**1)** [25 points] Compute the remainder of $2^{5353}$ when divided by 11. [Show work, including computations!]

*Solution.* We have:

$$\begin{aligned} 5353 &= 11 \cdot 486 + 7 \\ 486 &= 11 \cdot 44 + 2 \\ 44 &= 11 \cdot 4 + 0 \\ 4 &= 11 \cdot 0 + 4. \end{aligned}$$

So, $5353 = 7 + 2 \cdot 11 + 0 \cdot 11^2 + 4 \cdot 11^3$. Then, by *Fermat's Theorem*:

$$2^{5353} = 2^{7+2\cdot 11+0\cdot 11^2+4\cdot 11^3} \equiv 2^{7+2+0+4} = 2^{13} = 2^{2+1\cdot 11} \equiv 2^{2+1} = 8 \pmod{11}.$$

So, the remainder is 8. $\square$

*Alternative Solution.* Since if $p \nmid a$, where $p$ is prime, we have that $a^{p-1} \equiv 1 \pmod{p}$, then with $p = 11$ and $a = 2$ we get that $2^{10} \equiv 1 \pmod{11}$. Then:

$$2^{5353} = 2^{535\cdot 10+3} = \left(2^{10}\right)^{535} \cdot 2^3 \equiv 1^{535} \cdot 8 = 8 \pmod{11}.$$

Hence, the remainder is 8. $\square$

**2)** [25 points] Find all integers $x$ such that

$$3x \equiv 7 \pmod{10}$$
$$2x \equiv 4 \pmod{14}.$$

[If there is no such integer, explain how you could tell. *You need to show work!* Guessing solutions doesn't yield *any* credit.]

*Solution.* Start with the second equation. Since $\gcd(2, 14) = 2$, and $2 \mid 4$, we can divide the second equation [including the modulus] by 2 and get

$$x \equiv 2 \pmod{7}.$$

So, $x = 7k + 2$, for $k \in \mathbb{Z}$.

Substituting in the first, we get $3(7k + 2) \equiv 7 \pmod{10}$, so $21k \equiv 1 \pmod{10}$, or $k \equiv 1 \pmod{10}$.

Hence, $k = 10l + 1$, and so $x = 7 \cdot (10l + 1) + 2 = 70l + 9$, for $l \in \mathbb{Z}$.

*Alternative solution:* Since $7 \cdot 3 + (-2) \cdot 10 = 1$ [so $7 \cdot 3 \equiv 1 \pmod{10}$], we have that the first equation gives that $x \equiv 7 \cdot 7 = 49 \equiv 9 \pmod{10}$. So, $x = 10k + 9$, for some $k \in \mathbb{Z}$. [One could also use $x = 10k - 1$, since $9 \equiv -1 \pmod{10}$.]

Substituting in the second equation, we get: $2 \cdot (10k + 9) \equiv 4 \pmod{14}$, so $20k \equiv -14 \pmod{14}$, so $6k \equiv 0 \pmod{14}$. [With $x = 10k - 1$, we get $6k \equiv 6 \pmod{14}$.]

Now, $\gcd(6, 14) = 2$ and $2 \mid 0$ [or $2 \mid 6$], so we do have a solution. Dividing through out [including modulus] by 2, we get $3k \equiv 0 \pmod{7}$ [or $3k \equiv 3 \pmod{7}$]. Now $5 \cdot 3 + (-2) \cdot 7 = 1$ [i.e., $5 \cdot 3 \equiv 1 \pmod{7}$], so multiplying by 5, we get $k \equiv 0 \pmod{7}$ [or $k \equiv 15 \equiv 1 \pmod{7}$]. So, $k = 7l$ for $l \in \mathbb{Z}$ [or $k = 7l + 1$].

Substituting back, we get $x = 10 \cdot 7l + 9 = 70l + 9$, for $l \in \mathbb{Z}$ [or $x = 10 \cdot (7l + 1) - 1 = 70l + 9$ again]. $\square$

**3)** [25 points] Prove that there are no integers $x$, $y$, $z$ such that $x^2 + y^2 + z^2 = 999$.

[**Note:** This was a HW problem. *You need to show work!*]

*Proof.* Assume that are such integers $x$, $y$, and $z$. We then consider the equation modulo 8:

$$x^2 + y^2 + z^2 \equiv 999 \equiv 7 \pmod{8}.$$

But all squares modulo 8 are congruent to either 0, 1, or 4 [as seen in the book and class]. If none of $x^2$, $y^2$, and $z^2$ is 4 modulo 8, then the sum is at most 3 and so cannot be 7 modulo 8.

So, assume, without loss of generality, the $z^2 \equiv 4 \pmod{8}$. Then, we have:

$$x^2 + y^2 \equiv 3 \pmod{8}.$$

Again, if neither $x^2$ nor $y^2$ is 4 modulo 8, the sum is less than or equal to 2, so, again, one of them must be 4.

Assume then, without loss of generality, that $y^2 \equiv 4 \pmod{8}$. Then,

$$x^2 \equiv -1 \equiv 7 \pmod{8},$$

but that is impossible, as observed above. $\square$

**4)** [25 points] Prove that if $a, b \in \mathbb{Z}_{\geq 2}$ are such that both $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are *squares*, then both $a$ and $b$ must also be squares.

[**Hint:** In your HW you've proved that if $c \in \mathbb{Z}_{\geq 2}$ and its factorization into primes is $c = p_1^{g_1} \cdots p_k^{g_k}$, then $c$ is a square if and only if all $g_i$'s are *even*. You can use this here without proving it.]

*Proof.* Let $a = p_1^{e_1} \cdots p_k^{e_k}$, $b = p_1^{f_1} \cdots p_k^{f_k}$, with $p_i$'s distinct primes and $e_i, f_i \geq 0$.

Then, $\gcd(a, b) = p_1^{m_1} \cdots p_k^{m_k}$ and $\operatorname{lcm}(a, b) = p_1^{M_1} \cdots p_k^{M_k}$ where $m_i = \min\{e_i, f_i\}$ and $M_i = \max\{e_i, f_i\}$. Since both $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are squares, we have that $m_i$ and $M_i$ are both even.

Now, if $e_i \leq f_i$, then $e_i = m_i$ and $f_i = M_i$, and so both $e_i$ and $f_i$ are even.

If $e_i > f_i$, then $e_i = M_i$ and $f_i = m_i$, and so both $e_i$ and $f_i$ are, again, even.

Thus, we always have that both $e_i$ and $f_i$ are even [for all $i$]. Thus, both $a$ and $b$ are squares. $\square$