(1) Find the quotient and remainder in the Division Algorithm,
   (a) with divisor 16 and dividend 95,
   (b) with divisor 16 and dividend -95,
   (c) with divisor \([6.2]\) and dividend 95,
   (d) with divisor \([-6.2]\) and dividend 95.

   **Sol:**
   (a) \(95 = 16(5) + 15\), \(q = 5\), \(r = 15\)
   (b) \(-95 = 16(-6) + 1\), \(q = -6\), \(r = 1\)
   (c) \([6.2] = 6\), \(95 = 6(15) + 5\), \(q = 15\), \(r = 5\)
   (d) \([-6.2] = -7\), \(95 = -7(-13) + 4\), \(q = -13\), \(r = 4\)

(2) What is the value of \([x] + [-x]\) when \(x\) is real?

   **Sol:** The value is zero if \(x\) is an integer. If the value is not zero then it is the value -1.
   If \(x\) is an integer then it is easy to see that \([x] = -[-x]\) so \([x] + [-x] = 0\).
   If \(x\) is not an integer, first suppose \(x > 0\) Let \(x = n + r\), where \(n \in \mathbb{Z}^+\), and \(0 \leq r < 1\). Then \([x] = n\) and \([-x] = -n - 1\), thus \([x] + [-x] = -1\).
   If \(x < 0\) then \(-x > 0\) and since \(x = -(x)\), the above argument proves that in this case we also get -1.

   **Examples:** When \(x = 2\), \([2] + [-2] = 2 - 2 = 0\). When \(x = 3.5\), \([3.5] + [-3.5] = 3 - 4 = -1\)

(3) Show that there are no “prime triplets”, that is, primes, \(p\), \(p + 2\), and \(p + 4\) other than 3, 5, and 7.

   **Sol:** First, we divide \(p\) by 3. Since \(p \neq 3\), we know that \(p = 3q + r\) where either \(r = 1\) or \(r = 2\). Then, \(p + 2 = 3q + r + 2\) and \(p + 4 = 3(q + 1) + r + 1\).
   Either \(r + 2\) is divisible by 3, or \(r + 1\) is divisible by 3, thus either \(p + 2\) or \(p + 4\) is divisible by 3 if \(p\) is not.

(4) Use the Euclidean Algorithm to find the greatest common divisor of \(a\) and \(b\) and to express it as a linear combination of \(a\) and \(b\), where \(a = 1005\) and \(b = 320\).

   **Sol:**

   \[
   \begin{align*}
   1005 &= 320(3) + 45 \\
   320 &= 45(7) + 5 \\
   45 &= 5(9)
   \end{align*}
   \]
\[ \begin{align*}
5 &= 320 - 45(7) \\
45 &= 1005 - 320(3) \\
5 &= 320 - (1005 - 320(3))(7) \\
5 &= 320 - 1005(7) + 320(21) \\
5 &= 320(22) - 1005(7)
\end{align*} \]

(5) Find the prime factorization of \( a = 1005 \) and \( b = 320 \). Express the greatest common divisor of \( a \) and \( b \), \( (a, b) \), and the least common multiple of \( a \) and \( b \), \([a, b]\), in terms of the prime factorization of \( a \) and \( b \).

Sol:
\[ a = 1005 = 5 \cdot 201 = 5 \cdot 3 \cdot 67 \]
and we know 67 is prime because it has no prime factors less than \( \sqrt{67} = 8.18 \).
\[ b = 320 = 5 \cdot 64 = 5 \cdot 2^6 \]
\[ (a, b) = 5 \]
as shown above and
\[ [a, b] = 2^6 \cdot 3 \cdot 5 \cdot 67 = 64,320 \]

(6) Find all solutions of the following Linear Diophantine Equation.
\[ 35x + 133y = 1358 \]

Sol:
\[ 35x + 133y = 1358, \quad (35, 133) = 7, \quad 7|1358 \]
so there are infinitely many solutions as seen below. Find the gcd using the Euclidean Algorithm (work not shown here) \( 7 = 4 \cdot 35 - 133 \).

We multiply linear combination of gcd to get linear comb of 1358
\[ 194(7) = 194(4 \cdot 35 - 133), \quad 1358 = 776(35) - 194(133) \]
Let \( x_0 = 776 \) and \( y_0 = -194 \). Then we let \( x = 776 + 133/7(n) \) and \( y = -194 - 35/7(n) \), so that \( x = 776 + 19n \) and \( y = -194 - 5n \) These equations will return unique solutions for each \( n \).

(7) Find the least positive residue of \( 1! + 2! + 3! + \cdots + 75! \) modulo 15.

Sol:
Each factorial, \( n! \) for \( n \geq 5 \) is evenly divisible by 15 thus \( n! \equiv 0 \pmod{15} \) for \( n \geq 5 \). So we have:
\[ 1! + 2! + 3! + \cdots + 75! \equiv 1! + 2! + 3! + 4! + 0 + \cdots + 0 \pmod{15} \]
\[ \equiv 1 + 2 + 6 + 9 (mod 15) \]
\[ \equiv 3 (mod 15) \]

(8) Construct the table for multiplication modulo 6.

**Sol:**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

(9) Find the least positive residue modulo 25 of \(3^{47}\).

**Sol:** First we write 47 in binary \(47 = 2^5 + 2^3 + 2^2 + 2^1 + 2^0\), so that

\[3^{47} = 3^{(2^5+2^3+2^2+2^1+2^0)} = 3^{(2^5)}3^{(2^3)}3^{(2^2)}3^{(2^1)}3^{(2^0)}\]

We have

\[3^{(2^5)} \equiv 3 \pmod{25}\]

\[3^{(2^3)} \equiv 9 \pmod{25}\]

\[3^{(2^2)} \equiv 9^2 \equiv 6 \pmod{25}\]

\[3^{(2^1)} \equiv 6^2 \equiv 11 \pmod{25}\]

\[3^{(2^0)} \equiv 11^2 \equiv 21 \pmod{25}\]

Thus,

\[3^{47} \equiv 16 \cdot 11 \cdot 6 \cdot 9 \cdot 3 \pmod{25}\]

\[3^{47} \equiv 12 \pmod{25}\]

(10) Find all solutions of the linear congruence: \(15x \equiv 9 \pmod{27}\). Explain using solutions to Linear Diophantine Equations.

**Sol:**

\[15x \equiv 9 \pmod{27}\]

\[15x - 27y = 9\]

\[15(2) - 27(1) = 3\]

\[3[15(2) - 27(1)] = 3[3]\]

\[15(6) - 27(3) = 9\]
One Solution is $x = 6$ and $y = 3$. We are only interested in the value of $x$. All solutions are of the form:

$$x = 6 + (27/3)t, \quad y = 3 - (15/3)t$$

$$x = 6 + 9t, \quad y = 3 - 5t$$

There are 3 solutions modulo 27 because $(15, 27) = 3$ so $t = 0, 1, 2$ produces different solutions.

$$x = 6 + 9(0) = 6, \quad x = 6 + 9(1) = 15, \quad x = 6 + 9(2) = 24$$

(11) Using the Chinese Remainder theorem, find all solutions to the following system of linear congruences.

\[
\begin{align*}
    x &\equiv 1 \pmod{3} \\
    x &\equiv 2 \pmod{4} \\
    x &\equiv 3 \pmod{5}
\end{align*}
\]

**Sol:** Use the Chinese Remainder Theorem: There is a unique solution $X \pmod{M}$, where $M = 3 \cdot 4 \cdot 5$, whenever $(3, 4, 5) = 1$. This solution is

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3.$$  

$$M = 60, \quad M_1 = 60/3 = 20, \quad M_2 = 60/4 = 15, \quad M_3 = 60/5 = 12$$

$$a_1 = 1, \quad a_2 = 2, \quad a_3 = 3$$

$$M_1y_1 \equiv 1 \pmod{3}, \quad M_2y_2 \equiv 1 \pmod{4}, \quad M_3y_3 \equiv 1 \pmod{5}$$

$$y_1 = 2, \quad y_2 = 3, \quad y_2 = 3$$

So, $X = 238$

Since we know $X$ is unique modulo 60 we can factor out all multiples of 60.

Our solution of the problem is now 58 (mod 60).

Algebraically the solution can be described as $X = 60 \star n + 58$ where $n$ is an integer.

(12) Use Wilson’s Theorem to find the remainder when $7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43$ is divided by 11.

**Sol:**

$$7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43 \equiv 7 \cdot 8 \cdot 9 \cdot 4 \cdot 5 \cdot 6 \cdot 1 \cdot 2 \cdot 3 \cdot 10 \pmod{11}$$

$$7 \cdot 8 \cdot 9 \cdot 4 \cdot 5 \cdot 6 \cdot 1 \cdot 2 \cdot 3 \cdot 10 = 10!$$

So,

$$7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43 \equiv 10 \pmod{11}$$
(13) What is the remainder when $18!$ is divided by 437? Hint, $437 = 19 \cdot 23$. Use Wilson’s Theorem and the Chinese Remainder theorem.

**Sol:**

\[
437 = 19 \cdot 23 \\
18! \equiv 18 \pmod{19} \quad (1) \\
22! = 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv (-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot 18! \pmod{23} \\
\equiv 1 \cdot 18! \pmod{23} \\
\]

We also know $22! \equiv 22 \pmod{23}$. So,

\[
18! \equiv 22 \pmod{23} \quad (2) \\
\]

For (1) and (2), we know that there is a unique $x$ that satisfies,

\[
x \equiv 18 \pmod{19} \\
x \equiv 22 \pmod{23} \\
\]

By the Chinese remainder theorem, $x \equiv 436 \pmod{437}$ (work omitted here) and so

\[
18! \equiv 436 \pmod{437} \\
\]

(14) $\phi(n)$ is the Euler phi-function. Show that $\phi(5186) = \phi(5187) = \phi(5188)$.

**Sol:** First, factor each number into primes:

- $5186 = 2 \cdot 2593$
- $5187 = 3 \cdot 7 \cdot 13 \cdot 19$
- $5188 = 2^2 \cdot 1297$

Since the Euler phi-function is multiplicative, you can write each as a function of its primes:

\[
\phi(5186) = \phi(2) \cdot \phi(2593) \\
\phi(5187) = \phi(3) \cdot \phi(7) \cdot \phi(13) \cdot \phi(19) \\
\phi(5188) = \phi(2^2) \cdot \phi(1297) \\
\]

Finally, we can complete the calculations by using what we know about the Euler-phi function on primes, which is that $\phi(p^t) = p^t - p^{t-1}$.

\[
\phi(5186) = \phi(2) \cdot \phi(2593) = 1 \cdot 2592 = 2592 \\
\phi(5187) = \phi(3) \cdot \phi(7) \cdot \phi(13) \cdot \phi(19) = 2 \cdot 6 \cdot 12 \cdot 18 = 2592 \\
\phi(5188) = \phi(2^2) \cdot \phi(1297) = 2 \cdot 1296 = 2592 \\
\]

Therefore, $\phi(5186) = \phi(5187) = \phi(5188) = 2592$.

(15) Find all positive integers $n$ such that $\phi(n) = 4$. Be sure to prove that you have found all solutions.

**Sol:** $n = 5, 8, 10, \text{ and } 12$.

If $p^t | n$, then since $\phi$ is multiplicative, we know $\phi(p^t) | \phi(n)$ and since $\phi(p^t) = p^t - 1 | p - 1$, we have that $p^t - 1 | p - 1$.

We see that $p$ can only be 2, 3, or 5. So, $n = 2^a 3^b 5^c$.

If $p = 2$, then $t = 0, 1, 2, \text{ or } 3$. Suppose $t = 0$. Then $n = 3^b 5^c$ and $\phi(n) = 3^b 5^c (2/3)(4/5) = 4$. It must be that $b = 0$ and $c = 1$. Giving $n = 5$. 
Suppose $t = 1$. Then again, $\phi(n) = \phi(2)\phi(3^b5^c)$ which again implies $b = 0$ and $c = 1$. So $n = 10$ is a possibility.

Suppose $t = 2$. Then $4 = \phi(n) = \phi(2^2)\phi(3^b)\phi(5^c) = 2\phi(3^b)\phi(5^c)$ which can only happen if $b = 1$ and $c = 0$. This gives $n = 12$.

The last case is $t = 3$. Then $4 = \phi(n) = \phi(2^3)\phi(3^b)\phi(5^c) = 4\phi(3^b)\phi(5^c)$. So $b = 0$ and $c = 0$. This gives $n = 8$. 