1 Congruences

If $m$ is a given positive integer, then we can define an equivalence relation on $\mathbb{Z}$ (the set of all integers) by requiring that an integer $a$ is related to an integer $b$ if and only if $b - a$ is a multiple of $m$. This equivalence relation on $\mathbb{Z}$ gives rise to the partition of $\mathbb{Z}$, $C = \{[0]_m, [1]_m, \ldots, [m - 1]_m\}$, that consists of exactly $m$ subsets of $\mathbb{Z}$. (This was discussed in the course notes that accompany Chapter 1, Section 1.) The number $m$ is called the modulus of this equivalence relation.

Example 1 Let $m = 6$ and define an equivalence relation on $\mathbb{Z}$ by requiring that an integer $a$ is related to an integer $b$ if and only if $b - a$ is divisible by 6. (Thus, for example, 27 is related to 45 because $45 - 27 = 18$ is divisible by 6, but 15 is not related to 30 because $30 - 15 = 15$ is not divisible by 6.)

The partition of $\mathbb{Z}$ induced by this equivalence relation is $C = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ where

$[0]_6 = \{0, 6, 12, 18, \ldots\} \cup \{-6, -12, -18, -24, \ldots\}$

$[1]_6 = \{1, 7, 13, 19, \ldots\} \cup \{-5, -11, -17, -23, \ldots\}$

$[2]_6 = \{2, 8, 14, 20, \ldots\} \cup \{-4, -10, -16, -22, \ldots\}$

$[3]_6 = \{3, 9, 15, 21, \ldots\} \cup \{-3, -9, -15, -21, \ldots\}$

$[4]_6 = \{4, 10, 16, 22, \ldots\} \cup \{-2, -8, -14, -20, \ldots\}$

$[5]_6 = \{5, 11, 17, 23, \ldots\} \cup \{-1, -7, -13, -19, \ldots\}$. 

In the above example, notice that

\[ 0 \] \_6 \text{ is the set of all integers that have remainder } 0 \text{ when divided by } 6 \\
\[ 1 \] \_6 \text{ is the set of all integers that have remainder } 1 \text{ when divided by } 6 \\
\[ 2 \] \_6 \text{ is the set of all integers that have remainder } 2 \text{ when divided by } 6 \\
\[ 3 \] \_6 \text{ is the set of all integers that have remainder } 3 \text{ when divided by } 6 \\
\[ 4 \] \_6 \text{ is the set of all integers that have remainder } 4 \text{ when divided by } 6 \\
\[ 5 \] \_6 \text{ is the set of all integers that have remainder } 5 \text{ when divided by } 6.

In general, if \( m \) is some given positive integer, and \( r \) is an integer such that \( 0 \leq r < m \), then \([r]_m\) is the set of all integers that have remainder \( r \) when divided by \( m \). That is

\[ [r]_m = \{mq + r \mid q \in \mathbb{Z} \}. \]

For example, \([2]_6 = \{6q + 2 \mid q \in \mathbb{Z} \}\).

We will now define two new terms that will facilitate our study of the type of equivalence relation being discussed here.

\textbf{Definition 2} If \( m \) is a positive integer and \( a \) and \( b \) are integers such that \( b - a \) is divisible by \( m \), then we say that \( a \) is \textbf{congruent to} \( b \) \textbf{modulo} \( m \) and we write \( a \equiv b \mod m \).

\textbf{Definition 3} If \( m \) is a positive integer and \( a \) is an integer, then the \textbf{residue of} \( a \) \textbf{modulo} \( m \) is defined to be the remainder obtained (in the Division Algorithm) upon division of \( a \) by \( m \). The residue of \( a \) modulo \( m \) is denoted by \( a \mod m \).

\textbf{Remark 4} Note that it must always be the case that \( 0 \leq a \mod m < m \). Also note that we can always write \( a = qm + a \mod m \) for some unique integer \( q \).

\textbf{Example 5} To illustrate the above definitions, let us observe that

\[ -14 \equiv 4 \mod 6 \]

because \( 4 - (-14) = 18 \) is divisible by 6, and let us also observe that

\[ -14 \mod 6 = 4 \]
because the Division Algorithm gives us \(-14 = -3 \cdot 6 + 4\), and
\[
4 \mod 6 = 4
\]
because the Division Algorithm gives us \(4 = 0 \cdot 6 + 4\). Thus
\[
-14 \mod 6 = 4 \mod 6.
\]
Note that it is also true that
\[
[-14]_6 = [4]_6
\]
because both of these sets are equal to
\[
\{6q + 4 \mid q \in \mathbb{Z}\} = \{4, 10, 16, 22, \ldots\} \cup \{-2, -8, -14, -20, \ldots\}.
\]
As can be seen by studying the above example, the three statements
\begin{enumerate}
  \item \(-14 \equiv 4 \mod 6\)
  \item \(-14 \mod 6 = 4 \mod 6\)
  \item \([-14]_6 = [4]_6\)
\end{enumerate}
are really just three different ways of saying the same thing. The following Proposition states the equivalence of these three different way of looking at the concept of congruence.

**Proposition 6** Let \(m\) be a positive integer and let \(a\) and \(b\) be integers. Then the following three statements are equivalent. (This means that either all three statements are true or all three statements are false.)
\begin{enumerate}
  \item \(a \equiv b \mod m\)
  \item \(a \mod m = b \mod m\)
  \item \([a]_m = [b]_m\).
\end{enumerate}
Proof. First, suppose that statement 1 is true; that is suppose that \( a \equiv b \mod m \). Then \( b - a \) is divisible by \( m \). This means that there exists an integer \( t \) such that \( b - a = mt \). Also, by the Division Algorithm, there exist unique integers \( q_1 \) and \( q_2 \) such that \( a = q_1 m + a \mod m \) and \( b = q_2 m + b \mod m \). Thus

\[
b - a = (q_2 - q_1) m + \left( b \mod m - a \mod m \right)
\]

from which we obtain

\[
mt = (q_2 - q_1) m + \left( b \mod m - a \mod m \right)
\]

or, upon rearrangement of the above equation,

\[
b \mod m - a \mod m = (t - q_2 + q_1) m.
\]

This shows that \( b \mod m - a \mod m \) is divisible by \( m \) and hence that

\[
|b \mod m - a \mod m|
\]

is divisible by \( m \). However, we know that \( 0 \leq a \mod m < m \) and \( 0 \leq b \mod m < m \) and this implies that \( 0 \leq |b \mod m - a \mod m| < m \). The only possibility is that \( |b \mod m - a \mod m| = 0 \) and this means that \( b \mod m - a \mod m = 0 \) and that \( a \mod m = b \mod m \). We have now proved that if statement 1 is true, then statement 2 must also be true.

Now suppose that statement 2 is true; that is suppose that \( a \mod m = b \mod m \). Since \( a = q_1 m + a \mod m \) and \( b = q_2 m + b \mod m \) for some integers \( q_1 \) and \( q_2 \), we see that

\[
b - a = (q_2 - q_1) m + \left( b \mod m - a \mod m \right) = (q_2 - q_1) m
\]

and hence \( b - a \) is divisible by \( m \) and \( a \equiv b \mod m \). This proves that if statement 2 is true, then statement 1 must also be true. We have now proved that statements 1 and 2 are equivalent (meaning that either both statements must be true or both must be false). We will complete our proof of this Proposition by showing that statements 1 and 3 are also equivalent.

Suppose that statement 1 is true; that is, suppose that \( a \equiv b \mod m \). Then \( b - a \) is divisible by \( m \). This means that there exists an integer \( t \) such that \( b - a = mt \). We would like to prove that \( [a]_m = [b]_m \). Since this is an equation between sets, we must show that every member of the set \( [a]_m \) is also a member of the set \( [b]_m \) and that every member of the set \( [b]_m \) is also
a member of the set $[a]_m$. To this end, let $x \in [a]_m$. Then there exists an integer $q$ such that $x = qm + a$. However, since $a = b - tm$, we see that

$$x = qm + (b - tm) = (q - t)m + b.$$  

Since $q - t$ is an integer, we conclude that $x \in [b]_m$ and we have now proved that $[a]_m \subseteq [b]_m$. The proof that $[b]_m \subseteq [a]_m$ is similar and is left as homework. Since $[a]_m \subseteq [b]_m$ and $[b]_m \subseteq [a]_m$, then $[a]_m = [b]_m$ and we have now proved that if statement 1 is true, then statement 3 must also be true.

Finally, suppose that statement 3 is true. Then $[a]_m = [b]_m$ and this means that the sets $\{qm + a \mid q \in \mathbb{Z}\}$ and $\{qm + b \mid q \in \mathbb{Z}\}$ are equal. By the Division Algorithm, we know that there exist integers $Q$ and $r$ such that $b - a = Qm + r$. Since $b - r = Qm + a$, we see that $b - r$ is a member of the set $[a]_m$, which means that $b - r$ is also a member of the set $[b]_m$. Hence there exists an integer $q$ such that $b - r = qm + b$, from which we conclude that $r = -qm$. This allows us to conclude that

$$b - a = Qm + r = (Q - q)m,$$

and hence that $b - a$ is divisible by $m$, and hence that $a \equiv b \mod m$. Thus we have shown that the truth of statement 3 implies the truth of statement 1, and the proof of the Proposition is now complete. ■

**Example 7** If we divide 281 by 3, then the remainder is 2. Also, if we divide 554 by 3, then the remainder is 2. State this fact in three different ways.

**Answer:** We could say that

$$281 \equiv 554 \mod 3$$

or we could say that

$$281 \mod 3 = 554 \mod 3$$

or we could say that

$$[281]_3 = [554]_3.$$  

2 The Algebra of Congruences

The following Proposition states some of the basic algebraic properties of congruences.
Proposition 8 Suppose that $m$ is a positive integer. Also suppose that $a$, $b$, $c$, and $d$ are integers. Then:

1. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $(a + c) \equiv (b + d) \mod m$.
2. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.
3. If $a \equiv b \mod m$ and if $n \geq 0$ is an integer, then $a^n \equiv b^n \mod m$.

Proof.

1. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $b - a$ and $d - c$ are both divisible by $m$. Thus

$$(b + d) - (a + c) = (b - a) + (d - c)$$

is also divisible by $m$ and hence $(a + c) \equiv (b + d) \mod m$.

2. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then there exist integers $s$ and $t$ such that $b = a + sm$ and $d = c + tm$. Thus

$$bd = (a + sm)(c + tm)$$
$$= ac + atm + csm + stmm$$
$$= ac + (at + cs + stm)m$$

and since $at + cs + stm$ is an integer, we see that $bd - ac$ is divisible by $m$ and hence that $ac \equiv bd \mod m$.

3. Let $a$ and $b$ be integers and suppose that $a \equiv b \mod m$.

If $n = 0$, then $a^n = a^0 = 1$ and $b^n = b^0 = 1$ and it is clear that $a^n \equiv b^n \mod m$.

If $n = 1$, then $a^n = a^1 = a$ and $b^n = b^1 = b$ and, once again, it is clear that $a^n \equiv b^n \mod m$.

If $n = 2$, then $a^n = a^2$ and $b^n = b^2$. Using part 4 of this Proposition, we know that since $a \equiv b \mod m$, then $a \cdot a \equiv b \cdot b \mod m$. In other words $a^2 \equiv b^2 \mod m$. Thus $a^n \equiv b^n \mod m$ when $n = 2$. The rest of this proof follows easily by induction: Supposing that $a^n \equiv b^n \mod m$, it follows, since $a \equiv b \mod m$ and by Part 4 of this Proposition, that $a^n \cdot a \equiv b^n \cdot b \mod m$ and hence $a^{n+1} \equiv b^{n+1} \mod m$. 

6
The following two examples illustrate the surprising computational power that can be achieved in working with congruences. We can use congruences to answer certain questions concerning very large numbers that are too large to be handled by a calculator.

**Example 9** Let us compute $63^{57} \mod 5$. (In other words, we are going to compute the remainder obtained when $63^{57}$ is divided by 5.)

Since

\[
63 \mod 5 = 3 = 3 \mod 5 \\
63^2 \mod 5 = 3^2 \mod 5 = 9 \mod 5 = 4 = 4 \mod 5 \\
63^3 \mod 5 = (63 \cdot 4) \mod 5 = 252 \mod 5 = 2 = 2 \mod 5 \\
63^4 \mod 5 = (63 \cdot 2) \mod 5 = 126 \mod 5 = 1 = 1 \mod 5
\]

we see that

\[
63^{56} \mod 5 = 63^{14} \mod 5 = (63^4)^{14} \mod 5 = 1^{14} \mod 5 = 1 \mod 5
\]

and hence that

\[
63^{57} \mod 5 = (63 \cdot 63^{56}) \mod 5 = (63 \cdot 1) \mod 5 = 63 \mod 5 = 3.
\]

Note that, in retrospect, we did not need to use our computation of $63^3 \mod 5$. We could have gone directly from the computation of $63^2 \mod 5 = 4 \mod 5$ to

\[
63^4 \mod 5 = (63^2)^2 \mod 5 = 4^2 \mod 5 = 16 \mod 5 = 1.
\]

**Example 10** Let us compute $(2^{50} + 3) \mod 6$.

First note that

\[
(2^{50} + 3) \mod 6 = (2^{50} \mod 6 + 3 \mod 6) \mod 6
\]

Since

\[
2^5 \mod 6 = 32 \mod 6 = 2 = 2 \mod 6,
\]

we see that

\[
2^{25} \mod 6 = (2^5)^5 \mod 6 = 2^5 \mod 6 = 2 \mod 6
\]

and hence that

\[
2^{50} \mod 6 = (2^{25})^2 \mod 6 = 2^2 \mod 6 = 4 \mod 6 = 4.
\]

Thus

\[
(2^{50} + 3) \mod 6 = (2^{50} \mod 6 + 3 \mod 6) \mod 6 = (4 + 3) \mod 6 = 7 \mod 6 = 1.
\]
3 Solving Congruence Equations

Suppose that \(a\) and \(b\) are integers and that \(m\) is a positive integer. We would like to solve the equation

\[
ax \equiv b \mod m. \quad (1)
\]

This means that we would like to find all integers \(x\) that satisfy equation (1).

The first thing that we notice is that if an integer \(x\) satisfies equation (1), then there exists an integer \(y\) such that \(ax = b - my\). This means that the pair \((x, y)\) is a solution of the Diophantine equation

\[
ax + my = b. \quad (2)
\]

Conversely, if some pair \((x, y)\) is a solution of the Diophantine equation (2), then \(x\) is a solution of the congruence equation (1). Hence to solve (1), we really just need to solve (2). The set of \(x\) coordinates of solutions of (2) is the solution set of (1). As we will see, this solution set must either be the empty set or must be a congruence class modulo \(m/\gcd(a, m)\). We will also see that, in the latter case, the solution set can always be written as a union of congruence classes modulo \(m\).

First, recall that equation (2) has solutions if and only if \(\gcd(a, m)\) divides \(b\). Assuming that \(\gcd(a, m)\) divides \(b\) and assuming that \((x_0, y_0)\) is a solution of equation (2), then all solutions of (2) are given by

\[
(x, y) = \left(x_0 + \frac{m}{\gcd(a, m)} t, y_0 - \frac{a}{\gcd(a, m)} t\right)
\]

where \(t\) can be any integer. The \(x\) coordinates of these solutions are

\[
x = x_0 + \frac{m}{\gcd(a, m)} t
\]

(where \(t\) can be any integer) and these numbers are the solutions of the congruence equation (1). Thus, the solution set of (1) is \([x_0]_{m/\gcd(a, m)}\). We summarize this in the following theorem.

**Theorem 11** Let \(a\) and \(b\) be integers and let \(m\) be a positive integer:

1. If \(\gcd(a, m)\) does not divide \(b\), then the congruence equation (1) has no solutions.
2. If \( \gcd(a, m) \) divides \( b \), then the congruence equation (1) has infinitely many solutions. Furthermore, if \( x_0 \) is a solution of (1), then the solution set of (1) is \([x_0]_{m/\gcd(a,m)}\).

**Example 12** Find all solutions of the congruence equation

\[ 8x \equiv 3 \mod 2. \]

**Solution:** Since \( \gcd(8, 2) = 2 \) and since 2 does not divide 3, this congruence equation does not have any solutions.

**Example 13** Find all solutions of the congruence equation

\[ 8x \equiv 4 \mod 2. \]

**Solution:** Since \( \gcd(8, 2) = 2 \) and since 2 divides 4, this congruence equation does have solutions. It is easy to see by inspection that \( x_0 = 0 \) is a solution. Thus the complete solution set is

\[ [x_0]_{m/\gcd(a,m)} = [0]_1 = \mathbb{Z}. \]

In other words, **every** integer is a solution of this congruence equation.

**Example 14** Find all solutions of the congruence equation

\[ 3x \equiv 6 \mod 12. \]

**Solution:** Since \( \gcd(3, 12) = 3 \) and since 3 divides 6, this congruence equation does have solutions. It is easy to see by inspection that \( x_0 = 2 \) is a solution. Thus the complete solution set is

\[ [x_0]_{m/\gcd(a,m)} = [2]_4 = \{2, 6, 10, 14, \ldots \} \cup \{-2, -6, -10, -14, \ldots \}. \]

**Remark 15** In Example 13, we saw that the solution set of \( 8x \equiv 4 \mod 2 \) is \([0]_1 = \mathbb{Z}\). Note that we cannot, in solving this congruence, divide both sides of \( 8x \equiv 4 \) by 4 to obtain \( 2x \equiv 1 \mod 2 \). The latter congruence equation in fact has no solutions because \( \gcd(2, 2) = 2 \) and 2 does not divide 1. However, in solving the congruence equation \( ax \equiv b \mod m \), if \( a, b \), and \( m \) all have a common factor, then we can divide through by this common factor (making sure to also divide \( m \) by this common factor). Thus \( 8x \equiv 4 \mod 2 \) is equivalent to \( 4x \equiv 2 \mod 1 \). (Note that \( 4x \equiv 2 \mod 1 \) also has solution
set \([0]_1\), the same as the original congruence equation.) As another example, the equation \(3x \equiv 6 \mod 12\) is equivalent to \(x \equiv 2 \mod 4\), which has solution set \([2]_4\), just as we found in Example 14 without cancelling the factor of 3. The reason that this cancellation is permissible is that all solutions of the congruence equation \(ax \equiv b \mod m\) are found by solving the Diophantine equation \(ax + my = b\) and we know that division of this equation by a common factor of \(a\), \(m\), and \(b\) is permissible.

4 Unions and Intersections of Equivalence Classes

4.1 Unions of Equivalence Classes

The following theorem shows how an equivalence class modulo \(p\) (where \(p\) is some positive integer) can be written as the union of equivalence classes modulo \(q\), where \(q\) is a multiple of \(p\).

**Theorem 16** Suppose that \(p\) and \(q\) are positive integers and that \(q\) is divisible by \(p\). Specifically suppose that \(q = kp\) for some (positive) integer \(k\). Also, suppose that \(x_0\) is an integer. Then

\[
[x_0]_p = \bigcup_{r=0}^{k-1} [x_0 + pr]_q.
\]

Before proving this theorem, we will give an example that illustrate the theorem and we will also state two corollaries to the theorem.

**Example 17** Express \([5]_8\) as a union of equivalence classes modulo 24. Also, express \([5]_8\) as a union of equivalence classes modulo 40.

**Solution 18** Since \(24 = 3 \cdot 8\), our theorem tells us that

\[
[5]_8 = \bigcup_{r=0}^{2} [5 + 8r]_{24} = [5]_{24} \cup [13]_{24} \cup [21]_{24}.
\]

We can verify that this is correct by writing out the members of each of the equivalence classes involved:

\[
[5]_8 = \{5, 13, 21, 29, 37, 45, 53, \ldots\} \cup \{-3, -11, -19, -27, -35, -43, -51, \ldots\}
\]
\[
[5]_{24} = \{5, 29, 53, 77, \ldots\} \cup \{-19, -43, -67, -91, \ldots\}
\]
\[
[13]_{24} = \{13, 37, 61, 85, \ldots\} \cup \{-11, -35, -59, -83, \ldots\}
\]
\[
[21]_{24} = \{21, 45, 69, 93, \ldots\} \cup \{-3, -27, -51, -75, \ldots\}.
\]
Since \(40 = 5 \cdot 8\), we see that

\[
[5]_{s8} = \bigcup_{r=0}^{4} [5 + 8r]_{40} = [5]_{40} \cup [13]_{40} \cup [21]_{40} \cup [29]_{40} \cup [37]_{40}.
\]

For homework, you can write out the members of each of the above equivalence classes and convince yourself that the result is correct.

**Corollary 19** If \(p\) and \(q\) are positive integers and \(q = kt\), and if \(x_0\) is any integer, then \([x_0]_p\) is the union of exactly \(k\) equivalence classes modulo \(q\).

**Corollary 20** Assuming that \(\gcd(a, m)\) divides \(b\), and hence that the congruence equation \(ax \equiv b \mod m\) has a solution \(x_0\), the solution set of this congruence equation is

\[
[x_0]_{m/\gcd(a,m)} = \bigcup_{r=0}^{\gcd(a,m)-1} \left[ x_0 + \frac{m}{\gcd(a,m)} r \right]_m.
\]

To see that the above corollary follows from Theorem 16, we set \(p = m/\gcd(a,m)\) and \(q = m\). Then \(q = \gcd(a,m)p\) and we observe that the solutions set of \(ax \equiv b \mod m\) is

\[
[x_0]_{m/\gcd(a,m)} = [x_0]_p = \bigcup_{r=0}^{k-1} [x_0 + pr]_q = \bigcup_{r=0}^{\gcd(a,m)-1} \left[ x_0 + \frac{m}{\gcd(a,m)} r \right]_m.
\]

We now give the proof of Theorem 16.

**Proof.** Suppose that \(q = kp\) (where \(q\), \(p\), and \(k\) are all positive integers) and suppose that \(x_0\) is an integer. We want to prove that

\[
[x_0]_p = \bigcup_{r=0}^{k-1} [x_0 + pr]_q.
\]

Since this is an equation of sets, we use the usual approach – showing that each set is a subset of the other.

First, let \(x \in [x_0]_p\). Then there is some integer \(c\) such that \(x = x_0 + cp\).

By the Division Algorithm, there are integers \(t\) and \(r\) such that \(c = tk + r\) and \(0 \leq r < k\).
Thus
\[ x = x_0 + (tk + r)p = x_0 + tkp + pr = (x_0 + pr) + tq. \]

This shows that \( x \in [x_0 + pr]_q \). Since we know that \( 0 \leq r < k \), we conclude that \( x \in \bigcup_{r=0}^{k-1} [x_0 + pr]_q \) for some value of \( r \) between 0 and \( k - 1 \). This shows that \( x \in \bigcup_{r=0}^{k-1} [x_0 + pr]_q \) and hence \( [x_0]_p \subseteq \bigcup_{r=0}^{k-1} [x_0 + pr]_q \).

Now suppose that \( x \in \bigcup_{r=0}^{k-1} [x_0 + pr]_q \). Then \( x \in [x_0 + pr]_q \) for some value of \( r \). Thus there is an integer \( t \) such that \( x = (x_0 + pr) + tq \). Since \( q = kp \), we have \( x = x_0 + pr + tkp = x_0 + (r + tk)p \) and we see that \( x \in [x_0]_p \).

This proves that \( \bigcup_{r=0}^{k-1} [x_0 + pr]_q \subseteq [x_0]_p \) and the proof of the theorem is now complete. \( \blacksquare \)

**Exercise 21** Write \([6]_3\) as a union of equivalence classes modulo 9. Also write \([1]_4\) as a union of equivalence classes modulo 16. Also, show that it is not possible to write \([3]_4\) as a union of equivalence classes modulo 9.

**Exercise 22** Write the solution set of the congruence equation \( 48x \equiv 12 \mod 60 \) as a single equivalence class and as a union of equivalence classes modulo 60. Also, find the solution set of the congruence equation \( 2x \equiv 4 \mod 17 \). Is there more than one way to express this solution set? In general, if \( m \) is a prime number, what can you say about the solution set of \( ax \equiv b \mod m \)? In particular, will this equation always have solutions? If so, what does the solution set look like?

### 4.2 Intersections of Equivalence Classes

We will now prove a theorem concerning intersections of equivalence classes. It will be easiest to do this by first proving a couple of preliminary lemmas.

**Lemma 23** Suppose that \( m \) and \( n \) are positive integers and suppose that \( x_0 \) is an integer. Then
\[ [x_0]_m \cap [x_0]_n = [x_0]_{\text{lcm}(m,n)}. \]

Before proving this lemma, we illustrate it with an example.
Example 24 Since lcm (12, 16) = 48, our lemma tells us that if \( x_0 \) is any integer, then \( [x_0]_{12} \cap [x_0]_{16} = [x_0]_{48} \). Let us check that this is correct for \( x_0 = 3 \):

\[
[3]_{12} = \{3, 15, 27, 39, 51, 63, 75, \ldots\} \cup \{-9, -21, -33, -45, -57, -69, -81\ldots\}
\]
\[
[3]_{16} = \{3, 19, 35, 51, 67, 83, 99, \ldots\} \cup \{-13, -29, -45, -61, -77, -93, -109\ldots\}
\]
\[
[3]_{48} = \{3, 51, 99, 147, 195, \ldots\} \cup \{-45, -93, -141, -189, -237, \ldots\}\]

Proof. Assuming that \( m \) and \( n \) are positive integers and that \( x_0 \) is an integer, we want to prove that the two sets \( [x_0]_m \cap [x_0]_n \) and \( [x_0]_{\text{lcm}(m,n)} \) are equal.

Let \( x \in [x_0]_m \cap [x_0]_n \). Then \( x \in [x_0]_m \) and \( x \in [x_0]_n \). The fact that \( x \in [x_0]_m \) means that there exists an integer \( s \) such that \( x = x_0 + sm \). The fact that \( x \in [x_0]_n \) means that there exists an integer \( t \) such that \( x = x_0 + tn \). Therefore \( x - x_0 = sm = tn \), which means that \( x - x_0 \) is a common multiple of \( m \) and \( n \). Recalling that \( \text{lcm}(m,n) \) divides any common multiple of \( m \) and \( n \), we conclude that \( \text{lcm}(m,n) \) divides \( x - x_0 \). This means that there exists an integer \( k \) such that \( x - x_0 = k \cdot \text{lcm}(m,n) \) or, in other words, such that \( x = x_0 + k \cdot \text{lcm}(m,n) \). Therefore \( x \in [x_0]_{\text{lcm}(m,n)} \). We have now proved that \( [x_0]_m \cap [x_0]_n \subseteq [x_0]_{\text{lcm}(m,n)} \).

Now let \( x \in [x_0]_{\text{lcm}(m,n)} \). Then there exists an integer \( k \) such that \( x = x_0 + k \cdot \text{lcm}(m,n) \). Since \( \text{lcm}(m,n) \) is a multiple of both \( m \) and \( n \), there are integers \( s \) and \( t \) such that \( \text{lcm}(m,n) = sm = tn \). This shows that \( x = x_0 + ksm \) and \( x = x_0 + ktn \). Thus \( x \) is a member of both of the sets \( [x_0]_m \) and \( [x_0]_n \), which means that \( x \) is a member of the set \( [x_0]_m \cap [x_0]_n \). We have thus proved that \( [x_0]_{\text{lcm}(m,n)} \subseteq [x_0]_m \cap [x_0]_n \). The proof of the lemma is now complete. 

The above lemma has the following immediate corollary:

Corollary 25 If \( m \) and \( n \) are positive integers such that \( \gcd(m,n) = 1 \) and if \( x_0 \) is any integer, then

\[
[x_0]_m \cap [x_0]_n = [x_0]_{mn}.
\]

Proof. Recall that \( \text{lcm}(m,n) = (mn) / \gcd(m,n) \). If \( \gcd(m,n) = 1 \), then \( \text{lcm}(m,n) = mn \). 

Lemma 26 Suppose that \( m \) and \( n \) are positive integers and suppose that \( a \) and \( b \) are integers. Then \( [a]_m \cap [b]_n \neq \emptyset \) if and only if \( a \equiv b \mod \gcd(m,n) \).
Proof. Suppose that \([a]_m \cap [b]_n \neq \emptyset\). Then there is some integer \(x \in [a]_m \cap [b]_n\). Since \(x \in [a]_m\), there exists an integer \(s\) such that \(x = a + sm\).

Likewise, since \(x \in [b]_n\), there exists an integer \(t\) such that \(x = b - tn\). This means that \(b - a = sm + tn\). Recalling that every integer of the form \(sm + tn\) must be a multiple of \(\gcd(m, n)\) (from Section 1.3), we observe that \(b - a\) is a multiple of \(\gcd(m, n)\). Thus \(a \equiv b \mod \gcd(m, n)\).

Now, to prove the converse of this lemma, suppose that \(a \equiv b \mod \gcd(m, n)\). Then \(b - a\) is a multiple of \(\gcd(m, n)\). However, we know that there exist integers \(p\) and \(q\) such that \(\gcd(m, n) = pm + qn\). Therefore \(b - a\) is a multiple of \(pm + qn\). This means that there exists an integer \(k\) such that \(b - a = k(pm + qn)\) and this, in turn, implies that \(b - (kq)n = a + (kp)m\).

Since the number \(b - (kq)n\) is a member of \([b]_n\) and the number \(a + (kp)m\) is a member of \([a]_m\) and since these numbers are equal, we see that \([a]_m \cap [b]_n \neq \emptyset\).

Example 27 \([8]_9 \cap [3]_4 \neq \emptyset\) because \(\gcd(9, 4) = 1\) and \(8 \equiv 3 \mod 1\). Let us check this out:

\[
[8]_9 = \{8, 17, 26, \ldots \} \cup \{-1, -10, -19, \ldots \}
\]
\[
[3]_4 = \{3, 7, 11, \ldots \} \cup \{-1, -5, \ldots \}
\]

shows that \(-1 \in [8]_9 \cap [3]_4\).

Example 28 \([8]_9 \cap [4]_3 = \emptyset\) because \(\gcd(9, 3) = 3\) and \(8\) is not congruent to \(4\) modulo \(3\).

We will now put all of these pieces together in the form of the following theorem.

Theorem 29 If \(a \equiv b \mod \gcd(m, n)\), then there exists an integer \(x_0\) such that

\([a]_m \cap [b]_n = [x_0]_{\text{lcm}(m, n)}\).

Proof. Suppose that \(a \equiv b \mod \gcd(m, n)\). Then, by the preceding lemma, we know that \([a]_m \cap [b]_n \neq \emptyset\). This means that there exists some integer \(x_0 \in [a]_m \cap [b]_n\). Since \(x_0 \in [a]_m\), then \([a]_m = [x_0]_m\). Likewise, since \(x_0 \in [b]_n\), then \([b]_n = [x_0]_n\).

Therefore

\([a]_m \cap [b]_n = [x_0]_m \cap [x_0]_n = [x_0]_{\text{lcm}(m, n)}\).
The above theorem says that if \([a]_m \cap [b]_n \neq \emptyset\), then \([a]_m \cap [b]_n\) can be expressed as a single equivalence class modulo \(\text{lcm}(m, n)\). The problem that we encounter is to find a representative, \(x_0\), of this equivalence class. The way to find \(x_0\) is perhaps best illustrated by example.

**Example 30** Express \([4]_5 \cap [3]_{11}\) as a single equivalence class modulo 55. (Note that \(\text{lcm}(5, 11) = 55\).)

**Solution 31** In this case, there is an easy way to find \(x_0\). Just compute. Some members of \([4]_5\) are 4, 9, 14, 19, . . . and some members of \([3]_{11}\) are 3, 14, 25, . . . . Since 14 is a member of both equivalence classes, we see that \([4]_5 = [14]_5\) and \([3]_{11} = [14]_{11}\). Therefore

\[ [4]_5 \cap [3]_{11} = [14]_5 \cap [14]_{11} = [14]_{55}. \]

**Example 32** Express \([41]_{105} \cap [0]_8\) as a single equivalence class modulo 840. (Note that \(\text{lcm}(105, 8) = 840\).)

**Solution 33** We need to find a number, \(x_0\), such that \(x_0 = 41 + 105s\) and \(x_0 = 0 - 8t\) for some integers \(s\) and \(t\). To do this requires that we solve the Diophantine equation \(105s + 8t = -41\). Since

\[ 105 = 13 (8) + 1 \]

we see that

\[ 105 (1) + 8 (-13) = 1 \]

and thus (multiplying both sides of the above equation by \(-41\))

\[ 105 (-41) + 8 (533) = -41. \]

Therefore, we can take

\[ x_0 = 41 + 105 (-41) = 0 - 8 (533) = -4264. \]

We conclude that

\[ [41]_{105} \cap [0]_8 = [-4264]_{840}. \]

Since \([-4264]_{840} = [776]_{840}\), we can also write this as

\[ [41]_{105} \cap [0]_8 = [776]_{840}. \]
5 Solving Systems of Congruence Equations

The theory of the preceding section involving intersections of equivalence classes allows us to tackle the problem of solving systems of congruence equations. In order to see how to do this, let us look at a few examples.

Example 34 Solve the system

\[
\begin{align*}
    x &\equiv 2 \mod{3} \\
    4x &\equiv 6 \mod{6}.
\end{align*}
\]

Solution 35 Obviously, the first equation in the system has solution set \([2]_3\).

The second equation is equivalent to \(2x \equiv 3 \mod{3}\). Since \(\gcd(2, 3) = 1\) and 1 divides 3, this equation has solution set \([0]_3\). (The 0 is found by trying all possibilities: \(x = 0\), \(x = 1\), and \(x = 2\) and seeing that only \(x = 0\) works.)

The solution set of the system is \([2]_3 \cap [0]_3\), but this is obviously the empty set, so this equation system of congruence equations has no solution.

Example 36 Solve the system

\[
\begin{align*}
    2x &\equiv 1 \mod{5} \\
    2x &\equiv 1 \mod{9}.
\end{align*}
\]

Solution 37 The solution set of the first equation is \([3]_5\) and the solution set of the second equation is \([5]_9\). This means that the solution set of the system is \([3]_5 \cap [5]_9\). This intersection of congruence classes is equal to some congruence class modulo 45. To see which one, we need to find \(x_0\) such that

\[
x_0 = 3 + 5s = 5 - 9t.
\]

To do this, we must solve the Diophantine equation

\[
5s + 9t = 2.
\]

With a little experimentation, we discover that

\[
5(4) + 9(-2) = 2.
\]

Thus we see that we can take

\[
x_0 = 3 + 5(4) = 5 - 9(-2) = 23.
\]

The solution of the given system of congruence equations (expressed as a single equivalence class) is \([23]_{45}\).
Example 38  Solve the system of congruence equations

\[ x \equiv 2 \pmod{3} \]
\[ 4x \equiv 6 \pmod{7} \]
\[ 4x \equiv 5 \pmod{9}. \]

Solution 39  The first equation has solution set \([2]_3\) and the second equation has solution set \([5]_7\). Thus the solution set of just the first two equations is \([2]_3 \cap [5]_7\). This is equal to a single congruence class modulo 21. We need to find \(x_0\) such that

\[ x_0 = 2 + 3s = 5 - 7t. \]

To do this we must solve

\[ 3s + 7t = 3. \]

An obvious solution of this Diophantine equation is \((s, t) = (1, 0)\). Thus we can take

\[ x_0 = 2 + 3(1) = 5 - 7(0) = 5. \]

We conclude that the solution set of the first two equations is

\[ [2]_3 \cap [5]_7 = [5]_{21}. \]

Since the third equation of the system has solution set \([8]_9\), the entire system has solution set \([5]_{21} \cap [8]_9\). We must find \(x_0\) such that

\[ x_0 = 5 + 21s = 8 - 9t. \]

To do this, we must solve

\[ 21s + 9t = 3 \]

which is equivalent to

\[ 7s + 3t = 1. \]

We easily observe that

\[ 7(1) + 3(-2) = 1, \]

so we can take

\[ x_0 = 5 + 21(1) = 8 - 9(-2) = 26. \]

In conclusion, the solution set of this system of congruence equations is \([26]_{\text{lcm}(21,9)} = [26]_{63}\).
Let us randomly pick a member of the set \([26]_{63}\) and make sure that it works: One member of \([26]_{63}\) is \(x = 26 + (-8)(63) = -478\). Plugging this value into the system, we obtain

\[-478 \equiv 2 \pmod{3}\]
\[4(-478) \equiv 6 \pmod{7}\]
\[4(-478) \equiv 5 \pmod{9}.

or

\[-478 \equiv 2 \pmod{3}\]
\[-1912 \equiv 6 \pmod{7}\]
\[-1912 \equiv 5 \pmod{9}.

and all three of these equations are indeed true.

A special case of this work on solving systems of congruence equations is contained in the Chinese Remainder Theorem.

**Theorem 40 (Chinese Remainder Theorem)** Suppose that \(m_1, m_2, \ldots, m_n\) are positive integers that are pairwise relatively prime (meaning that \(\gcd(m_i, m_j) = 1\) when \(i \neq j\)). Also suppose that \(b_1, b_2, \ldots, b_n\) are any integers. Then the system of congruence equations

\[x \equiv b_1 \pmod{m_1}\]
\[x \equiv b_2 \pmod{m_2}\]
\[\vdots\]
\[x \equiv b_n \pmod{m_n}\]

has a solution \(x_0\). Furthermore, the entire solution set of this system is \([x_0]_{m_1 m_2 \cdots m_n}\).

**Proof.** Since \(\gcd(1, m_1) = 1\), the first equation of the system has solution set \([b_1]_{m_1}\). Likewise, the second equation has solution set \([b_2]_{m_2}\). Therefore, the solution set of the first two equations is \([b_1]_{m_1} \cap [b_2]_{m_2}\) and we know that this is equal to some equivalence class modulo \(m_1 m_2\) since \(\gcd(m_1, m_2) = 1\). Suppose that

\([b_1]_{m_1} \cap [b_2]_{m_2} = [z]_{m_1 m_2}\).
The solution set of the third equation (if there is a third equation) is \([b_3]_{m_3}\). This means that the solution set of the first three equations is \([z]_{m_1 m_2} \cap [b_3]_{m_3}\). Since \(\gcd(m_1, m_3) = 1\) and \(\gcd(m_2, m_3) = 1\), then \(\gcd(m_1 m_2, m_3) = 1\) (by a homework problem in Section 1.3 which was also on Exam 1). Therefore \([z]_{m_1 m_2} \cap [b_3]_{m_3}\) is equal to some equivalence class modulo \(m_1 m_2 m_3\). Since this type of reasoning can obviously be continued, we have proved the theorem.

**Example 41** Consider the system of congruence equations

\[
\begin{align*}
x &\equiv 2 \pmod{3} \\
x &\equiv 1 \pmod{5} \\
x &\equiv 6 \pmod{7} \\
x &\equiv 8 \pmod{8}.
\end{align*}
\]

Since the numbers 3, 5, 7, and 8 are pairwise relatively prime, the Chinese Remainder Theorem guarantees us that the above system has a solution and that the solution set of this system is some equivalence class modulo \(3 \cdot 5 \cdot 7 \cdot 8 = 840\).

**Exercise 42** Find the solution set of the system of congruence equations in Example 41. (The answer is \([776]_{840}\).)

**Exercise 43** In the textbook, Section 2.1 (pages 68 and 69), do problems 1, 5, 6, 7, 9, 11, 14, 15, 17, 18, and 19.