1) [20 points] Find all integers x such that

$$5x \equiv 3 \pmod 6$$
$$3x \equiv 1 \pmod{10}.$$

[If there is no such integer, explain how you could tell.]

Solution. Since $5 \equiv -1 \pmod 6$, the first equation gives us that $x \equiv -3 \equiv 3 \pmod 6$ So, $x = 6k + 3$ for some $k \in \mathbb{Z}$.

Substituting in the second equation, we get $3(6k+3) \equiv 1 \pmod{10}$, i.e., $18k \equiv -8 \pmod{10}$, or $8k \equiv 2 \pmod{10}$. Since $(8, 10) = 2 \mid 2$, we get $4k \equiv 1 \pmod 5$. Since $4 \equiv -1 \pmod 5$, we have $k \equiv -1 \equiv 4 \pmod 5$, i.e., $k = 5l + 4$ for $l \in \mathbb{Z}$.

So, [all] the solutions are $x = 6(5l + 4) + 3 = 30l + 27$, for $l \in \mathbb{Z}$. □

2) [20 points] Let

$$n = 604239 \cdot (450027)^{6695} + 7082819$$

Find its residue modulo 11 [i.e., the remainder when n is divided by 11].

[**Hint:** Remember that if the [decimal] digits are given by $a = d_k d_{k-1} \cdots d_0$, then $a \equiv d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^{k-1} d_k + (-1)^k d_k \pmod{11}$.]

Solution. We have:

$$604239 \equiv 9 - 3 + 2 - 4 + 0 - 6 = -2 \pmod{11}$$
$$450027 \equiv 7 - 2 + 0 - 0 + 5 - 4 = 6 \pmod{11}$$
$$7082819 \equiv 9 - 1 + 8 - 2 + 8 - 0 + 7 = 29 \equiv 9 - 2 = 7 \pmod{11}.$$

So,

$$n \equiv -2 \cdot 6^{6695} + 7 \pmod{11}.$$

Also:

$$6695 = 11 \cdot 608 + 7$$
$$608 = 11 \cdot 55 + 3$$
$$55 = 11 \cdot 5 + 0$$
$$5 = 11 \cdot 0 + 5$$

and hence $6695 = 7 + 3 \cdot 11 + 0 \cdot 11^2 + 5 \cdot 11^3$. So:

$$\begin{aligned} 6^{6695} &\equiv 6^{7+3+0+5} = 6^{15} = 6^{4+1\cdot 11} \equiv 6^{1+4} \\ &= 6^5 = 6^2 \cdot 6^2 \cdot 6 \equiv 36 \cdot 36 \cdot 6 \equiv 3 \cdot 3 \cdot 6 \equiv 54 \equiv -1 \pmod{11} \end{aligned}$$

Thus,

$$n \equiv -2 \cdot (-1) + 7 = 9 \pmod{11}.$$

□

3) [20 points] Prove that $x^2 + y^2 = 3{,}000{,}000{,}003$ has no solution with $x, y, z \in \mathbb{Z}$.

Proof. We have that x^2 and y^2 are either 0 or 1 modulo 4, so the only possibilities for $x^2 + y^2$ modulo 4 are 0, 1 and 2. But $3{,}000{,}000{,}003 \equiv 3 \pmod{4}$. So, there are no such $x, y \in \mathbb{Z}$. □

4) Congruences modulo 7:

(a) [10 points] Prove that $b \equiv 0 \pmod{7}$ if and only if $-2b \equiv 0 \pmod{7}$. [Remember that there are two parts to this: the "if" and the "only if".]

Proof. If $b \equiv 0 \pmod{7}$, then $-2b \equiv -2 \cdot 0 = 0 \pmod{7}$.

Conversely, if $-2b \equiv 0 \pmod{7}$, then $-6b \equiv 3 \cdot 0 = 0 \pmod{7}$. Since $-6 \equiv 1 \pmod{7}$, this means $b \equiv 0 \pmod{7}$.

[One could also easily do this using unique factorization.] □

(b) [10 points] Prove that if the decimal digits of a are given by $a = d_k d_{k-1} \cdots d_1 d_0$, then a is divisible by 7 if and only if $d_k d_{k-1} \cdots d_1 - 2 \cdot d_0$ is divisible by 7. [For example, this means that 1234 is divisible by 7 if and only if $123 - 2 \cdot 4 = 115$ is divisible by 7.]

[**Hint:** You can use the previous part, even if you could not do it.]

Proof. We have that

$$\begin{aligned}
7 \mid a \text{ iff } & d_k d_{k-1} \cdots d_1 d_0 \equiv 0 \pmod 7 \\
\text{iff } & d_k d_{k-1} \cdots d_1 \cdot 10 + d_0 \equiv 0 \pmod 7 \\
\text{iff } & d_k d_{k-1} \cdots d_1 \cdot 3 + d_0 \equiv 0 \pmod 7 \\
\text{iff } & [\text{using part (a)}]\ d_k d_{k-1} \cdots d_1 \cdot (-6) + -2d_0 \equiv 0 \pmod 7 \\
\text{iff } & d_k d_{k-1} \cdots d_1 + -2d_0 \equiv 0 \pmod 7 \\
\text{iff } & 7 \mid (d_k d_{k-1} \cdots d_1 + -2d_0).
\end{aligned}$$

□

5) [20 points] Prove that if $a, b, n \in \mathbb{Z}_{>0}$ and $a^n \mid b^n$, then $a \mid b$.
[**Hint:** This would have been much harder in the last exam.]

Proof. We use Lemma 1.54 from the book. Write

$$\begin{aligned}
a &= p_1^{e_1} \cdots p_k^{e_k} \\
b &= p_1^{f_1} \cdots p_k^{f_k},
\end{aligned}$$

where p_i's are distinct primes and $e_i, f_i \in \mathbb{Z}_{\geq 0}$. [We've sen in class that we can do this.] Then,

$$\begin{aligned}
a^n &= p_1^{n \cdot e_1} \cdots p_k^{n \cdot e_k} \\
b^n &= p_1^{n \cdot f_1} \cdots p_k^{n \cdot f_k},
\end{aligned}$$

and since $a^n \mid b^n$, we must have that $n \cdot e_i \leq n \cdot f_i$ for all $i \in \{1, \ldots, k\}$. But this means that $e_i \leq f_i$ for all $i \in \{1, \ldots, k\}$, and hence $a \mid b$. □