 4.4.3. *(Chinese Remainder Theorem): Let* $m_1, m_2, \cdots m_k$ *be pairwise relatively prime integers. Then for k number of integers* $a_1, a_2, \cdots a_k$ *the system of congruences* $x \equiv a_1(\mathrm{mod}\ m_1), x \equiv a_2(\mathrm{mod}\ m_2), \cdots x \equiv a_k(\mathrm{mod}\ m_k)$ *has a unique solution modulo* $M = m_1 m_2 \cdots m_k$.

Proof. Let $M_r = \dfrac{M}{m_r} = m_1 m_2 \cdots m_{r-1} m_{r+1} \cdots m_k$ is the product of all integers omitting m_r, shows that $\gcd(M_r, m_r) = 1$. Then from the Corollary 4.4.1 it is possible to find a unique solution x_r of the linear congruence $M_r x \equiv 1(\mathrm{mod}\ m_r)$. Our task is to show that the integer $\tilde{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots a_k M_k x_k$ is a simultaneous solution of the above system. First our aim is to check, $\tilde{x}$ satisfies $x \equiv a_1(\mathrm{mod}\ m_1)$. Since all the integers $M_2, M_3, \cdots M_k$ contain m_1 as a factor so $a_i M_i x_i \equiv 0(\mathrm{mod}\ m_1)$ for all $i = 2, 3, \cdots k$, then $\tilde{x} \equiv a_1 M_1 x_1(\mathrm{mod}\ m_1)$. As $M_1 x_1 \equiv 1(\mathrm{mod}\ m_1)$ it follows that $\tilde{x} \equiv a_1(\mathrm{mod}\ m_1)$. This shows that $\tilde{x}$ satisfies the linear congruence $x \equiv a_1(\mathrm{mod}\ m_1)$. Proceeding as above, we can show that $\tilde{x}$ also satisfies other congruences.

To proceed for the uniqueness part, let x' and $\tilde{x}$ be its two solutions. Then we have $x' \equiv a_r \equiv \tilde{x} (\text{mod } m_r)$ for $r = 1, 2, \cdots, k$. Therefore m_r divides $(x' - \tilde{x})$ for each $r = 1, 2, \cdots, k$. Since all m_r's are relatively prime then from Corollary 2.4.1 we have $M = m_1 m_2 \cdots m_k | (x' - \tilde{x})$. This implies $x' \equiv \tilde{x} (\text{mod } M = m_1 m_2 \cdots m_k)$. Therefore $\tilde{x}$ is the unique solution of the given system. □

In the following example, we have illustrated the preceding theorem lucidly.

Example 4.4.5. *Let us consider a system of simultaneous linear congruences as* $x \equiv 2 (\text{mod } 3)$, $x \equiv 4 (\text{mod } 5)$, $x \equiv 5 (\text{mod } 7)$. *Here* $M = 3 \cdot 5 \cdot 7 = 105$ *then we have* $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$. *As* $M_r x_r \equiv 1 (\text{mod } m_r)$ *so the linear congruences are* $35x_1 \equiv 1 (\text{mod } 3)$, $21x_2 \equiv 1 (\text{mod } 5)$, $15x_3 \equiv 1 (\text{mod } 7)$. *Those linear congruences are satisfied by* $x_1 = 2$, $x_2 = 1$, $x_3 = 1$ *respectively. Thus a solution of the system is given by* $\tilde{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 = 140 + 84 + 75 \equiv 299 (\text{mod } 105)$. *Thus the unique solution of this system is* $\tilde{x} \equiv 89 (\text{mod } 105)$.

4.5 Worked out Exercises

Problem 4.5.1. *Solve:* (1) $36x \equiv 8 (\text{mod } 102)$ (2) $140x \equiv 133 (\text{mod } 301)$.

Solution 4.5.1. *1. Since* $\gcd(36, 102) = 6 \nmid 8$, *therefore* $\nexists$ *any solution.*

2. Here $140 = 2^2 \cdot 5 \cdot 7$, $301 = 7 \times 43$. *Therefore* $\gcd(140, 301) = 7$ *and* $7 | 133$. *Hence* 7 *incongruent solutions do exist. Dividing both sides of the congruence by* 7 *we have,*

$$
\begin{aligned}
20x &\equiv 19 (\text{ mod } 43) \\
40x &\equiv 38 \\
43x - 40x &\equiv 43 - 38 (\text{ mod } 43) \\
3x &\equiv 5 (\text{ mod } 43) \\
42x &\equiv 70 (\text{ mod } 43) \\
43x - 42x &\equiv 86 - 70 (\text{ mod } 43) \\
x &\equiv 16 (\text{ mod } 43). \\
\therefore\ x &\equiv 16 + 43t, \text{ for } t = 0, 1, 2, 3, 4, 5, 6. \\
\therefore\ x &\equiv 16, 59, 102, 145, 188, 231, 274 (\text{ mod } 301).
\end{aligned}
$$

Problem 4.5.2. *Using congruences, solve the Diophantine equations:* $12x + 25y = 331$.

Solution 4.5.2. *Note that*

$$\begin{aligned}
12x &\equiv 331(\mod 25),\\
\textit{or, } 24x &\equiv 662(\mod 25),\\
\textit{or, } 25x - 24x &\equiv 662 - 650(\mod 25),\\
\textit{or, } x &\equiv 12(\mod 25).\\
\therefore\ x &= 12 + 25u,\ \forall u \in \mathbb{Z}.\\
\textit{Further, } 25y &\equiv 331(\mod 12),\\
\textit{or, } 25y - 24y &\equiv 331 - 324(\mod 12),\\
\textit{or, } y &\equiv 7(\mod 12).\\
\therefore\ y &= 7 + 12v,\ \forall v \in \mathbb{Z}.\\
\therefore\ 12x + 25y &= 12(12 + 25u) + 25(7 + 12v),\\
\textit{or, } 331 &= 319 + 300u + 300v,\\
\textit{or, } 12 &= 25u + 25v.\\
\therefore\ x &= 12 + 25u = 24 - 25v.
\end{aligned}$$

Hence $x = 24 - 25v,\ y = 7 + 12v$ *for* $v \in \mathbb{Z}$.

Problem 4.5.3. *Solve:* $x \equiv 5(\mathrm{mod}\ 6),\ x \equiv 4(\mathrm{mod}\ 11),\ x \equiv 3(\mathrm{mod}\ 17)$.

Solution 4.5.3. *Here*

$$\begin{aligned}
x &\equiv 5(\mod 6) & N &= 6 \cdot 11 \cdot 17 = 1122.\\
x &\equiv 4(\mod 11) & N_1 &= 11 \cdot 17 = 187.\\
x &\equiv 3(\mod 17) & N_2 &= 6 \cdot 17 = 102.\\
& & N_3 &= 6 \cdot 11 = 66.
\end{aligned}$$

Now $187x_1 \equiv 1(\mathrm{mod}\ 6) \Rightarrow 187x_1 - 186x_1 = x_1 \equiv 1(\mathrm{mod}\ 6)$. *Again*

$$\begin{aligned}
102x_2 &\equiv 1(\mod 11) & 66x_3 &\equiv 1(\mod 17)\\
102x_2 - 99x_2 = 3x_2 &\equiv 1(\mod 11) & 66x_3 - 68x_3 = -2x_3 &\equiv 1(\mod 17)\\
21x_2 &\equiv 7(\mod 11) & 18x_3 &\equiv -9(\mod 17)\\
21x_2 - 22x_2 = -x_2 &\equiv 7(\mod 11) & 18x_3 - 17x_3 = x_3 &\equiv -9(\mod 17).
\end{aligned}$$

$$\therefore\ x_1 = 1,\ x_2 = -7,\ x_3 = -9.$$

$$\therefore\ a_1N_1x_1 = 5 \cdot 187 \cdot 1,\ a_2N_2x_2 = 4 \cdot (102) \cdot (-7),\ a_3N_3x_3 = 3 \cdot (66) \cdot (-9).$$

$$\therefore\ a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = -3703.$$

$$\therefore\ x \equiv -3703 + 4 \cdot 1122 = 785(\mod 1122).$$

Problem 4.5.4. *Obtain three consecutive integers, each having a square factor.*

Solution 4.5.4. *Note that* $a \equiv 0(\mod 2^2)$, $a+1 \equiv 0(\mod 3^2)$, $a+2 \equiv 0(\mod 5^2)$. *Since* $2^2, 3^2$ *and* 5^5 *are relatively prime to each other, therefore by virtue of Chinese Remainder Theorem we find*

$$\begin{aligned} a &\equiv 0(\mod 4) & N &= 4\cdot 9\cdot 25 = 900\\ a &\equiv -1(\mod 9) & N_1 &= 9\cdot 25 = 225\\ a &\equiv -2(\mod 25) & N_2 &= 4\cdot 25 = 100\\ & & N_3 &= 4\cdot 9 = 36. \end{aligned}$$

Now $225x_1 \equiv 1(\mod 4) \Rightarrow 225x_1 - 224x_1 = x_1 \equiv 1(\mod 4)$. *Again*

$$\begin{aligned} 100x_2 &\equiv 1(\mod 9) & 36x_3 &\equiv 1(\mod 25)\\ 100x_2 - 99x_2 &\equiv 1(\mod 9) & 72x_3 &\equiv 2(\mod 25)\\ x_2 &\equiv 1(\mod 9) & 72x_3 - 75x_3 &\equiv -3(\mod 25)\\ & & 3x_3 &\equiv -2(\mod 25)\\ & & 24x_3 &\equiv -16(\mod 25)\\ & & 24x_3 - 25x_3 = -x_3 &\equiv -16(\mod 25)\\ & & x_3 &\equiv 16(\mod 25). \end{aligned}$$

$$\therefore\ a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = -1252.$$

$$\therefore\ x \equiv 548(\mod 900).$$

Thus the desired three consecutive numbers are 548, 549, 550.

Problem 4.5.5. *Prove that the congruences* $x \equiv a(\mod n)$ *and* $x \equiv b(\mod m)$ *admit a simultaneous solution if and only if* $\gcd(n,m)\big|(a-b)$*; if a solution exists, confirm that it is unique modulo* $lcm(n,m)$.

Solution 4.5.5. *Suppose there exists a solution for* x. *Let* $d = \gcd(n,m)$. *This implies* $\exists\ r, s \in \mathbb{Z}$ *such that* $n = dr, m = ds$. *Now*

$$\begin{aligned} x \equiv a(\mod n) &\Rightarrow x = a + nt, t \in \mathbb{Z},\\ x \equiv b(\mod m) &\Rightarrow x = b + mk, k \in \mathbb{Z}. \end{aligned}$$

$$\therefore\ a + nt = b + mk \Rightarrow nt - mk = b - a.$$

Substituting for m, n *we obtain*

$$d(sk - rt) = a - b \Rightarrow d = \gcd(n,m)\big|(a-b).$$

Next, let us assume $d = \gcd(m, n)$ *and* $d|(a-b)$. *Then for some* $t \in \mathbb{Z}, dt = a-b \Rightarrow \exists\, x_0, y_0$ *such that* $nx_0 + my_0 = d$. *Therefore* $dt = nx_0t + my_0t = a-b \Rightarrow my_0t + b = a - x_0tn$. *Let* $x \equiv a(\mathrm{mod}\ n)$, $x \equiv b(\mathrm{mod}\ m)$. *So* $\exists$ *a simultaneous solutions. Let* y *be any other solution. Then*

$$\begin{aligned} x &\equiv a(\ \mathrm{mod}\ n) & y &\equiv a(\ \mathrm{mod}\ n).\\ x &\equiv b(\ \mathrm{mod}\ m) & y &\equiv b(\ \mathrm{mod}\ m).\\ \therefore\ x &\equiv y(\ \mathrm{mod}\ n).\\ x &\equiv y(\ \mathrm{mod}\ m). \end{aligned}$$

By virtue of worked out Problem 4.3.8, we obtain $x \equiv y(\mathrm{mod}\ lcm(m, n))$.

Problem 4.5.6. *A certain integer between* 1 *and* 1200 *leaves the remainders* $1, 2, 6$ *when divided by* $9, 11, 13$, *respectively. What is the integer?*

Solution 4.5.6. *From the given conditions, we have*

$$\begin{aligned} x &\equiv 1(\ \mathrm{mod}\ 9), & 1 < x < 1200.\\ x &\equiv 2(\ \mathrm{mod}\ 11),\\ x &\equiv 6(\ \mathrm{mod}\ 13). \end{aligned}$$

Since $9, 13, 11$ *are relatively prime, therefore Chinese Remainder Theorem is applicable here. Rest proceeding similarly as in Problem 4.5.4, we obtain the integer* 838.

Problem 4.5.7. *Obtain the two incongruent solutions modulo* 210 *of the system:*

$$\begin{aligned} 2x &\equiv 3(\ \mathrm{mod}\ 5)\\ 4x &\equiv 2(\ \mathrm{mod}\ 6)\\ 3x &\equiv 2(\ \mathrm{mod}\ 7). \end{aligned}$$

Solution 4.5.7. *Here*

$$2x \equiv 3(\ \mathrm{mod}\ 5) \tag{4.5.1}$$

$$4x \equiv 2(\ \mathrm{mod}\ 6) \tag{4.5.2}$$

$$3x \equiv 2(\ \mathrm{mod}\ 7). \tag{4.5.3}$$

$$\begin{aligned} \textit{From}(4.5.1),\ 4x &\equiv 6(\ \mathrm{mod}\ 5), & \textit{From}(4.5.2),\ 4\frac{x}{2} &\equiv \frac{2}{2}(\ \mathrm{mod}\ \frac{6}{2}),\\ 4x - 5x = x &\equiv 1(\ \mathrm{mod}\ 5), & 2x &\equiv 1(\ \mathrm{mod}\ 3),\\ x &\equiv -1 + 5(\ \mathrm{mod}\ 5), & 4x &\equiv 2(\ \mathrm{mod}\ 3),\\ x &\equiv 4(\ \mathrm{mod}\ 5). & 4x - 3x = x &\equiv 2(\ \mathrm{mod}\ 3),\\ & & x &\equiv 2(\ \mathrm{mod}\ 6). \end{aligned}$$

Since $\gcd(4,6) = 2$, *therefore from Theorem 4.4.2 we can say that there* $\exists$ 2 *incongruent solutions given by* $x_0, x_0 + \frac{6}{2}, x_0$ *being a solution. Here* $x_0 = 2$ *is a solution, so* 5 *is the other. Therefore* $x \equiv 5(\mathrm{mod}\ 6)$ *is the other congruence equation. From (4.5.3), we obtain*

$$\begin{aligned} 6x &\equiv 4(\ \mathrm{mod}\ 7),\\ 6x - 7x = -x &\equiv -3(\ \mathrm{mod}\ 7),\\ -x &\equiv -3(\ \mathrm{mod}\ 7),\\ \therefore\ x &\equiv 3(\ \mathrm{mod}\ 7). \end{aligned}$$

Therefore $x \equiv 4(\mathrm{mod}\ 5),\ x \equiv 2(\mathrm{mod}\ 6)$ *or* $x \equiv 5(\mathrm{mod}\ 6),\ x \equiv 3(\mathrm{mod}\ 7)$. *Note that* $N = 5 \cdot 6 \cdot 7 = 210$. *Therefore* $N_1 = 6 \cdot 7 = 42,\ N_2 = 5 \cdot 7 = 35$ *and* $N_3 = 5 \cdot 6 = 30$. *Thus*

$$\begin{aligned} 42x_1 &\equiv 1(\ \mathrm{mod}\ 5)\\ 42x_1 - 40x_1 = 2x_1 &\equiv 1(\ \mathrm{mod}\ 5).\\ 6x_1 &\equiv 3(\ \mathrm{mod}\ 5)\\ 6x_1 - 5x_1 = x_1 &\equiv 3(\ \mathrm{mod}\ 5)\\ x_1 &\equiv 3(\ \mathrm{mod}\ 5). \end{aligned} \qquad \begin{aligned} 35x_2 &\equiv 1(\ \mathrm{mod}\ 6)\\ 35x_2 - 36x_2 = -x_2 &\equiv 1(\ \mathrm{mod}\ 6)\\ x_2 &\equiv 5(\ \mathrm{mod}\ 6). \end{aligned}$$

$$\begin{aligned} 30x_3 &\equiv 1(\ \mathrm{mod}\ 7)\\ 30x_3 - 28x_3 = 2x_3 &\equiv 1(\ \mathrm{mod}\ 7)\\ 8x_3 &\equiv 4(\ \mathrm{mod}\ 7)\\ 8x_3 - 7x_3 = x_3 &\equiv 4(\ \mathrm{mod}\ 7). \end{aligned}$$

Therefore $a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = 1214$ *or* 1739*(Verify!). Thus the solutions are* $x \equiv 164(\mathrm{mod}\ 210)$ *or* $x \equiv 59(\mathrm{mod}\ 210)$.

Problem 4.5.8. *Obtain the eight incongruent solutions of the linear congruence* $3x + 4y \equiv 5(\mathrm{mod}\ 8)$.

Solution 4.5.8. *Set* $3x \equiv 5 - 4y(\mathrm{mod}\ 8)$. *Since* $\gcd(3,8) = 1$ *and* $1|(5 - 4y)$, *there exists one solution for any value of* y. *Because there are eight incongruent values of* $5 - 4y(y = 0,1,2,3,4,5,6,7)$, *let us solve this for each values of* y. *First, let us take* $y \equiv 0(\mathrm{mod}\ 7)$. *Then*

$$\begin{aligned} 3x &\equiv 5(\ \mathrm{mod}\ 8)\\ 15x &\equiv 25(\ \mathrm{mod}\ 8)\\ 16x - 15x = x &\equiv -1 \equiv 7(\ \mathrm{mod}\ 8). \end{aligned}$$

By similar reasoning, $x \equiv 3(\text{mod } 8)$ *for* $y \equiv 1(\text{mod } 8)$, $x \equiv 7(\text{mod } 8)$ *for* $y \equiv 2(\text{mod } 8)$, $x \equiv 3(\text{mod } 8)$ *for* $y \equiv 3(\text{mod } 8)$, $x \equiv 7(\text{mod } 8)$ *for* $y \equiv 4(\text{mod } 8)$, $x \equiv 3(\text{mod } 8)$ *for* $y \equiv 5(\text{mod } 8)$, $x \equiv 7(\text{mod } 8)$ *for* $y \equiv 6(\text{mod } 8)$ *and* $x \equiv 3(\text{mod } 8)$ *for* $y \equiv 7(\text{mod } 8)$.

Problem 4.5.9. *The basket-of-eggs problem is often phrased in the following form: One egg remains when the eggs are removed from the basket* $2, 3, 4, 5,$ *or* 6 *at a time; but, no eggs remain if they are removed* 7 *at a time. Find the smallest number of eggs that could have been in the basket.*

Solution 4.5.9. *From the given conditions, we have*

$$x \equiv 1(\text{ mod } 2) \tag{4.5.4}$$

$$x \equiv 1(\text{ mod } 3) \tag{4.5.5}$$

$$x \equiv 1(\text{ mod } 4) \tag{4.5.6}$$

$$x \equiv 1(\text{ mod } 5) \tag{4.5.7}$$

$$x \equiv 1(\text{ mod } 6) \tag{4.5.8}$$

$$x \equiv 0(\text{ mod } 7). \tag{4.5.9}$$

If (4.5.6) is true, then $x = 1 + 4n = 1 + 2(2n)$. *Since* $\gcd(2, 4) \neq 1$, *therefore we can eliminate (4.5.4). Moreover, if (4.5.8) is true, then* $x = 1 + 6n = 1 + 3(2n)$. *Because* $\gcd(3, 6) \neq 1$, *whence we can eliminate (4.5.5). Multiplying (4.5.6) by* 3 *and (4.5.8) by* 2, *we obtain*

$$3x \equiv 3(\text{ mod } 3 \cdot 4) = 3(\text{ mod } 12) \tag{4.5.10}$$

$$2x \equiv 2(\text{ mod } 2 \cdot 6) = 2(\text{ mod } 12). \tag{4.5.11}$$

$$\therefore\ 3x - 3 \equiv 2x - 2(\text{ mod } 12),$$

$$x \equiv 1(\text{ mod } 12). \tag{4.5.12}$$

If (4.5.12) holds true, then (4.5.6) and (4.5.8) is also so. Now we have $x \equiv 1(\text{mod } 5)$, $x \equiv 0(\text{mod } 7)$ *and* $x \equiv 1(\text{mod } 12)$. *Note that* $5, 7, 12$ *are relatively prime. Thus* $N = 5 \cdot 7 \cdot 12 = 420$. *Therefore* $N_1 = 7 \cdot 12 = 84$, $N_2 = 5 \cdot 12 = 60$ *and* $N_3 = 5 \cdot 7 = 35$. *Hence*

$$84x_1 \equiv 1(\text{ mod } 5) \qquad 35x_3 \equiv 1(\text{ mod } 12)$$

$$84x_1 - 85x_1 = -1x_1 \equiv 1(\text{ mod } 5) \qquad 35x_3 - 36x_3 = -x_3 \equiv 1(\text{ mod } 12)$$

$$x_1 \equiv -1(\text{ mod } 5). \qquad x_3 \equiv 5 - 1(\text{ mod } 12).$$

Since $a_2 = 0$, *therefore* $60x_2 \equiv 1(\text{mod } 7)$. *Thus* $a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = -119$*(Verify!). Hence* $-119 + 420 = 301$ *eggs in basket.*

4.6 System of Linear Congruences

In this section, our discussion will be restricted to solve the system of linear congruence equations involving the same numbers of unknowns with the same modulus.

Let us begin with an example. Consider the system of linear congruence equations:

$$x + 2y \equiv 1 (\text{mod } 5) \tag{4.6.1}$$

$$2x + y \equiv 1 (\text{mod } 5). \tag{4.6.2}$$

Now (4.6.1) $\times$ 2 $-$ (4.6.2) yields

$$3y \equiv 1 (\text{mod } 5).$$

Note that 2 is the inverse of 3 modulo 5. So multiplying both sides of the foregoing equation by 2 we get,

$$y \equiv 2 (\text{mod } 5).$$

Similarly, (4.6.2) $\times$ 2 $-$ (4.6.1) we get,

$$3x \equiv 1 (\text{mod } 5).$$

Since 2 is the inverse of 3 modulo 5, therefore proceeding as above we get

$$x \equiv 2 (\text{mod } 5).$$

Thus the solutions of the system of linear congruences are in pairs satisfying $x \equiv 2 (\text{mod } 5)$ and $y \equiv 2 (\text{mod } 5)$.

This example motivates us to devise a general method for solving the system of linear congruences.

Theorem 4.6.1. *Let p, q, r, s, u, v and m be integers with $m > 0$, such that $\gcd(D, m) = 1$ where $D = ps - qr$. Then the system of congruences*

$$px + qy \equiv u (\text{mod } m) \tag{4.6.3}$$

$$rx + sy \equiv v (\text{mod } m) \tag{4.6.4}$$

has a unique solution modulo m given by,

$$x \equiv \bar{D}(us - qv) (\text{mod } m)$$

$$y \equiv \bar{D}(pv - ur) (\text{mod } m)$$

where $\bar{D}$ is the inverse of D modulo m.

Proof. Let us begin with a calculation. Here (4.6.3) $\times s -$ (4.6.4) $\times q$ yields

$$Dx \equiv (us - qv)(\text{mod } m).$$

Since $\bar{D}$ is the inverse of D modulo m, therefore multiplying both sides by $\bar{D}$ we get

$$x \equiv \bar{D}(us - qv)(\text{mod } m).$$

Similarly, applying $\bar{D}$ on (4.6.3) $\times r -$ (4.6.4) $\times s$ gives

$$y \equiv \bar{D}(pv - ur)(\text{mod } m).$$

Our claim is that any pair (x, y) is a solution. For this we have,

$$\begin{aligned} px + qy &\equiv \bar{D}\{p(us - qv) + q(pv - ur)\}(\text{mod } m) \\ &\equiv \bar{D}u(ps - qr)(\text{mod } m) \\ &\equiv \bar{D}Du(\text{mod } m) \\ &\equiv u(\ \text{mod } m) \\ \text{and } rx + sy &\equiv \bar{D}\{r(us - qv) + s(pv - ur)\}(\text{mod } m) \\ &\equiv \bar{D}v(ps - qr)(\text{mod } m) \\ &\equiv \bar{D}Dv(\text{mod } m) \\ &\equiv v(\text{mod } m). \end{aligned}$$

This proves the theorem. □

In the Theorem 4.6.1 we have discussed the solution for a system of two linear congruences with two unknowns. But the method fails for n linear congruences with n unknowns where $n > 2$. To overcome this, we require the algebra of matrices. The following definition on congruence relation between matrices will pave the way for our future discussions.

Definition 4.6.1. *For any two matrices $S = (s_{ij})_{n\times k}$ and $T = (t_{ij})_{n\times k}$, S is said to be congruent to T modulo $m(> 0)$ if $s_{ij} \equiv t_{ij}(\text{mod } m)$ for every i and j with $1 \leq i \leq n$, $1 \leq j \leq k$. This is denoted as $S \equiv T(\text{mod } m)$.*

Example 4.6.1. *Consider* $S = \begin{pmatrix} 8 & 4 \\ 9 & 7 \end{pmatrix}$ *and* $T = \begin{pmatrix} 13 & 4 \\ 14 & 12 \end{pmatrix}$. *Then* $S \equiv T($ mod 5).

Proposition 4.6.1. *For any two matrices $[S]_{n\times k}$ and $[T]_{n\times k}$ with $S \equiv T(\text{mod } m)$, $\exists$ matrices $[U]_{k\times p}$ and $[V]_{p\times n}$ respectively, with all integer entries, such that $SU \equiv TU(\text{mod } m)$ and $VS \equiv VT(\text{mod } m)$.*

Proof. Let $S = (s_{ij})_{n\times k}$, $T = (t_{ij})_{n\times k}$ and $U = (u_{ij})_{k\times p}$ be the matrices with integral entries. Now the entries of SU and TU are $\sum_{r=1}^{n} s_{ir}u_{rj}$ and $\sum_{r=1}^{n} t_{ir}u_{rj}$ respectively. Since $S \equiv T(\text{mod } m)$, therefore we have $s_{ir} \equiv t_{ir}(\text{mod } m)$ for all i and r. In view of Theorem 4.2.1 we get,

$$\sum_{r=1}^{n} s_{ir}u_{rj} \equiv \sum_{r=1}^{n} t_{ir}u_{rj}(\text{mod } m).$$

This proves $SU \equiv TU(\text{mod } m)$. Similarly we can show that $VS \equiv VT(\text{mod } m)$. □

We continue our development of the method for solving system of congruences,

$$\begin{aligned} s_{11}x_1 + s_{12}x_2 + \ldots s_{1n}x_n &\equiv t_1(\text{mod } m)\\ s_{21}x_1 + s_{22}x_2 + \ldots s_{2n}x_n &\equiv t_2(\text{mod } m)\\ &\vdots\\ s_{n1}x_1 + s_{n2}x_2 + \ldots s_{nn}x_n &\equiv t_n(\text{mod } m). \end{aligned}$$

The system can be written as $SX \equiv T(\text{mod } m)$, where

$$S = \begin{pmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n}\\ s_{2,1} & s_{2,2} & \cdots & s_{2,n}\\ \vdots & \vdots & \ddots & \vdots\\ s_{m,1} & s_{m,2} & \cdots & s_{m,n} \end{pmatrix} X = \begin{pmatrix} x_1\\ x_2\\ \vdots\\ x_n \end{pmatrix} \text{ and } T = \begin{pmatrix} t_1\\ t_2\\ \vdots\\ t_n \end{pmatrix}.$$

This method is based on finding the inverse $\bar{S}$ of S modulo m. Here $\bar{S}$ is defined as $\bar{S}S \equiv S\bar{S} \equiv I(\text{mod } m)$, where $I_{n\times n}$ is the identity matrix.

To illustrate this, let us choose $S = \begin{pmatrix} 1 & 2\\ 3 & 4 \end{pmatrix}$. Then $\bar{S} = \begin{pmatrix} 3 & 1\\ 4 & 2 \end{pmatrix}$ where $S\bar{S} = \begin{pmatrix} 11 & 5\\ 25 & 11 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0\\ 0 & 1 \end{pmatrix}$ (mod 5) and $\bar{S}S = \begin{pmatrix} 6 & 10\\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0\\ 0 & 1 \end{pmatrix}$ (mod 5). Next proposition describes a method for finding inverses of 2×2 matrices.

Proposition 4.6.2. *Let $S = \begin{pmatrix} a & b\\ c & d \end{pmatrix}$ be a matrix with integer entries and m be a positive integer such that $D = \det S = ad - bc$ with $\gcd(D, m) = 1$. Then the matrix $\bar{S} = \bar{D}\begin{pmatrix} d & -b\\ -c & a \end{pmatrix}$ is the inverse of S modulo m, where $\bar{D}$ is the inverse of D modulo m.*

Proof. Whether $\bar{S}$ is the inverse of S, it suffices to examine $S\bar{S} \equiv \bar{S}S \equiv I(\mod m)$. For this, let us consider

$$S\bar{S} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bar{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \equiv \bar{D} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \equiv \bar{D}D \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv I(\mod m)$$

$$\bar{S}S \equiv \bar{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \bar{D} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \equiv \bar{D}D \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv I(\mod m).$$

Since $\bar{D}$ is inverse of D modulo m, therefore $\bar{D}D \equiv 1 (\mod m)$ holds in both the cases. Thus $\bar{S}$ is the inverse of S modulo m. □

Finally we are going to conclude with a need to find the solution for the system of congruences $SX \equiv T(\mod m)$ where S is a $n \times n$ matrix. For that we need to find $\bar{S}$, the inverse of S modulo m. In our last proposition, we have found the inverse $\bar{S}$ for 2×2 matrices. But for $n \times n$ matrices where $n > 2$, we need to find $\bar{S}$ with the notion of the adjoint of a matrix S denoted by *adj* S. Our first task is to find $\bar{S}$ for an $n \times n$ matrix. The following proposition serves this purpose.

Proposition 4.6.3. *Let S be an $n \times n$ matrix with integer entries and m be a positive integer with $\gcd(D, m) = 1$. Then the matrix $\bar{S} = \bar{D}(adj\ S)$ is the inverse of S modulo m where $D = \det S$ and $\bar{D}$ is the inverse of D modulo m.*

Proof. Note that $\gcd(D, m) = 1$ implies $\det S \neq 0$. Now from the property of adjoint of a square matrix, we have

$$S(adj\ S) = (\det S)I = DI.$$

Also $\gcd(D, m) = 1$ implies that $\exists$ an inverse $\bar{D}$ of D modulo m. This follows that,

$$S(\bar{D}(\text{adj}S)) \equiv S(\text{adj}S)\bar{D} \equiv D\bar{D} \equiv I(\mod m) \text{ and}$$
$$\bar{D}(\text{adj}S)S \equiv \bar{D}D \equiv I(\mod m).$$

Combining we get $\bar{S} = \bar{D}(\text{adj } S)$ is an inverse of S modulo m. □

This leads us to solve the system $SX \equiv T(\mod m)$. Here if we multiply both sides of the congruence by $\bar{S}$ we obtain,

$$\bar{S}(SX) \equiv \bar{S}T(\mod m)$$
$$(\bar{S}S)X \equiv \bar{S}T(\mod m)$$
$$X \equiv \bar{S}T(\mod m).$$

The following example illustrates the fact lucidly.

Example 4.6.2. *Let us consider the system,*

$$x + 2y + 3z \equiv 1(\text{mod } 7)$$
$$x + 3y + 5z \equiv 1(\text{mod } 7)$$
$$x + 4y + 6z \equiv 1(\text{mod } 7).$$

This can be written as $SX \equiv T(\text{mod } m)$ *where*

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 5 \\ 1 & 4 & 6 \end{pmatrix},\ X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Here $D = \det S = -1$. *Then* $\bar{D} = 6$. *Also adj* $S = \begin{pmatrix} -2 & 0 & 1 \\ -1 & 3 & -2 \\ 1 & -2 & 1 \end{pmatrix}$. *Thus we have*

$$\bar{S} = 6\begin{pmatrix} -2 & 0 & 1 \\ -1 & 3 & -2 \\ 1 & -2 & 1 \end{pmatrix} = \begin{pmatrix} -12 & 0 & 6 \\ -6 & 18 & -12 \\ 6 & -12 & 6 \end{pmatrix}$$
$$X \equiv \begin{pmatrix} -12 & 0 & 6 \\ -6 & 18 & -12 \\ 6 & -12 & 6 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}(\text{mod } 7) \equiv \begin{pmatrix} -6 \\ 0 \\ 0 \end{pmatrix}(\text{mod } 7).$$

$\therefore$ *The solution is* $x \equiv 1(\text{mod } 7),\ y \equiv 0(\text{mod } 7),\ z \equiv 0(\text{mod } 7)$.

4.7 Worked out Exercises

Problem 4.7.1. *Find the solution of the system of linear congruences*

$$2x + 3y \equiv 5(\text{mod } 7)$$
$$x + 5y \equiv 6(\text{mod } 7).$$

Solution 4.7.1. *Multiplying second equation by* 2 *and then subtracting with first one we get*

$$-7y \equiv -7(\text{ mod } 7).$$

This shows that y *can take any residue modulo* 7. *If* $y = 0$, *then* $x \equiv 6(\text{mod } 7)$. *So the first solution is* $(6, 0)$. *Continuing this manner we can find other solutions too.*

Problem 4.7.2. *Find the inverse modulo* 5 *for the matrix*

$$S = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$$

Solution 4.7.2. *Here* $D = 4 - 2 = 2$. *Then* $\bar{D}D \equiv 1 (\mathrm{mod}\ 5) \Rightarrow \bar{D} = 3$. *Let* $\bar{S}$ *be the inverse of* S. *Then*

$$\bar{S} = 3 \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & -6 \\ -3 & 6 \end{pmatrix}. \ \therefore \ \bar{S} \equiv \begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix} (\mathrm{mod}\ 5).$$

Problem 4.7.3. *Find the inverse modulo* 5 *for the matrix*

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{pmatrix}$$

Solution 4.7.3. *Here* $D = 1(12-20) - 2(6-5) + 3(4-2) = -4$. *Then* $\bar{D}D \equiv 1 (\mathrm{mod}\ 7) \Rightarrow \bar{D} = 5$. *Now*

$$adj\ S = \begin{pmatrix} -1 & 0 & 4 \\ -1 & 3 & -2 \\ 2 & -2 & 0 \end{pmatrix} \ shows\ \bar{S} = 5 \begin{pmatrix} -1 & 0 & 4 \\ -1 & 3 & -2 \\ 2 & -2 & 0 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{pmatrix} (\mathrm{mod}\ 7).$$

4.8 Exercises:

1. Find the remainders when 2^{50} and 41^{65} are divided by 7.

2. Establish the following divisibility statements by theory of congruence for integers $n(\geq 1)$:
   (a) $7 \big| 5^{2n} + 3 \cdot 2^{5n-2}$;
   (b) $17 \big| 2^{3n+1} + 3 \cdot 5^{2n+1}$;
   (c) $43 \big| 6^{n+2} + 7^{2n+1}$.

3. For $n(\geq 1)$, show that $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} (\mathrm{mod}\ 181)$.

4. Find the remainder when 2^{340} is divided by 341.

5. Prove the assertions below:
   (a)If a is an odd integer, then $a^2 \equiv 1 (\mathrm{mod}\ 8)$.
   (b)For any integer a, $a^4 \equiv 0$ or $1 (\mathrm{mod}\ 5)$.

6. Prove the following statements:
   (a) The product of any set of n consecutive integers is divisible by n. (b) Any n consecutive integers form a complete set of residues modulo n.

7. Using theory of congruence show that $89 \mid 2^{44} - 1$ and $97 \mid 2^{48} - 1$.

8. Solve the following linear congruences:
   (a) $5x \equiv 2 (\mod 26)$;
   (b) $34x \equiv 60 (\mod 98)$.

9. Using congruences, solve the Diophantine equations below:
   (a) $4x + 51y = 9$;
   (b) $5x - 53y = 17$.

10. Solve each of the following sets of simultaneous congruences:
    (a) $x \equiv 5 (\mod 11), x \equiv 14 (\mod 29), x \equiv 15 (\mod 31)$;
    (b) $2x \equiv 1 (\mod 5), 3x \equiv 9 (\mod 6), 4x \equiv 1 (\mod 7), 5x \equiv 9 (\mod 11)$.

11. Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

12. Check that whether the system $x \equiv 5 (\mod 6)$ and $x \equiv 7 (\mod 15)$ has a solution or not.

13. Solve the system of congruences,
    $3x + 4y \equiv 5 (\mod 13)$
    $2x + 5y \equiv 7 (\mod 13)$.

14. Find an integer having the remainders $2, 3, 4, 5$ when divided by $3, 4, 5, 6$ respectively.

15. Verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ form a complete set of residues modulo 11, but
    $0, 1, 2^2, 3^2, \ldots, 10^2$ does not.

16. Find the solution of the following system of linear congruences,

$$4x + y \equiv 5 (\mod 7)$$
$$x + 2y \equiv 4 (\mod 7)$$

17. Find the solution of the following system of linear congruences,

$$x + 3y \equiv 1 (\mod 5)$$
$$3x + 4y \equiv 2 (\mod 5).$$

18. Find the inverse modulo 5 for the matrix,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

19. Find the inverse modulo 7 for the matrix,

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

20. Find all solutions of the following system,

$$\begin{aligned} x + y &\equiv 1(\mod 7) \\ x + z &\equiv 1(\mod 7) \\ y + z &\equiv 1(\mod 7). \end{aligned}$$