1. Find an inverse modulo 17 to each of the following integers:

   (a) 4 (b) 5 (c) 7 (d) 16

   (a) We can do this using trial-and-error or the Euclidean algorithm. We begin by noting that we want to find $x, y \in \mathbb{Z}$ so that $4x - 1 = 17y$, i.e. $4x - 17y = 1$. Trial-and-error for y yields

y	0	1	2	3
$1 + 17y$	1	18	35	52

   and since we see that $52 = 4 \cdot 13$, we have $4 \cdot 13 - 17 \cdot 3 = 1$, so $4 \cdot 13 \equiv 1 \mod 17$. Hence, 13 is an inverse to 4 mod 17.

   (b) We can use the same trial-and-error table as above to note that $5 \cdot 7 = 1 + 2 \cdot 17$, so $5 \cdot 7 \equiv 1 \mod 17$ and hence, 7 is an inverse to 5 mod 17.

   (c) Since 7 is an inverse to 5 mod 17, it must be the case that 7 is an inverse to 5 mod 17.

   (d) Note that $16 \equiv -1 \mod 17$. -1 is its own inverse mod 17 since $(-1) \cdot (-1) \equiv 1 \mod 17$. Hence, $16 \cdot 16 \equiv 1 \mod 17$ and so 16 is its own inverse mod 17.

2. Which integers leave a remainder of 1 when divided by both 2 and 3?

   x has a remainder of 1 when divided by 2 and 3 if and only if $x \equiv 1 \mod 2$ and $x \equiv 1 \mod 3$. We see that $x = 1$ is such a number. Moreover, Sun-Tsu's theorem tells us that this is the only solution mod 6. Hence, every integer which leaves a remainder of 1 when divided by both 2 and 3 is of the form $1 + 6k$ for some $k \in \mathbb{Z}$.

3. Solve the following systems of congruences:

(a) $x \equiv 2 \mod 11$
$x \equiv 3 \mod 12$
$x \equiv 4 \mod 13$

(b) $3x \equiv 1 \mod 7$
$2x \equiv 4 \mod 9$
$5x \equiv 0 \mod 10$

(a) Here's a quick trick for this one (told to me by Izzy Harker). $2 \equiv -9 \mod 11$, $3 \equiv -9 \mod 12$, and $4 \equiv -9 \mod 13$, so we can replace our system of congruences by

$$\begin{aligned} x &\equiv -9 \mod 11 \\ x &\equiv -9 \mod 12 \\ x &\equiv -9 \mod 13 \end{aligned}$$

We see that $x = -9$ is such and number and since $11, 12$, and 13 are pairwise relatively prime, Sun-Tsu's Theorem implies that the solutions all have the form $x \equiv -9 \mod 11 \cdot 12 \cdot 13$.

If you wish to do this using the proof of Sun-Tsu's theorem, we can set $M = 11 \cdot 12 \cdot 13$, $L_1 = 12 \cdot 13 = 156$, $L_2 = 11 \cdot 13 = 143$, and $L_3 = 11 \cdot 12 = 132$. We wish to solve the congruences

$$\begin{aligned} 156y_1 &\equiv 1 \mod 11 \\ 143y_2 &\equiv 1 \mod 12 \\ 132y_3 &\equiv 1 \mod 13 \end{aligned}$$

Reducing the coefficients yields the more manageable

$$\begin{aligned} 2y_1 &\equiv 1 \mod 11 \\ 11y_2 &\equiv 1 \mod 12 \\ 2y_3 &\equiv 1 \mod 13 \end{aligned}$$

and we can quickly see that we can take $y_1 = 6$, $y_2 = 11$, and $y_3 = 7$. The proof of Sun-Tsu's Theorem now tells us that every solution to our original system of congruences is congruent to

$$a_1L_1y_1 + a_2L_2y_2 + a_3L_3y_3 = 2 \cdot 156 \cdot 6 + 3 \cdot 143 \cdot 11 + 4 \cdot 132 \cdot 7 = 10287$$

modulo $11 \cdot 12 \cdot 13$. A quick computation confirms that $-9 \equiv 10287 \mod 11 \cdot 12 \cdot 13$

(b) We first convert our system of linear congruences into something Sun-Tsu's Theorem is better able to handle. Note that $3 \cdot 5 \equiv 1 \mod 7$, so $3x \equiv 1 \mod 7$ if and only if $x \equiv 5 \mod 7$. Likewise, $2 \cdot 5 \equiv 1 \mod 9$, so $2x \equiv 4 \mod 9$ if and only if $x \equiv 20 \equiv 2 \mod 9$. The last congruence is a bit trickier to handle. Note, however, that since $(5, 10) = 5$, we can "divide" both sides of the congruence by 5 to find that $5x \equiv 0 \mod 10$ if and only if $x \equiv 0 \mod 2$. Our system of linear congruences then becomes

$$\begin{aligned} x &\equiv 5 \mod 7 \\ x &\equiv 2 \mod 9 \\ x &\equiv 0 \mod 2 \end{aligned}$$

Using the notation from Sun-Tsu's theorem, we have $m_1 = 7$, $m_2 = 9$, $m_3 = 2$, $L_1 = 9 \cdot 2 = 18$, $L_2 = 7 \cdot 2 = 14$, $L_3 = 7 \cdot 9 = 63$. We want to find $y_1, y_2, y_3 \in \mathbb{Z}$ satisfying

$$\begin{aligned} 18y_1 &\equiv 1 \mod 7 \\ 14y_2 &\equiv 1 \mod 9 \\ 63y_3 &\equiv 1 \mod 2 \end{aligned}$$

and reducing the coefficients yields

$$\begin{aligned} 4y_1 &\equiv 1 \mod 7 \\ 5y_2 &\equiv 1 \mod 9 \\ y_3 &\equiv 1 \mod 2 \end{aligned}$$

Hence, we can take $y_1 = 2$, $y_2 = 2$, $y_3 = 1$. We finally find that every solution to our original set of congruences is equivalent to

$$5 \cdot 18 \cdot 2 + 2 \cdot 14 \cdot 2 + 0 \cdot 63 \cdot 1 = 236$$

modulo $2 \cdot 7 \cdot 9 = 126$.

4. Show that the system of congruences

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \end{aligned}$$

has a solution if and only if $(m_1, m_2) \mid (a_1 - a_2)$. Show that when there is a solution, it is unique modulo $\text{lcm}(m_1, m_2)$

Suppose first that there exists $x \in \mathbb{Z}$ satisfying $x \equiv a_1 \mod m_1$ and $x \equiv a_2 \mod m_2$. Then there exist $y_1, y_2 \in \mathbb{Z}$ so that $x - a_1 = m_1 y_1$ and $x - a_2 = m_2 y_2$. Subtracting these equations yields $a_1 - a_2 = m_1 y_1 - m_2 y_2$. Since $(m_1, m_2) \mid (m_1 y_1 - m_2 y_2)$, we have $(m_1, m_2) \mid a_1 - a_2$.

Conversely, suppose that $(m_1, m_2) \mid a_1 - a_2$. Then there exist integers $y_1, y_2 \in \mathbb{Z}$ so that $m_1 y_1 + m_2 y_2 = a_1 - a_2$. Then $a_1 + m_1 y_1 = a_2 + m_2 y_2$. Set $x = a_1 + m_1 y_1 = a_2 + m_2 y_2$. Since $x = a_1 + m_1 y_1$, $x \equiv a_1 \mod m_1$. Also, since $x = a_2 + m_2 y_2$, $x \equiv a_2 \mod m_2$. Therefore, the system of congruences has a solution.

For the final part of the solution, suppose that $x, y \in \mathbb{Z}$ are both congruent to $a_1 \mod m_1$ and congruent to $a_2 \mod m_2$. Then $x \equiv y \mod m_1$ and $x \equiv y \mod m_2$, i.e. $m_1 \mid x - y$ and $m_2 \mid x - y$. Since $\frac{m_1}{(m_1, m_2)} \mid m_1$, we conclude that $\frac{m_1}{(m_1, m_2)} \mid x - y$. However, $\frac{m_1}{(m_1, m_2)}$ and m_2 are relatively prime and they both divide $x - y$. Therefore, their product $\frac{m_1 m_2}{(m_1, m_2)} = \text{lcm}(m_1, m_2)$ also divides $x - y$, i.e. $x \equiv y \mod \text{lcm}(m_1, m_2)$. Therefore, the solutions to this system of congruences are unique modulo $\text{lcm}(m_1, m_2)$.

5. Use the previous problem to solve the system of congruences

$$x \equiv 4 \mod 6$$
$$x \equiv 13 \mod 15$$

6. Show that there are arbitrarily long strings of consecutive integers each divisible by a perfect square greater than 1.
Hint: Use Sun-Tsu's Theorem on an appropriate system of congruences.

We show that for every $k \in \mathbb{N}$, there is a string of k consecutive integers each of which is divisible by a perfect square greater than 1. Let p_n denote the nth prime (starting with $p_1 = 2$) and consider the system of linear congruences

$$\begin{aligned} x &\equiv -1 \mod 4 \\ x &\equiv -2 \mod 9 \\ x &\equiv -3 \mod 25 \\ &\vdots \\ x &\equiv -k \mod p_k^2 \end{aligned}$$

Since the moduli are pairwise relatively prime, Sun-Tsu's Theorem guarantees that there is a solution to this system of congruences. This implies, however, that $x+1$ is divisible by 2^2, $x+2$ is divisible by 3^2, $x+3$ is divisible by 5^2, etc. until $x+k$ is divisible by p_k^2. But now we have that $x+1, x+2, \ldots, x+k$ is a list of k consecutive integers, each of which is divisible by a square greater than 1.