1. *Find all solutions to the following system of linear congruences:*

$$\begin{aligned} x &\equiv 0 \mod 2 \\ x &\equiv 0 \mod 3 \\ x &\equiv 1 \mod 5 \\ x &\equiv 6 \mod 7 \end{aligned}$$

Approach 1.

Begin by observing that $x = 6$ satisfies each of the above congruences. Since $2, 3, 5$, and 7 are pairwise relatively prime, Sun-Tsu's theorem indicates that this solution is unique modulo $2 \cdot 3 \cdot 5 \cdot 7 = 210$. Hence, every solution to this system of congruences is congruent to 6 modulo 210. Moreover, if $y \equiv 6 \mod 210$, then y satisfies all of the above congruences by problem 3 on homework 6. Therefore, every solution to the above system of congruences lies in the set $\{6 + 210k : k \in \mathbb{Z}\}$.

Approach 2.

Let $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, and $m_4 = 7$. Then let $a_1 = 0$, $a_2 = 0$, $a_3 = 1$, and $a_4 = 6$. Define $M := \prod_{i=1}^{4} m_i = 210$ and $M_i := \frac{M}{m_i}$. We use the proof of Sun-Tsu's theorem to find a solution to the above system of congruences. For each $1 \leqslant i \leqslant 4$, we solve the congruence $M_i y_i \equiv 1 \mod m_i$:

$$\begin{aligned} 105 \cdot 1 &\equiv 1 \mod 2 \\ 70 \cdot 1 &\equiv 1 \mod 3 \\ 42 \cdot 3 &\equiv 1 \mod 5 \\ 30 \cdot 4 &\equiv 1 \mod 7 \end{aligned}$$

Then the proof of Sun-Tsu's theorem indicates that $x = \sum_{i=1}^{4} a_i M_i y_i = 846$ is the unique solution (modulo 210) to the system of congruences. Moreover, if $y \equiv 6 \mod 210$, then y satisfies all of the above congruences by problem 3 on homework 6. Therefore, every solution to the above system of congruences lies in the set $\{846 + 210k : k \in \mathbb{Z}\}$.

2. *Find all solutions of the congruence* $x^2 + 6x - 31 \equiv 0 \mod 72$.

Suppose first that $x \in \mathbb{Z}$ satisfies $x^2 + 6x - 31 \equiv 0 \mod 72$. Then by problem 3 on homework 6, x also satisfies $x^2 + 6x - 31 \equiv 0 \mod 8$ and $x^2 + 6x - 31 \equiv 0 \mod 9$. To simplify computations and notation, define $f, g : \mathbb{Z} \to \mathbb{Z}$ so that $f(y)$ is the least nonnegative residue of $y^2 + 6y - 31$ modulo 8 and $g(y)$ is the least nonnegative residue of $y^2 + 6y - 31$ modulo 9. We have the following tables of values for f and g

y	0	1	2	3	4	5	6	7	8
$f(y)$	1	0	1	4	1	0	1	4	
$g(y)$	5	3	3	5	0	6	5	6	0

Since x satisfies $f(x) \equiv 0 \mod 8$ and $g(x) \equiv 0 \mod 9$, we see now that we must have $x \equiv 1 \mod 8$ or $x \equiv 5 \mod 8$. Additionally, we must have $x \equiv 4 \mod 9$ or $x \equiv 8 \mod 9$.

If $x \equiv 1 \mod 8$ and $x \equiv 4 \mod 9$, then Sun-Tsu's theorem indicates that x must be congruent to 49 modulo 72. Moreover, a quick computation verfies that $49^2 + 6 \cdot 49 - 31 \equiv 0 \mod 72$, so $x \equiv 49 \mod 72$ gives a solution.

If $x \equiv 1 \mod 8$ and $x \equiv 8 \mod 9$, then Sun-Tsu's theorem indicates that x must be congruent to 17 modulo 72. Again, a quick computation verifies that $17^2 + 6 \cdot 17 - 31 \equiv 0 \mod 72$, so $x \equiv 17 \mod 72$ gives another solution.

If $x \equiv 5 \mod 8$ and $x \equiv 4 \mod 9$, then Sun-Tsu's theorem indicates that x must be congruent to 13 modulo 72. Yet again, $13^2 + 6 \cdot 13 - 31 \equiv 0 \mod 72$ and so $x \equiv 13 \mod 72$ gives a third solution.

The only remaining possibility for x is that $x \equiv 5 \mod 8$ and $x \equiv 8 \mod 9$. In this case, Sun-Tsu's theorem indicates that x must be congruent to 53 modulo 72. One final check yields $53^2 + 6 \cdot 53 - 31 \equiv 0 \mod 72$ for a fourth and final solution, namely $x \equiv 53 \mod 72$.

3. *Show that if $a, b, c \in \mathbb{Z}$ and $(a, b) = 1$, then there exists an integer $n \in \mathbb{Z}$ so that $(an + b, c) = 1$*

Proof 1.

Case 1: Every prime factor of c divides b.

In this case, take $n = 1$. Let p be a prime factor of c. Then since $p \mid b$ and $p \nmid a$ (since $(a, b) = 1$), $p \nmid a + b$. Hence, $a + b$ and c share no common prime factors, i.e. $(a + b, c) = 1$.

Case 2: Some prime factor(s) of c do not divide b.

In this case, take

$$n = \prod_{\substack{p \mid c \\ p \text{ prime} \\ p \nmid b}} p$$

Now let q be a prime factor of c. If $q \mid b$, then $q \nmid n$ and $q \nmid a$, so $q \nmid an$ implying that $q \nmid an + b$. If $q \nmid b$, then $q \mid n$, so $q \mid an$ and hence, $q \nmid an + b$. Hence, $an + b$ and c share no common prime factors, i.e. $(an + b, c) = 1$.

Proof 2.

Since $(a, b) = 1$, the set of numbers $\{an + b : n \in \mathbb{N}\}$ forms an arithmetic progression with infinitely many primes by Dirichlet's Theorem. Hence, there exists a prime $p = an+b$ with $p > c$, so $(an+b, c) = (p, c) = 1$.