Question 1. [p 139. #13]
Which combinations of pennies, dimes, and quarters have a total value of 99¢?

Solution: Let $x =$ # of pennies, $y =$ # of dimes, $z =$ # of quarters, then we want to solve the linear diophantine equation
\[ x + 10y + 25z = 99 \] (1)
in nonnegative integers.

Let $a = 1$, $b = 10$, $c = 25$, and $d = (a, b, c) = 1$, then $d \mid 99$ so there are solutions to (1). Setting
\[ 2y + 5z = t \] (2)
then $1 = 2 \cdot (-2) + 5 \cdot 1$, so that $t = 2 \cdot (-2t) + 5 \cdot t$, and a particular solution to (2) is $y_0 = -2t$, $z_0 = t$, and so the general solution to (2) is
\[ y = -2t + 5s \]
\[ z = t - 2s \]
where $s, t \in \mathbb{Z}$.

But then $x = 99 - 10y - 25z$ becomes $x = 99 - 5t$, and the general solution to (1) is
\[ x = 99 - 5t \]
\[ y = -2t + 5s \]
\[ z = t - 2s \]
where $s, t \in \mathbb{Z}$.

Since $x, y, z$ have to be nonnegative, then $(s, t)$ must lie in the region of the $s, t-$plane determined by the inequalities:
\[ 99 - 5t \geq 0 \]
\[ -2t + 5s \geq 0 \]
\[ t - 2s \geq 0. \]

That is,
\[ t \leq 19 \]
\[ 2t \leq 5s \]
\[ 2s \leq t \]

So we need to find the lattice points (i.e. points with integer coordinates) $(s, t)$ which lie inside the region shown.
This is most easily done by starting with \( t = 0 \), then \( t = 1 \), \ldots and finally \( t = 19 \), and for each \( t \) value, determining the values of \( s \) so that \((s, t)\) is in the region. For example,

If \( t = 0 \), then \( s = 0 \), and this implies that \( x = 99 \), \( y = 0 \), \( z = 0 \).

If \( t = 19 \), then \( s = 8 \) or \( s = 9 \), and this implies that \( x = 4 \), \( y = 2 \), \( z = 3 \) or \( x = 4 \), \( y = 7 \), \( z = 1 \).

Question 2. [p 149. #5]

Show that if \( a \) is an odd integer, then \( a^2 \equiv 1 \pmod{8} \).

**Solution:**

If \( a \equiv 1 \pmod{8} \), then \( a^2 \equiv 1^2 \equiv 1 \pmod{8} \).

If \( a \equiv 3 \pmod{8} \), then \( a^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod{8} \).

If \( a \equiv 5 \pmod{8} \), then \( a^2 \equiv 5^2 \equiv 25 \equiv 1 \pmod{8} \).

If \( a \equiv 7 \pmod{8} \), then \( a^2 \equiv 7^2 \equiv 49 \equiv 1 \pmod{8} \).

Therefore, \( a^2 \equiv 1 \pmod{8} \) for any odd integer \( a \) since every odd integer is congruent to 1, 3, 5, or 7 modulo 8.

Question 3. [p 149. #6]

Find the least nonnegative residue modulo 13 of each of the following integers.

(a) 22 \hspace{1cm} (d) \(-1\)

(b) 100 \hspace{1cm} (e) \(-100\)

(c) 1001 \hspace{1cm} (f) \(-1000\)

**Solution:**

(a) \( 22 \equiv 9 \pmod{13} \).

(b) \( 100 \equiv 9 \pmod{13} \).

(c) \( 1001 \equiv 0 \pmod{13} \).

(d) \( -1 \equiv 12 \pmod{13} \).

(e) \( -100 \equiv 4 \pmod{13} \).

(f) \( -1000 \equiv 1 \pmod{13} \).
Question 4. [p 149. #7]
Find the least positive residue of $1! + 2! + \cdots + 100!$ modulo each of the following integers.

(a) 2  (c) 12  
(b) 7  (d) 25  

Solution:

(a) $1! + 2! + \cdots + 100! \equiv 1 \pmod{2}$

(b) $1! + 2! + 3! + 4! + 5! + 6! + 7! + \cdots + 100! \equiv 1 + 2 + 6 + 24 + 120 + 720 \equiv 5 \pmod{7}$

(c) $1! + 2! + 3! + 4! + \cdots + 100! \equiv 9 \pmod{12}$

(d) $1! + 2! + \cdots + 9! + 10! + \cdots + 100! \equiv 1! + 2! + \cdots + 9! \pmod{25}$

Question 5. [p 150. #21]
For which positive integers $n$ is it true that

$$1^2 + 2^2 + 3^2 + \cdots + (n - 1)^2 \equiv 0 \pmod{n}?$$

Solution:

Recall that

$$1^2 + 2^2 + 3^2 + \cdots + (n - 1)^2 = \frac{(n - 1)n(2n - 1)}{6},$$

and since $(n, n - 1) = 1$ and $(n, 2n - 1) = 1$, then

$$n \mid \frac{(n - 1)n(2n - 1)}{6} \quad \text{if and only if} \quad 6 \mid (n - 1)(2n - 1).$$

Also, since $(n - 1, 2n - 1) = 1$, then $6 \mid (n - 1)(2n - 1)$ if and only if either (i) $6 \mid n - 1$, or (ii) $2 \mid n - 1$ and $3 \mid 2n - 1$.

(i) $6 \mid n - 1$ if and only if $n = 6k + 1$, that is, if and only if $n \equiv 1 \pmod{6}$.

(ii) $2 \mid n - 1$ and $3 \mid 2n - 1$ if and only if $n = 2k + 1$ and $2n = 3l + 1$. Now, $2n$ is even, so that $l$ is odd, say, $l = 2m + 1$. Thus, $2n = 6m + 4$, or $n = 3m + 2$. But since $n$ is odd, then $m$ must be odd, say, $m = 2q - 1$, so that $n = 6q - 1$, that is, $n \equiv -1 \pmod{6}$.

Therefore, $1^2 + 2^2 + 3^2 + \cdots + (n - 1)^2 \equiv 0 \pmod{n}$ if and only if $n \equiv \pm 1 \pmod{6}$. 

Question 6. [p 150. #25]
Show that if \( n \equiv 3 \pmod{4} \), then \( n \) cannot be the sum of the squares of two integers.

SOLUTION:
- If \( a \equiv 0 \pmod{4} \) then \( a^2 \equiv 0 \pmod{4} \)
- If \( a \equiv 1 \pmod{4} \) then \( a^2 \equiv 1 \pmod{4} \)
- If \( a \equiv 2 \pmod{4} \) then \( a^2 \equiv 0 \pmod{4} \)
- If \( a \equiv 3 \pmod{4} \) then \( a^2 \equiv 1 \pmod{4} \)

Therefore, if \( n = a^2 + b^2 \), then \( n \equiv 0, 1, \text{ or } 2 \pmod{4} \), but \( n \not\equiv 3 \pmod{4} \).

Question 7. [p 150. #20]
Show that if \( n \) is an odd positive integer or if \( n \) is a positive integer divisible by 4, then

\[
1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.
\]

Is this statement true if \( n \) is even but not divisible by 4?

SOLUTION: Recall that

\[
1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 = \frac{n^2(n-1)^2}{4},
\]

so that if \( n \) is an odd positive integer, then \( n-1 \) is even and \( 4 \mid (n-1)^2 \), so that \( n \mid \frac{n^2(n-1)^2}{4} \), and

\[
1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.
\]

If \( n \) is a multiple of 4, then \( \frac{n}{4} \) is an integer, and \( n \mid \frac{n^2(n-1)^2}{4} \), so that

\[
1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.
\]

in this case also.

If \( n \) is even, but \( 4 \nmid n \), then \( n = 2k \) where \( k \) is an odd integer, and \( n-1 \) is also odd, so that

\[
\frac{n^2(n-1)^2}{4} = k^2(2k-1)^2
\]

is an odd integer, and since \( n \) is even, then

\[
1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \not\equiv 0 \pmod{n}.
\]

Question 8. [p 157. #18]
Show that if \( p \) is an odd prime and \( a \) is a positive integer which is not divisible by \( p \), then the congruence \( x^2 \equiv a \pmod{p} \) has either no solution or exactly two incongruent solutions.

SOLUTION: Note first that if \( x_0^2 \equiv a \pmod{p} \), then \((-x_0)^2 \equiv a \pmod{p} \), so that \(-x_0 \) is also a solution.

Now note that \( x_0 \not\equiv -x_0 \pmod{p} \), since this implies that \( 2x_0 \equiv 0 \pmod{p} \), which is impossible since \( p \) is odd and \( p \nmid x_0 \), since \( x_0^2 \equiv a \pmod{p} \) and \( p \nmid a \).
To see that there are no more than two incongruent solutions, assume that $x = x_0$ and $x = x_1$ are both solutions to $x^2 \equiv a \pmod{p}$, then $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$, so that

$$x_0^2 - x_1^2 \equiv (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p},$$

so that $p \mid x_0 - x_1$ or $p \mid x_0 + x_1$, that is,

$$x_1 \equiv x_0 \pmod{p} \quad \text{or} \quad x_1 \equiv -x_0 \pmod{p}.$$

Thus, if there is a solution to $x^2 \equiv a \pmod{p}$, then there are exactly two incongruent solutions.

**Question 9. [p 167. #33]**

The three children in a family have feet that are 5 inches, 7 inches, and 9 inches long. When they measure the length of the dining room of their house using their feet, they each find that there are 3 inches left over. How long is the dining room?

**Solution:** Let $n$ be the length of the dining room (in inches), we solve the following simultaneous congruences using the Chinese remainder theorem:

$$n \equiv 3 \pmod{5}$$
$$n \equiv 3 \pmod{7}$$
$$n \equiv 3 \pmod{9}.$$

Here

$$a_1 = 3, \quad a_2 = 3, \quad a_3 = 3$$
$$m_1 = 5, \quad m_2 = 7, \quad m_3 = 9,$$

and

$$M_1 = 7 \cdot 9 = 63, \quad M_2 = 5 \cdot 9 = 45, \quad M_3 = 5 \cdot 7 = 35.$$

Also, solving the congruences

$$M_1 y_1 \equiv 1 \pmod{m_1}$$
$$M_2 y_2 \equiv 1 \pmod{m_2}$$
$$M_3 y_3 \equiv 1 \pmod{m_3}$$

for the inverses $y_1$, $y_2$, and $y_3$, we have

$$y_1 \equiv 2 \pmod{5}, \quad y_2 \equiv 5 \pmod{7}, \quad y_3 \equiv 8 \pmod{9},$$

and the unique solution modulo $5 \cdot 7 \cdot 9$ is given by

$$n = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 3 \cdot 63 \cdot 2 + 3 \cdot 45 \cdot 5 + 35 \cdot 9 = 378 + 675 + 945 = 1998 \equiv 3 \pmod{315}.$$

Therefore a reasonable answer would be $n = 3 + 315 = 318$ inches, or 26 feet, 6 inches.

**Question 10. [p 221. #12]**

Using Fermat’s little theorem, find the least positive residue of $2^{1000000}$ modulo 17.

**Solution:** Since $p = 17$ is prime and $17 \nmid 2$, then by Fermat’s little theorem, $2^{16} \equiv 1 \pmod{17}$. 
Now, $1000000 = 2^{19} + 2^{18} + 2^{17} + 2^{16} + 2^{14} + 2^9 + 2^6$, so that
\[ 2^{1000000} = 2^{219} \cdot 2^{218} \cdot 2^{217} \cdot 2^{216} \cdot 2^{214} \cdot 2^9 \cdot 2^6 \]
and
\[ 2^{1000000} = (2^{2^1})^{215} \cdot (2^{2^2})^{214} \cdot (2^{2^4})^{213} \cdot (2^{2^4})^{212} \cdot (2^{2^4})^{210} \cdot (2^{2^4})^{27} \cdot (2^{2^4})^{2^2} \]
so that $2^{1000000} \equiv 1 \pmod{17}$. 