Exercise 1. Solve the following systems of linear congruences.

(i) \begin{align*}
x &\equiv 0 \mod 2 \\
x &\equiv 0 \mod 3 \\
x &\equiv 1 \mod 5 \\
x &\equiv 6 \mod 7 \\
x &\equiv 2 \mod 11 \\
x &\equiv 3 \mod 12 \\
x &\equiv 4 \mod 13 \\
x &\equiv 5 \mod 17 \\
x &\equiv 5 \mod 19
\end{align*}

Solutions: (i) Since \(0 \equiv 6 \mod 2, \quad 0 \equiv 6 \mod 3, \quad \text{and} \quad 1 \equiv 6 \mod 5,\) the given system of congruences can be rewritten as

\begin{align*}
x &\equiv 6 \mod 2 \\
x &\equiv 6 \mod 3 \\
x &\equiv 6 \mod 5 \\
x &\equiv 6 \mod 7
\end{align*}

This last system has the obvious solution \(x = 6.\) On the other hand, since the moduli 2, 3, 5, and 7 are pairwise relatively prime, the Chinese Remainder Theorem asserts that the system has a unique solution modulo \(2 \cdot 3 \cdot 5 \cdot 7 = 210.\) We deduce that

\(x \equiv 6 \mod 210\)

is the solution set of the given system.

Alternate Solution. Setting \(n_1 = 2, \quad n_2 = 3, \quad n_3 = 5, \quad \text{and} \quad n_4 = 4,\) we have \(N = 210\) and

\(N_1 = 105, \quad N_2 = 70, \quad N_3 = 42, \quad \text{and} \quad N_4 = 30.\)

Following the proof of the Chinese Remainder Theorem provided in class, we use the Euclidean Algorithm to obtain

\[1 \cdot 105 + 1 \cdot 70 + (-2) \cdot 42 + (-3) \cdot 30.\]

Since \(a_1 = 0 = a_2, \quad a_3 = 1, \quad \text{and} \quad a_4 = 6,\) we deduce that the solution of (i) is

\[x \equiv 0 \cdot 1 \cdot 105 + 0 \cdot 1 \cdot 70 + 1 \cdot (-2) \cdot 42 + 6 \cdot (-3) \cdot 30 = -84 - 540 = -624 = 6 - 630 \equiv 6 \mod 210.\]

(ii) Since

\begin{align*}
x &\equiv 2 \equiv -9 \mod 11 \\
x &\equiv 3 \equiv -9 \mod 12 \\
x &\equiv 4 \equiv -9 \mod 13
\end{align*}

we see that \(x = -9\) is a solution to the first three congruences of the system. Observing that the moduli are pairwise relatively prime (each of 11 and 13 are prime since none are divisible by 2 and 3, while the prime factors of 12 are precisely 2 and 3), the Chinese Remainder Theorem allows us to conclude that

\[x \equiv -9 \mod 11 \cdot 12 \cdot 13 = 1716\]
is the unique solution of the first three congruences. On the other hand, the last two congruences have the obvious solution \( x = 5 \), hence a second application of the Chinese Remainder Theorem shows that

\[
x \equiv 5 \mod 17 \cdot 19 = 323
\]

is the unique solution of the last two congruences.

In summary, \( x \) is a solution of the given system (ii) if and only if it is a solution of the system

\[
\begin{align*}
x &\equiv -9 \mod 1716 \\
x &\equiv 5 \mod 323
\end{align*}
\]

Using the Euclidean Algorithm, we calculate

\[
1 = (-85) \cdot 323 + 16 \cdot 1716.
\]

Using the proof of the Chinese Remainder Theorem provided in class, we deduce that

\[
x \equiv (-9) \cdot (-85) \cdot 323 + 5 \cdot 16 \cdot 1716 = 384375 \mod 1716 \cdot 323 = 554268
\]

is the unique solution of the given system.

**Alternate Solution.** The first equation has the general solution

\[
x = 2 + 11t. \quad (a)
\]

Substituting in the second equation,

\[
2 + 11t \equiv 3 \mod 12
\]

which simplifies to

\[
11t \equiv 1 \mod 12.
\]

Observing that \(-1\) is an inverse of 11 modulo 12, the last equation has the solution

\[
t \equiv -1 \mod 12.
\]

Substituting for \( t \) in \((a)\), we deduce that the system

\[
\begin{align*}
x &\equiv 2 \mod 11 \\
x &\equiv 3 \mod 12
\end{align*}
\]

has the solution

\[
x \equiv -9 \mod 132.
\]

Writing

\[
x = -9 + 132s, \quad (b)
\]

substitution into the third congruence yields

\[
-9 + 132s \equiv 4 \mod 13,
\]

which simplifies to

\[
2s \equiv 0 \mod 13.
\]

Observing \( \gcd(2, 13) = 1 \), the last equation has the unique solution

\[
s \equiv 0 \mod 13.
\]
Substituting for $s$ in (b), we deduce that the system

\[
\begin{align*}
    x &\equiv 2 \mod 11 \\
    x &\equiv 3 \mod 12 \\
    x &\equiv 4 \mod 13
\end{align*}
\]

has the solution

\[x \equiv -9 \mod 1716.\]

Writing

\[x = -9 + 1716r, \quad (c)\]

substitution into the fourth congruence yeilds

\[-9 + 1716r \equiv 5 \mod 17,\]

which, observing $1716 \equiv -1 \mod 17$, simplifies to

\[-r \equiv 14 \mod 17.\]

This has the unique solution $r \equiv -14 \equiv 3 \mod 17$. Substituting for $r$ in (c), we deduce that the system

\[
\begin{align*}
    x &\equiv 2 \mod 11 \\
    x &\equiv 3 \mod 12 \\
    x &\equiv 4 \mod 13 \\
    x &\equiv 5 \mod 17
\end{align*}
\]

has the solution

\[x \equiv 5139 \mod 29172.\]

Finally, writing

\[x = 5139 + 29172q, \quad (d)\]

substitution into the final congruence yields

\[5139 + 29172q \equiv 5 \mod 19,\]

which, observing $29172 \equiv 7 \mod 19$, simplifies to

\[7q \equiv 15 \mod 19.\]

Observing that 11 is an inverse of 7 modulo 19, we see that the last congruence has the unique solution

\[q \equiv 15 \cdot 11 = 165 \equiv 13 \mod 19.\]

Substituting for $q$ in (d), we deduce that the given system has the unique solution

\[x \equiv 384375 \mod 554268.\]

Exercise 2. (i) Find all integers that leave remainder 9 when it is divided by either 10 or 11, but that are divisible by 13.

(ii) If eggs are removed from a basket 2, 3, 4, 5, and 6 at a time, there remains, respectively, 1, 2, 3, 4, and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?
Solution : (i) We are required to find all integers \( x \) such that
\[
\begin{align*}
  x &\equiv 9 \mod 10 \\
  x &\equiv 9 \mod 11 \\
  x &\equiv 0 \mod 13
\end{align*}
\]
Since 10 and 11 are relatively prime, the Chinese Remainder Theorem asserts that the first two equations are equivalent to the single equation
\[
x \equiv 9 \mod 110,
\]
hence the system is equivalent to
\[
\begin{align*}
  x &\equiv 9 \mod 110 \\
  x &\equiv 0 \mod 13 \quad \text{(a)}
\end{align*}
\]
Using the Euclidean Algorithm, we have
\[
1 = 17 \cdot 13 + (-2) \cdot 110.
\]
The proof of the Chinese Remainder Theorem allows us to conclude that the solution of the system (a) is
\[
x \equiv 9 \cdot 17 \cdot 13 + 0 \cdot (-2) \cdot 110 = 1989 \equiv 559 \mod 1430.
\]
In summary, the integers which leave remainder 9 when divided by 10 or 11 and that are divisible by 13 are precisely those of the form
\[
x = 559 + 1430t, \quad t \in \mathbb{Z}.
\]
(ii) If \( x \) denotes the number of eggs in the basket then the given conditions yield the system of congruences
\[
\begin{align*}
  x &\equiv 1 \mod 2 \\
  x &\equiv 2 \mod 3 \\
  x &\equiv 3 \mod 4 \\
  x &\equiv 4 \mod 5 \\
  x &\equiv 5 \mod 6 \\
  x &\equiv 0 \mod 7 \quad \text{(a)}
\end{align*}
\]
Consider the first of five congruences in the system (a). Observing
\[
1 \equiv -1 \mod 2, \quad 2 \equiv -1 \mod 3, \quad 3 \equiv -1 \mod 4, \quad 4 \equiv -1 \mod 5, \quad \text{and} \quad 5 \equiv -1 \mod 5,
\]
any solution \( x \) of (a) must satisfy the system
\[
\begin{align*}
  x &\equiv -1 \mod 2 \\
  x &\equiv -1 \mod 3 \\
  x &\equiv -1 \mod 4 \\
  x &\equiv -1 \mod 5 \\
  x &\equiv -1 \mod 6
\end{align*}
\]
hence
\[
x \equiv -1 \mod \text{lcm}(2, 3, 4, 5, 6) = 60.
\]
Conversely, any solution of the last congruence is a solution of the preceding five congruences. We deduce that the system (a) has the same solution set as the system
\[
\begin{align*}
  x &\equiv -1 \mod 60 \\
  x &\equiv 0 \mod 7 \quad \text{(b)}
\end{align*}
\]
The system (b) can be solved by appealing to the Chinese Remainder Theorem. Using the Euclidean Algorithm, we have

\[ 1 = (-17) \cdot 7 + 2 \cdot 60, \]

hence that solution of (b) consists of the congruence class

\[ x = -1 \cdot (-17) \cdot 7 + 0 \cdot 2 \cdot 60 = 119 \mod 480. \]

The number \( x \) of eggs thus has the form \( 119 + 480t \) for some integer \( t \). The least positive number occurs precisely when \( t = 0 \), which yields 119 eggs.

**Exercise 3.** Show that the system of congruences

\[ \begin{align*}
x &\equiv a_1 \mod n_1 \\
x &\equiv a_2 \mod n_2
\end{align*} \]

has a solution if and only if \( \gcd(n_1, n_2)|(a_1 - a_2) \). Furthermore, show that the solution (if it exists) is unique modulo \( \text{lcm}(n_1, n_2) \).

**Solution:** Set \( d = \gcd(n_1, n_2) \). If \( x = a \) is a solution of the system then the definition of congruences allows us to deduce that \( a - a_1 \) and \( a - a_2 \) are divisible by \( n_1 \) and \( n_2 \), respectively. Since \( n_1 \) and \( n_2 \) are both divisible by \( d \), it follows that \( d \) divides both \( a - a_1 \) and \( a - a_2 \), hence it also divides

\[ (a - a_1) - (a - a_2) = a_2 - a_1. \]

Conversely, suppose \( d \) divides the difference \( a_1 - a_2 \). The first equation of the given system has the solution

\[ x = a_1 + sn_1, \quad s \in \mathbb{Z}. \] \hspace{1cm} (1)

Substituting into the second equation,

\[ a_1 + sn_1 \equiv a_2 \mod m_1, \]

which can be rewritten as

\[ sn_1 \equiv a_2 - a_1 \mod m_1. \] \hspace{1cm} (2)

Since \( d = \gcd(n_1, n_2) \) is assumed to divide \( a_2 - a_1 \), the latter equation is known to have a solution \( s = s_0 \). Substituting for \( s \) in (1) will yield a solution \( x \) of the original system.

Furthermore, recalling that

\[ s = s_0 + k \frac{n_2}{d} \]

is the general solution of (2), the general solution of the original system is seen to be

\[ x = a_1 + \left( s_0 + k \frac{n_2}{d} \right) n_1 = a_1 + s_0n_1 + k \frac{n_1n_2}{d} = a_1 + s_0n_1 + k \text{lcm}(n_1, n_2), \quad k \in \mathbb{Z}, \]

i.e. the solution set of the original system consists of the unique congruence class

\[ x \equiv a_1 + s_0n_1 \mod \text{lcm}(n_1, n_2). \]

**Exercise 4.** Let \( m \) be a positive integer with prime factorization

\[ m = 2^{a_0}p_1^{a_1} \cdots p_r^{a_r} \]

where the \( p_i \) are distinct odd primes. Show that the congruence

\[ x^2 \equiv 1 \mod m \]
has exactly $2^{r+e}$ solutions, where

$$
e = \begin{cases} 
0, & \text{if } \alpha_0 = 0 \text{ or } 1; \\
1, & \text{if } \alpha_0 = 2; \\
2, & \text{if } \alpha_0 > 2. 
\end{cases}
$$

**Solution:** We note that if $x \mod m$ is a solution of the congruence

$$x^2 \equiv 1 \mod m \quad (1)$$

then the $r + 1$-tuple $(x \mod 2^{\alpha_0}, x \mod p_1^{\alpha_1}, \ldots, x \mod p_r^{\alpha_r})$ is a solution of the system of congruences

$$x_0^2 \equiv 1 \mod 2^{\alpha_0}$$
$$x_1^2 \equiv 1 \mod p_1^{\alpha_1}$$
$$\vdots$$
$$x_r^2 \equiv 1 \mod p_r^{\alpha_r} \quad (1')$$

On the other hand, if $(x_0 \mod 2^{\alpha_0}, x_1 \mod p_1^{\alpha_1}, \ldots, x_r \mod p_r^{\alpha_r})$ is a solution of $(1')$ then the Chinese Remainder Theorem provides a unique congruence class modulo $m$ such that

$$x \equiv x_0 \mod 2^{\alpha_0}, \quad x \equiv x_i \mod p_i^{\alpha_i}, \quad 1 \leq i \leq r.$$ 

In particular, writing $p_0 = 2$,

$$x^2 \equiv x_i^2 \equiv 1 \mod p_i^{\alpha_i}$$

for each $i$, hence

$$x^2 \equiv 1 \mod 2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r} = m.$$ 

The preceding discussion allows us to deduce that the number of solutions the original congruence $(1)$ is equal to the number of the solutions of the system of linear congruences $(1)'$. Since each of the variables in $(1)'$ are distinct, the number of solutions of $(1)'$ is equal to the product of the number of solutions of each of the individual equations. From exercise 7(b) of Assignment 3, the congruence

$$x_0^2 \equiv 1 \mod 2^{\alpha_0}$$

has 1 solution if $\alpha_0 = 1$, 2 solutions if $\alpha_0 = 2$, and 4 solutions if $\alpha_0 \geq 3$. Noting that the congruence

$$x_0^2 \equiv 1 \mod 1$$

has one incongruent solution modulo 1, we deduce

$$x_0^2 \equiv 1 \mod 2^{\alpha_0}$$

has $2^e$ solutions with $e$ as defined above. If $p$ is an odd prime and $k \geq 1$ then, as seen in class, the congruence

$$x^2 \equiv 1 \mod p^k$$

has exactly two incongruent solutions modulo $p^k$, namely $\pm 1$. As it contains $r$ different congruences of the last type, the system $(1)'$ thus has

$$2^e \cdot 2^r = 2^{e+r}$$

distinct solutions, which allows us that $(1)$ has the same number of distinct solutions modulo $m$.

**Exercise 5.** Find all the solutions of the following congruences.

(i) $X^3 + 8X^2 - X - 1 \equiv 0 \mod 11.$
(ii) $X^3 + 8X^2 - X - 1 \equiv 0 \mod 121.$
(iii) $X^3 + 8X^2 - X - 1 \equiv 0 \mod 1331$.

**Solution**: Set $f(X) = X^3 + 8X^2 - X - 1$.

(i) By inspection

$$4^3 + 8(4^2) - 4 - 1 = 64 + 128 - 4 - 1 = 187 = 11 \cdot 17 \equiv 0 \mod 11,$$

hence $X \equiv 4 \mod 11$ is a root of $f(X)$ modulo 11. Using long division

$$X^3 + 8X^2 - X - 1 \equiv (X - 4)(X^2 + X + 3) \mod 11.$$

By inspection,

$$5^2 + 5 + 3 = 25 + 5 + 3 = 33 = 11 \cdot 3 \equiv 0 \mod 11,$$

so $x \equiv 5 \mod 11$ is another root of $f(X)$ modulo 11. A second application of the long division shows

$$X^3 + 8X^2 - X - 1 \equiv (X - 4)(X^2 + X + 3) \equiv (X - 4)(X - 5)(X - 5) \mod 11.$$

From this, we deduce that the solutions of $X^3 + 8X^2 - X - 1 \equiv 0 \mod 11$ are $X \equiv 4 \mod 11$ and $X \equiv 5 \mod 11$.

(ii) Observing $121 = (11)^2$, the solutions of

$$X^3 + 8X^2 - X - 1 \equiv 0 \mod 121$$

arise from those of the congruence modulo 11 via Hensel’s Lemma. Before examining the cases, note

$$f'(X) = 3X^2 + 16X - 1 \equiv 3X^2 + 5X - 1 \mod 11.$$

(I) $f'(4) \equiv 3(4)^2 + 5(4) - 1 = 48 + 20 - 1 = 67 \equiv 1 \mod 11$. Hensel’s Lemma asserts that

$$s = 4 - f(4) = 4 - 187 = -183 \equiv 59 \mod 121$$

is the unique lift of 4 mod 11 to a root of $f(X)$ modulo 121.

(II) $f'(5) = 3(5)^2 + 5(5) - 1 = 75 + 5 - 1 = 99 \equiv 0 \mod 11$. Observing

$$f(5) = 5^3 + 8(5)^2 - 5 - 1 = 125 - 200 - 5 - 1 = -81 \not\equiv 0 \mod 121,$$

Hensel’s Lemma asserts that 5 does not lift to a solution modulo 121.

In summary, the congruence

$$X^3 + 8X^2 - 5 - 1 \equiv 0 \mod 121$$

has the unique solution $X \equiv 59 \mod 121$.

(iii) Observing $131 = (11)^3$, the solutions of

$$X^3 + 8X^2 - X - 1 \equiv 0 \mod 1331$$

arise from those of the congruence modulo $121 = (11)^2$ by Hensel’s Lemma. From (iii), the latter congruence has the unique solution

$$X \equiv 59 \mod 121.$$

Observing $f'(59) \equiv f'(4) \equiv 1 \mod 11$, Hensel’s Lemma asserts that

$$r = 59 - f(59) = 59 - [(59)^3 + 8(59)^2 - 59 - 1]$$

$$= 59 - [205379 + 27848 - 59 - 1]$$

$$= 59 - 233167 = -233108 \equiv -183 \mod 1331$$

is the unique lift of 59 mod 121 to a root of $f(X)$ modulo 1331.
In summary,

\[ X^3 + 8X^2 - X - 1 \equiv 0 \mod 1331 \]

has the unique solution \( x \equiv -183 \mod 1331 \).

**Exercise 6.** Solve the following congruences.

(i) \( 3X^2 - 8X + 4 \equiv 0 \mod 72 \).

(ii) \( X^6 - 2X^5 - 35 \equiv 0 \mod 6125 \).

**Solution:**

(i) Observing \( 72 = 8 \cdot 9 \), the Chinese Remainder Theorem allows one to conclude that the given congruence is equivalent to the system of congruences

\[
\begin{align*}
3X^2 - 8X + 4 & \equiv 0 \mod 8 \\
3X^2 - 8X + 4 & \equiv 0 \mod 9
\end{align*}
\]

Set \( f(X) = 3X^2 - 8X + 4 \). In the case of the prime 2, we have

\[ f(X) \equiv X^2 \mod 2, \]

which has the unique root \( X \equiv 0 \mod 2 \). Observing

\[ f'(X) = 6X - 8 \equiv 0 \mod 2 \]

and

\[ f(0) = 4 \equiv 0 \mod 4, \]

Hensel’s Lemma asserts that the solution 0 modulo 2 lifts to two solutions modulo 4, namely 0 and 2. The former solution does not lift to a solution modulo 8, since \( f'(0) \equiv 0 \mod 2 \) and \( f(0) \not\equiv 0 \mod 8 \). As

\[ f(2) = 3(2)^2 - 8(2) + 4 = 12 - 16 + 4 = 0, \]

the solution \( X = 2 \) lifts to two distinct solutions modulo 8, namely 2 and 6. In summary, the congruence

\[ 3X^2 - 8X + 4 \equiv 0 \mod 8 \]

has two exactly two solutions modulo 8, namely \( X \equiv 2 \mod 8 \) and \( X \equiv 6 \mod 8 \).

In the case of the prime 3,

\[ f(X) \equiv -8X + 4 \equiv X + 1 \mod 3 \]

has the unique root \( X \equiv -1 \mod 3 \). Observing

\[ f'(X) \equiv -8 \equiv 1 \mod 3 \]

and

\[ f(-1) = 3 + 8 + 4 = 15, \]

Hensel’s Lemma asserts that

\[ X = -1 - (1)(15) = -16 \equiv 2 \mod 9 \]

is the unique lift of \(-1 \mod 3\) to a root of \( f(X) \) modulo 9. In summary, the congruence

\[ 3X^2 - 8X + 4 \equiv 0 \mod 9 \]

has the unique solution \( X = 2 \) modulo 9.

In light of the preceding discussion, if \( X \) is a solution of the congruence

\[ 3X^2 - 8X + 4 \equiv 0 \mod 72 \]
then either

\[ X \equiv 2 \mod 8 \quad \text{or} \quad X \equiv 6 \mod 8 \]
\[ X \equiv 2 \mod 9 \quad \text{or} \quad X \equiv 2 \mod 9 \]

The Chinese Remainder Theorem asserts that the first system has the unique solution \( X \equiv 2 \mod 72 \).

Observing

\[ 1 = 9 - 8, \]
we see that the second system has the solution

\[ X \equiv 6 \cdot 9 - 2 \cdot 8 = 38 \mod 72. \]

In conclusion, the congruence

\[ 3X^2 - 8X + 4 \equiv 0 \mod 72 \]

has two solutions, namely \( X \equiv 2 \mod 72 \) and \( X \equiv 38 \mod 72 \).

(ii) Set \( f(X) = X^6 - 2X^5 - 35 \). Noting

\[ 6125 = 125 \cdot 49 = 5^3 \cdot 7^2, \]

the solution of the congruence

\[ f(X) \equiv 0 \mod 6125 \]

reduces via the Chinese Remainder Theorem to the solution of the system of congruences

\[ f(X) \equiv 0 \mod 125 \]
\[ f(X) \equiv 0 \mod 49 \]

Working with the prime \( p = 5 \), we observe

\[ f(x) = X^6 - 2X^5 - 35 \equiv X^6 - 2X^5 = X^5(X - 2) \mod 5. \]

It follows immediately that solution of the congruence \( f(X) \equiv 0 \mod 5 \) are \( x = 0 \) and \( 2 \) modulo 5.

To find the roots of \( f(X) \) modulo 125, we apply Hensel’s Lemma. There are two cases to consider. We first note

\[ f'(X) = 6X^5 - 10X^4 \equiv X^5 \mod 5. \]

(1) \( X \equiv 0 \mod 5 \): In this case, \( f'(0) \equiv 0 \mod 5 \). Observing

\[ f(0) = -35 \not\equiv 0 \mod 25 \]

Hensel’s Lemma asserts that the root 0 does not lift to a root modulo 25. A fortiori, it doesn’t lift to a root modulo 125.

(II) \( X \equiv 2 \mod 5 \): In this case,

\[ f'(2) \equiv 2^5 = 32 \equiv 2 \mod 5 \]

has inverse 3 mod 5. Observing

\[ f(2) = 2^5 - 2(2)^5 - 35 = -35, \]

Hensel’s Lemma asserts

\[ X \equiv 2 - 3 \cdot (-35) = 107 \equiv 7 \mod 25 \]

is the unique lift of 2 mod 5 to a root of modulo 25. Since

\[ f'(7) \equiv f'(2) \equiv 2 \mod 5, \]
Hensel’s Lemma asserts that 7 has a unique lift to a root of \( f(x) \) modulo 125. Observing
\[
f(7) = 7^6 - 2(7)^5 - 35 = 7^5(7 - 2) - 35 = 5 \cdot 7^5 - 35 = 35(7^4 - 1) = 35(2401 - 1) = 35 \cdot 2400 \equiv 0 \mod 125,
\]
we deduce \( x \equiv 7 \mod 125 \) is the appropriate lift.

In summary, the only root of \( f(X) \) modulo 125 is \( x \equiv 7 \mod 125 \).

Working with the prime 7, note
\[
f(X) = X^6 - 2X^5 - 35 \equiv X^6 - 2X^5 = x^5(X - 2) \mod 7.
\]

We deduce that the congruence \( f(X) \equiv 0 \mod 7 \) has the solutions \( X = 0 \) and \( 2 \) modulo 7.

To find the roots of \( f(X) \) modulo 49, we apply Hensel’s Lemma. There are two cases to consider. We first note
\[
f'(X) = 6X^5 - 10X^4 \equiv -X^5 - 3X^4 = -x^4(X + 3).
\]

(I) \( x \equiv 0 \mod 7 \) : In this case, \( f'(0) \equiv 0 \mod 5 \). Observing
\[
f(0) = -35 \not\equiv 0 \mod 49
\]
Hensel’s Lemma asserts that the root 0 does not lift to a root of \( f(X) \) modulo 49.

(II) \( X \equiv 2 \mod 7 \) : In this case,
\[
f'(2) \equiv -2^4(2 + 3) = -16 \cdot 5 \equiv -2 \cdot 5 = -10 \equiv -3 \mod 7
\]
has inverse 2 modulo 7. Observing
\[
f(2) = 2^6 - 2(2)^5 - 35 = -35,
\]
Hensel’s Lemma asserts that
\[
X = 2 - 2(-35) = 2 + 70 = 72 \equiv 23 \mod 49
\]
is the unique lift of 2 to a root of \( f(X) \) modulo 49.

In summary, \( f(X) \) has one root modulo 49, namely \( X \equiv 23 \mod 49 \).

The preceding discussion shows that if
\[
X^6 - 2X^5 - 35 \equiv 0 \mod 6125
\]
then
\[
X \equiv 7 \mod 125 \quad \text{and} \quad X \equiv 23 \mod 49.
\]

By the Euclidean Algorithm,
\[
-29 \cdot 125 + 74 \cdot 49 = 1.
\]
The Chinese Remainder Theorem thus allows us to conclude that the last system of congruences has the unique solution
\[
X = 23 \cdot (-29) \cdot 125 + 7 \cdot 74 \cdot 49 = -57993 \equiv 3257 \mod 6125
\]

In summary, the equation
\[
X^6 - 2X^5 - 35 \equiv 0 \mod 6125
\]
has the unique solution
\[
X \equiv 3257 \mod 6125
\]

**Bonus Question** Let \( a, b, \) and \( c \) be integers with \( \gcd(a, b) = 1 \). Show that there exists an integer \( n \) such that \( \gcd(an + b, c) = 1 \).
Solution: Let $n$ be the product of the primes which divide $c$ but do not divide $b$. Let $p$ be an arbitrary prime divisor of $c$. If it does not divide $b$ then $p$ divides $n$, hence

$$an + b \equiv b \neq 0 \mod p.$$ 

On the other hand, if it divides $b$ then $p$ does not divide $a$, since $\gcd(a, b) = 1$, nor does it divides $n$, by construction. Thus,

$$an + b \equiv an \neq 0 \mod p.$$ 

The preceding shows that $an + b$ and $c$ have no common prime divisors, hence

$$\gcd(an + b, c) = 1,$$

as required.