Exercises to turn in:

1. In each case determine whether the statement is true or false. (A calculator will be useful for the larger numbers.)

   (a) \( 40 \equiv 13 \) (mod 9)  \( \quad \) (b) \( -29 \equiv 1 \) (mod 7)  \( \quad \) (c) \( 8 \equiv 48 \) (mod 14)  \( \quad \) (d) \( -8 \equiv 48 \) (mod 14)  \( \quad \) (e) \( 7754 \equiv 357482 \) (mod 3643)  \( \quad \) (f) \( 4015 \equiv 33303 \) (mod 1295)

   \textbf{Answers:}

   (a) \textbf{True}: \( 40 - 13 = 27 = 9 \cdot 3 \) so \( 40 \equiv 13 \) (mod 9).

   (b) \textbf{False}: \( -29 - 1 = -30 \) and \( 7 \nmid -30 \) so \( -29 \not\equiv 1 \) (mod 7).

   (c) \textbf{False}: \( 8 - 48 = -40 \) and \( 14 \nmid -40 \), so \( 8 \not\equiv 48 \) (mod 14).

   (d) \textbf{True}: \( -8 - 48 = -56 = 14 \cdot 4 \) so \( -8 \equiv 48 \) (mod 14).

   (e) \textbf{True}: \( 357482 - 7754 = 349728 = 3643 \cdot 96 \) so \( 7754 \equiv 357482 \) (mod 3643).

   (f) \textbf{False}: \( 33303 - 4015 = 29288 = 22 \cdot 1295 + 798 \) so \( 1295 \nmid 33303 - 4015 \) and hence \( 4015 \not\equiv 33303 \) (mod 1295).

2. In each case find all integers \( k \) making the statement true.

   (a) \( 4 \equiv 2k \) (mod 7) \( \quad \) (b) \( 12 \equiv 3k \) (mod 10)  \( \quad \) (c) \( 3k \equiv k \) (mod 9)  \( \quad \) (d) \( 5k \equiv k \) (mod 15)

   \textbf{Answers:}

   (a) \( k \equiv 2 \) (mod 7), i.e., \( k = 2 + 7t \) where \( t \in \mathbb{Z} \).

   (b) \( k \equiv 4 \) (mod 10), i.e., \( k = 4 + 10t \) where \( t \in \mathbb{Z} \).

   (c) \( 3k \equiv c \) (mod 9) \( \iff \) \( 2k \equiv 0 \) (mod 9) \( \iff \) \( k \equiv 0 \) (mod 9) \( \iff \) \( k = 9t \) for \( t \in \mathbb{Z} \).

   (d) \( 5k \equiv k \) (mod 15) \( \iff \) \( 4k \equiv 0 \) (mod 15) \( \iff \) \( k \equiv 0 \) (mod 15) \( \iff \) \( k = 15t \) for \( t \in \mathbb{Z} \).

3. Find all incongruent solutions to each of the following congruences.

   (a) \( 7x \equiv 3 \) (mod 15)  \( \quad \) (b) \( 6x \equiv 5 \) (mod 15)  \( \quad \) (c) \( 3x \equiv 1 \) (mod 12)  \( \quad \) (d) \( 3x \equiv 1 \) (mod 11)  \( \quad \) (e) \( 15x \equiv 5 \) (mod 17)  \( \quad \) (f) \( 5x \equiv 5 \) (mod 18)  \( \quad \) (g) \( x^2 \equiv 1 \) (mod 8)  \( \quad \) (h) \( x^2 \equiv 3 \) (mod 7)

   \textbf{Answers:}

   (a) \( \text{Since gcd}(7, 15) = 1 \) any two solutions are congruent mod 15 (Theorem 8.1, Page 57 of the Congruence Supplement). To find this solution, start with \( 15 - 7 \cdot 2 = 1 \) and multiply by 3 to get \( 3 \cdot 15 + 7 \cdot (-6) = 3 \). Hence \( x = -6 \) is one solution to \( 7x \equiv 3 \) (mod 15) and all other solutions are of the form \( -6 + 15k \) for \( k \in \mathbb{Z} \). Note that the smallest positive solution is \( -6 + 15 = 9 \). \textit{Check:} \( 7 \cdot 9 = 63 \equiv 3 \) (mod 15).
(b) Since \( \gcd(6, 15) = 3 \) and \( 3 \nmid 5 \), Part (a) of Theorem 8.1 shows that there are no solutions to \( 6x \equiv 5 \pmod{15} \).

(c) Since \( \gcd(3, 12) = 3 \) and \( 3 \nmid 1 \), there are no solutions to \( 3x \equiv 1 \pmod{12} \).

(d) Since \( \gcd(3, 11) = 1 \) there is exactly one solution modulo 11, and by inspection \( 4 \cdot 3 \equiv 1 \pmod{11} \). Hence \( x \equiv 4 \pmod{11} \).

(e) Since \( \gcd(15, 17) = 1 \) there is exactly one solution modulo 17. To find it, start by using the Euclidean Algorithm to write 17r + 15s = 1:

\[
\begin{align*}
17 &= 15 + 12 \\
15 &= 2 \cdot 7 + 1,
\end{align*}
\]

so reversing these two steps gives:

\[
\begin{align*}
1 &= 15 - 7 \cdot 2 \\
&= 15 - 7(17 - 15) \\
&= 8 \cdot 15 - 7 \cdot 17.
\end{align*}
\]

This last equation gives \( 15 \cdot 8 \equiv 1 \pmod{17} \) and multiplication by 5 gives \( 15 \cdot 40 \equiv 5 \pmod{17} \). Hence the solutions of the congruence are \( x \equiv 40 \pmod{17} \). The smallest positive solution is \( 6 = 40 - 2 \cdot 17 \). Check: \( 15 \cdot 6 = 90 = 17 \cdot 5 + 5 \) so \( 15 \cdot 6 \equiv 5 \pmod{17} \).

(f) Since \( \gcd(5, 18) = 1 \), there is only one solution modulo 18, and that solution is found by inspection to be \( x = 1 \). Thus all solutions are \( x \equiv 1 \pmod{18} \).

(g) There are only 8 congruence classes modulo 8, so just compute the squares of each to see which are 1 modulo 8:

<table>
<thead>
<tr>
<th>x  \pmod{8}</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>x^2 \pmod{8}</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Thus, the solutions to \( x^2 \equiv 1 \pmod{8} \) are \( x \equiv k \pmod{8} \) where \( k = 1, 3, 5, 7 \).

(h) There are only 7 congruence classes modulo 7, so just compute the squares of each to see which are 3 modulo 7:

<table>
<thead>
<tr>
<th>x  \pmod{7}</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>x^2 \pmod{7}</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Thus, there are no solutions to \( x^2 \equiv 3 \pmod{7} \).

4. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.

(a) \( 72x \equiv 47 \pmod{200} \)

\[ \textbf{Solution.} \] \( \gcd(72, 200) = 8 \) so there are exactly 8 incongruent solutions. (Theorem 8.1, Part (b)).
(b) \(1537x \equiv 2862 \pmod{6731}\)

\[\textbf{Solution.}\] Using the Euclidean Algorithm (or a prime factorization table) one finds that \(\gcd(1537, 6731) = 53\), so there are exactly 53 incongruent solutions to the linear congruence \(1537x \equiv 2862 \pmod{6731}\).

5. If \(a \in \mathbb{Z}\) and \(n > 1\) then a \textit{multiplicative inverse of} \(a\) \textit{mod} \(n\) is a solution of the congruence \(ax \equiv 1 \pmod{n}\).

(a) Explain how Theorem 8.1 (Page 57) of the handout shows that \(a\) has a multiplicative inverse \textit{mod} \(n\) if and only if the greatest common divisor \((a, n) = 1\). Note that this theorem also shows you explicitly how to find the multiplicative inverse of \(a\) \textit{mod} \(n\), when it exists.

\[\textbf{Solution.}\] The theorem states that the congruence \(ax \equiv c \pmod{n}\) has a solution if (Part (b)) and only if (Part (a)) the greatest common divisor \(g\) of \(a\) and \(n\) divides \(c\). But if \(c = 1\), the only possible divisors of \(c\) are \(\pm 1\). Thus \(g|1\) if and only if \(g = 1\).

(b) Find the inverse of 13 mod 35.

\[\textbf{Solution.}\] Use the Euclidean Algorithm to write \(1 = 3 \cdot 35 - 8 \cdot 13\). This equation says that \(-8 \cdot 13 \equiv 1 \pmod{35}\), so the multiplicative inverse of 13 modulo 35 is \(-8\). Since \(-8 \equiv 27 \pmod{35}\), an equivalent answer is 27.

(c) Find the inverse of 9 mod 16.

\[\textbf{Solution.}\] Since \(1 = 9 \cdot 9 - 5 \cdot 16\), the multiplicative inverse of 9 modulo 16 is 9 (mod 16). That is, 9 is its own inverse modulo 16.

6. Let \(n = d_kd_{k-1} \cdots d_2d_1d_0\) be the decimal representation of \(n\). Recall that this means that

\[n = d_k10^k + d_{k-1}10^{k-1} + \cdots + d_210^2 + d_110 + d_0,
\]

and each \(d_j\) is an integer between 0 and 9.

(a) Show that \(3|n\) if and only if \(3|(d_0 + d_1 + \cdots + d_k)\).

\[\textit{Proof.}\] Since \(10 \equiv 1 \pmod{3}\), it follows (Page 53, Congruence Supplement) that \(10^j \equiv 1 \pmod{3}\) for all positive integers \(j\). Then, assuming that \(n = d_kd_{k-1} \cdots d_2d_1d_0\) is the decimal representation of \(n\), it follows (by substituting for the congruence \(10^j \equiv 1 \pmod{3}\) for \(1 \leq j \leq k\) that

\[n \equiv d_k10^k + d_{k-1}10^{k-1} + \cdots + d_210^2 + d_110 + d_0 \pmod{3}.
\]

Thus, we have shown that if \(n = d_kd_{k-1} \cdots d_2d_1d_0\) is the decimal representation of \(n\), then

\[n \equiv d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0 \pmod{3},
\]
that is, $n$ is congruence modulo 3 to the sum of its decimal digits. Since $3|n$ if and only if $n \equiv 0 \pmod{3}$, it follows that $3|n$ if and only if $3|(d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0)$ since both $n$ and $d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0$ have the same remainder upon division by 3.

(b) Show that $11|n$ if and only if $11|(d_0 - d_1 + d_2 - d_3 + \cdots \pm d_k)$.

Proof. Since $10 \equiv -1 \pmod{11}$, it follows (Page 53, Congruence Supplement) that $10^j \equiv (-1)^j \pmod{11}$ for all positive integers $j$. Then, assuming that $n = d_kd_{k-1}\cdots d_2d_1d_0$ is the decimal representation of $n$, it follows (by substituting for the congruence $10^j \equiv (-1)^j \pmod{11}$ for $1 \leq j \leq k$ that
\[
\begin{align*}
n &= d_k10^k + d_{k-1}10^{k-1} + \cdots + d_210^2 + d_110 + d_0 \\
&\equiv (-1)^kd_k + (-1)^{k-1}d_{k-1} + \cdots + d_2 - d_1 + d_0 \pmod{11}.
\end{align*}
\]

Thus, we have shown that if $n = d_kd_{k-1}\cdots d_2d_1d_0$ is the decimal representation of $n$, then
\[
n \equiv (-1)^kd_k + (-1)^{k-1}d_{k-1} + \cdots + d_2 - d_1 + d_0 \pmod{11},
\]
that is, $n$ is congruence modulo 11 to the alternating sum of its decimal digits. Since $11|n$ if and only if $n \equiv 0 \pmod{11}$, it follows that $11|n$ if and only if $11|((-1)^kd_k + (-1)^{k-1}d_{k-1} + \cdots + d_2 - d_1 + d_0)$ since both $n$ and $(-1)^kd_k + (-1)^{k-1}d_{k-1} + \cdots + d_2 - d_1 + d_0$ have the same remainder upon division by 11.

Hint: Use the congruences $10 \equiv 1 \pmod{3}$ and $10 \equiv -1 \pmod{11}$ and the rules of congruence arithmetic on Page 53 of the handout.