4.4 Solving Congruences using Inverses

Solving linear congruences is analogous to solving linear equations in calculus. Our first goal is to solve the linear congruence \( ax \equiv b \pmod{m} \) for \( x \). Unfortunately we cannot always divide both sides by \( a \) to solve for \( x \).

Example 1. \( 24 \equiv 8 \pmod{16} \). However, if we divide both sides of the congruence by 8, we end up with a wrong congruence: \( 3 \not\equiv 1 \pmod{16} \). In fact, \( 3 \equiv 3 \pmod{16} \).

Although we cannot always divide both sides of a congruence by any integer to produce a valid congruence, we can if this integer is relatively prime to the modulus, as shown in Theorem 7 in Section 4.3:

Theorem. Suppose \( m, a, b, c \in \mathbb{Z} \) and \( m \not\equiv 0 \). \( ac \equiv bc \pmod{m} \) and \( \gcd(c, m) = 1 \Rightarrow a \equiv b \pmod{m} \).

One method to solve \( ax \equiv b \pmod{m} \) for \( x \), is to use an integer \( \bar{a} \) such that \( \bar{a}a \equiv 1 \pmod{m} \).

Definition 1. If \( \bar{a} \in \mathbb{Z} \) satisfies \( a\bar{a} \equiv 1 \pmod{m} \), we say \( \bar{a} \) is inverse of \( a \) modulo \( m \).

The following theorem guarantees that the inverse of \( a \) exists whenever \( a \) and \( m \) are relatively prime.

Theorem 1. If \( \gcd(a, m) = 1 \) and \( m > 1 \), then an inverse of \( a \) modulo \( m \) exists. Furthermore, this inverse is unique modulo \( m \). (That is, there is a unique positive integer \( \bar{a} < m \) that is an inverse of \( a \) modulo \( m \) and every other inverse of \( a \) modulo \( m \) is congruent to \( \bar{a} \) modulo \( m \).)

Proof. By Bézout’s Theorem, since \( \gcd(a, m) = 1 \), there exist integers \( s \) and \( t \) such that

\[
1 = sa + tm.
\]

Therefore

\[
sa + tm \equiv 1 \pmod{m}.
\]

Because \( tm \equiv 0 \pmod{m} \), it follows that

\[
sa \equiv 1 \pmod{m}.
\]

Therefore \( s \) is an inverse of \( a \) modulo \( m \).

To show that the inverse of \( a \) is unique, suppose that there is another inverse \( b \) of the \( a \) modulo \( m \). Thus we have \( ba \equiv 1 \pmod{m} \). This congruence means \( m \mid ba - 1 \). Similarly, \( m \mid sa - 1 \). Therefore \( m \) divides the difference \( (ba - 1) - (sa - 1) = ba - sa \). Thus \( ba \equiv sa \pmod{m} \). It follows from Theorem 7 in Section 4.3 that \( b \equiv s \pmod{m} \).
To solve \( ax \equiv b \) (mod \( m \)), if the inverse of \( a \) exists, we may multiply both sides by this inverse and obtain \( x \). Thus it is useful to first solve \( ay \equiv 1 \) (mod \( m \)).

Using inspection to find an inverse of \( a \) modulo \( m \) is easy when \( m \) is small. For example, to find an inverse of 3 modulo 7, we can find \( j \cdot 3 \) for \( j = 1, 2, \ldots, 6 \), stopping when we find a multiple of 3 that is one more than a multiple of 7. So \( 2 \cdot 3 \equiv 6 \equiv -1 \) (mod 7). Thus \( -2 \cdot 3 \equiv 1 \) (mod 7). Note that every integer congruent to \(-2\) modulo 7 is also an inverse of 3, such as 5, \(-9\), 12, and so on.

Therefore the inverse of 3 modulo 7 is \(-2 \equiv 5 \) (mod 7).

A more efficient way to find the inverse of an \( a \) modulo \( m \), especially for large numbers, is by reversing the steps in Euclidean Algorithm and finding the Bézout’s linear combination of gcd(\( a, m \)) = 1 in terms of \( a \) and \( m \). That is, find \( sa + tm = 1 \), where \( s \) and \( t \) are integers. Reducing both sides of this equation modulo \( m \) tells us that \( s \) is an inverse of \( a \) modulo \( m \).

**Example 2.** Find an inverse of 4 modulo 15 by first finding Bézout coefficients of 4 and 15.

**Solution.** Because \( \text{gcd}(4, 15) = 1 \), Theorem 1 tells us that an inverse of 4 modulo 15 exists. The Euclidean algorithm ends quickly when used to find the greatest common divisor of 4 and 15:

\[
\begin{align*}
15 &= 3 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0
\end{align*}
\]

So

\[
\begin{align*}
1 &= 1 \cdot 4 - 1 \cdot 3 \\
15 - 3 \cdot 4 &= 3 \\
\therefore 1 &= 1 \cdot 4 - (15 - 3 \cdot 4) \\
\therefore 1 &= 4 \cdot 4 + (-1) \cdot 15
\end{align*}
\]

We see that 4 is the inverse of 4 modulo 15. Indeed, \( 4 \cdot 4 \equiv 16 \equiv 1 \) (mod 15).

Once we have an inverse \( \bar{a} \) of \( a \) modulo \( m \), we can solve the congruence \( ax \equiv b \) (mod \( m \)) by multiplying both sides of the linear congruence by \( a \).

**Example 3.** What are the solutions of the linear congruence \( 3x \equiv 4 \) (mod 7)?

**Solution.** We saw that 5 is an inverse of 3 modulo 7. Multiplying both sides of the congruence by 5 shows that

\[ 5 \cdot 3x \equiv 5 \cdot 4 \pmod{7}. \]

Thus \( x \equiv 20 \equiv 6 \) (mod 7).

To check whether \( x \equiv 6 \) (mod 7) is a solution:

\[ 3x \equiv 3 \cdot 6 \pmod{7} \Rightarrow 3x \equiv 18 \equiv 4 \pmod{7}, \]

2
as desired. Thus all \( x \equiv 6 \pmod{7} \) are solutions, namely \(-8, -1, 6, 13, 20, \ldots\).

In the first century, the Chinese mathematician Sun-Tsu asked:
There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the following question: What are the solutions of the systems of congruences?

**Example 4.** Can we find \( x \) such that
\[
\begin{align*}
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 2 \pmod{7}
\end{align*}
\]
When does such an \( x \) exist? How to find it?

The Chinese remainder theorem, named after the Chinese heritage of problems involving systems of linear congruences, states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo the product of the moduli.

**Theorem 2 (The Chinese Remainder Theorem).** Let \( m_1, m_2, \ldots, m_n \) be pairwise relatively prime positive integers greater than one and \( a_1, a_2, \ldots, a_n \) arbitrary integers. Then the system
\[
\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
& \vdots \\
x &\equiv a_n \pmod{m_n}
\end{align*}
\]
has a unique solution modulo \( m = m_1m_2\cdots m_n \). (That is, there is a solution \( x \) with \( 0 \leq x < m \), and all other solutions are congruent modulo \( m \) to this solution.)

**Proof.** To establish this theorem, we need to show that a solution exists and that it is unique modulo \( m \). We show that the solution exists by describing how to get \( x \). The proof of uniqueness is a homework problem (Exercise 30 in Section 4.4).

To construct a simultaneous solution, first let
\[M_k = \frac{m}{m_k}\]
for \( k = 1, 2, \ldots, n \). That is, \( M_k \) is the product of the moduli except for \( m_k \). Because \( m_i \) and \( m_k \) have no common factors greater than 1 when \( i \neq k \), it follows that \( \gcd(m_k, M_k) = 1 \). Consequently, by Theorem 1, we know that there is an integer \( y_k \), an inverse of \( M_k \) modulo \( m_k \), such that
\[M_ky_k \equiv 1 \pmod{m_k}.
\]
To construct a simultaneous solution, form the sum
\[x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n.
\]
We will now show that $x$ is a simultaneous solution. First, note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the $k$th term in this sum are congruent to 0 modulo $m_k$. Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k},$$

for $k = 1, 2, \ldots, n$. We have shown that $x$ is a simultaneous solution to the $n$ congruences.

**Solution to Sun-Tsu’s Problem.** The moduli 3, 5, and 7 are pairwise relatively prime, so the Chinese Remainder Theorem applies.

Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 5 \cdot 7 = 35$, $M_2 = m/5 = 3 \cdot 7 = 21$, and $M_3 = m/7 = 3 \cdot 5 = 15$.

The inverse of $M_1$ modulo 3 is 2 because $35 \cdot 2 \equiv 2 \cdot 2 \equiv 4 \equiv 1 \pmod{3}$.

The inverse of $M_2$ modulo 5 is 1 because $21 \cdot 1 \equiv 21 \equiv 1 \pmod{5}$.

The inverse of $M_3$ modulo 7 is 1 because $15 \cdot 1 \equiv 15 \equiv 1 \pmod{7}$.

The solutions to this system are those $x$ such that

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$

$$= 140 + 63 + 30$$

$$= 233$$

$$\equiv 23 \pmod{105}.$$

It follows that 23 is the smallest positive integer that is a simultaneous solution.

We conclude that 23 is the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

Another method, called back substitution, is often more efficient to solve a system of linear congruences. The following example demonstrates this method.

**Example 5.** Find all integers $x$ such that $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{6}$, and $x \equiv 3 \pmod{7}$.
Solution.

\[ x \equiv 1 \pmod{5} \]
\[ \therefore x = 5t + 1 \quad \text{for some integer } t \]
\[ \therefore 5t + 1 \equiv 2 \pmod{6} \]
\[ \therefore 5t \equiv 1 \pmod{6} \]
\[ \therefore (-1 \cdot 5t) \equiv (-1 \cdot 1) \pmod{6} \]
\[ \therefore t \equiv -1 \equiv 5 \pmod{6} \]
\[ \therefore t = 6u + 5 \quad \text{for some integer } u \]
\[ \therefore x = 5(6u + 5) + 1 \]
\[ \therefore x = 30u + 26 \]
\[ \therefore 30u + 26 \equiv 3 \pmod{7} \]
\[ \therefore 30u \equiv -23 \pmod{7} \]
\[ \therefore 30u \equiv 5 \pmod{7} \]
\[ \therefore (-3 \cdot 30u) \equiv (-3 \cdot 5) \pmod{7} \]
\[ \therefore u \equiv -15 \pmod{7} \]
\[ \therefore u \equiv -1 \pmod{7} \]
\[ \therefore u \equiv 6 \pmod{7} \]
\[ \therefore u = 7v + 6 \quad \text{for some integer } v \]
\[ \therefore x = 30(7v + 6) + 26 \]
\[ \therefore x = 210v + 180 + 26 \]
\[ \therefore x = 210v + 206 \]

Translating the last equation back into a congruence, we find the solution to the simultaneous congruences,

\[ x \equiv 206 \pmod{210}. \]

Fermat’s Little Theorem

One of the most useful of important discoveries of the great French mathematician Pierre de Fermat is that \( p \) divides \( a^{p-1} - 1 \) whenever \( p \) is prime and \( a \) is an integer not divisible by \( p \).

**Theorem 3** (Fermat’s Little Theorem). If \( p \) is prime and \( a \in \mathbb{Z}, p \not\mid a \), then

\[ a^{p-1} \equiv 1 \pmod{p}. \]

Furthermore, for every integer \( a \), we have

\[ a^p \equiv a \pmod{p}. \]

**Proof.** Suppose that integer \( a \) is not divisible by prime \( p \). Then no two of integers \( a, 2a, 3a, \ldots, (p - 1)a \) are congruent modulo \( p \), for if two of these integers were
congruent modulo $p$, say $ia$ and $ja$, where $1 \leq i < j < p$, then we would have $p \mid ja - ia$, or $p \mid a(j - i)$. By Lemma 2 in Section 4.3, since $a$ is not divisible by $p$, $p$ must divide $j - i$, which is impossible, because $0 < j - i < p$. Therefore, no two of the integers $a, 2a, 3a, \ldots, (p - 1)a$ are congruent modulo $p$. Therefore, each must be congruent to a different number from 1 to $p - 1$. Thus if we multiply them all together, we will obtain the same product, modulo $p$, as if we had multiplied all the numbers from 1 to $p - 1$. Therefore,

$$2 \cdot 3 \cdots (p - 1) \equiv a(2a)(3a) \cdots (p - 1)a \pmod{p}. $$

The right-hand side of this congruence is $(p - 1)! \cdot a^{p-1}$, and the left-hand side is $(p - 1)!$. Therefore,

$$(p - 1)! \equiv a^{p-1}(p - 1)! \pmod{p}. $$

The contrapositive statement of Lemma 3 in Section 4.3 states that if $p \nmid a_i$, then $p \nmid a_1a_2 \cdots a_n$, when $p$ is a prime. Thus here we have $p \nmid (p - 1)!$. Since $\gcd(p, (p - 1)!) = 1$, by Theorem 7 in Section 4.3, we conclude that the above congruence may be written as

$$a^{p-1} \equiv 1 \pmod{p}. $$

For the second part of Fermat’s Little Theorem, if $p \mid a$, then both sides of $a^p \equiv a \pmod{p}$ are 0 modulo $p$, so the congruence holds. If $p \nmid a$, then we may multiply both sides of

$$a^{p-1} \equiv 1 \pmod{p}$$

by $a$ to obtain

$$a^p \equiv a \pmod{p}. $$

Fermat’s little theorem is extremely useful in computing the remainders modulo $p$ of large powers of integers.

**Example 6.** Find $7^{222} \pmod{11}$.

**Solution.** By Fermat’s little theorem, we know that $7^{10} \equiv 1 \pmod{11}$. Thus

$$7^{222} = 7^{220+2} = 7^{220} \cdot 7^2 = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 49 \equiv (49 - 44) \equiv 5 \pmod{11}. $$

Therefore $7^{222} \pmod{11} = 5$. 

The above example illustrated how we can use Fermat’s little theorem to compute $a^n \pmod{p}$, where $p$ is prime and $p \nmid a$. First, we use the division algorithm to find the quotient $q$ and remainder $r$ when $n$ is divided by $p - 1$, so that $n = q(p - 1) + r$ where $0 \leq r < p - 1$. It follows that $a^n = a^{q(p - 1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}$. Hence, to find $a^n \pmod{p}$, we only need to compute $a^r \pmod{p}$. 
