5. Modular Arithmetic.

a) Let a and $m > 1$ be natural numbers with a common divisor $d > 1$. Prove that the congruence equation $ax \equiv 1 \pmod m$ does not have a solution.

Let $a \in \mathbb{N}$, $m \in \mathbb{N}$. $m > 1$. Let common divisor of a, m, which is d, $d > 1$.
WTP: $ax \equiv 1 \pmod m$. does not have a solution.
I'll use prove by contradiction. Assume $ax \equiv 1 \pmod m$ has a solution.
From the definition. gives. $m \mid (ax-1)$, which $\exists k \in \mathbb{Z}$. s.t. $ax - 1 = m \cdot k$.
Since d is the common divisor of a, m, gives $d \mid a \wedge d \mid m$, which $\exists k_1, k_2 \in \mathbb{Z}$. s.t. $a = d \cdot k_1$. $m = d \cdot k_2$.
Since $ax - 1 = m \cdot k$, gives $d \cdot k_1 x - 1 = d \cdot k_2 \cdot k$, which. $d(k_1 x - k_2 \cdot k) = 1$.
Since $k_1, x, k_2, k \in \mathbb{Z}$, take $k' \in \mathbb{Z}$, $k' = k_1 x - k_2 \cdot k$, which $d \cdot k' = 1$, gives $d \mid 1$
However, since $d > 1$. contradicts to $d \mid 1$.
Therefore. $ax \equiv 1 \pmod m$ does not have a solution.

∎

b) First solve the equation $x^2 = x$ for integers, then solve $x^2 \equiv x \pmod 5$ and $x^2 \equiv x \pmod 6$.

① Since $x \in \mathbb{Z}$. the solution to $x^2 = x$ is $x = 1$.

② $x^2 \equiv x \pmod 5$ gives. $x^2 - x \equiv 0 \pmod 5$. gives.
$x(x-1) \equiv 0 \pmod 5$
According to the Euclid Lemma, since 5 is a prime,
$5 \mid x$ or $5 \mid (x-1)$.
(1) $5 \mid x$. gives $x \equiv 0 \pmod 5$.
(2) $5 \mid x-1$. gives $x \equiv 1 \pmod 5$.

③ Considering $x^2 \equiv x \pmod 2$. gives $x(x-1) \equiv 0 \pmod 2$. which $2 \mid x$ or $2 \mid (x-1)$.
(1) $2 \mid x$. gives $x \equiv 0 \pmod 2$.
(2) $2 \mid (x-1)$ gives $x \equiv 1 \pmod 2$.

Considering $x^2 \equiv x \pmod 3$, gives $x(x-1) \equiv 0 \pmod 3$. which $3 \mid x$ or $3 \mid (x-1)$.
(1) $3 \mid x$. gives $x \equiv 0 \pmod 3$. (2) $3 \mid (x-1)$, gives $x \equiv 1 \pmod 3$.
When I. $x \equiv 0 \pmod 2$; $x \equiv 0 \pmod 3$, gives, $\exists k_1, l_1 \in \mathbb{Z}$. s.t. $x = 2k_1$; $x = 3l_1$, gives.
$\begin{cases} 3x = 6k_1 \\ 2x = 6l_1 \end{cases} \Rightarrow 5x = 6(k_1 + l_1) \Rightarrow 5x = 0 \pmod 5). \Rightarrow x = 0 \pmod 5$.
When II. $x \equiv 0 \pmod 2$; $x \equiv 1 \pmod 3$. gives $\exists k_2, l_2 \in \mathbb{Z}$. s.t. $x = 2k_2$; $x - 1 = 3l_2$. $(x = 3l_2 + 1)$. gives.
$\begin{cases} 3x = 6k_2 \\ 2x = 6l_2 + 2 \end{cases} \Rightarrow 5x = 6(k_2 + l_2) + 2 \Rightarrow 5x \equiv 2 \pmod 6 \Rightarrow 5x \equiv 20 \pmod 6 \Rightarrow 5 \cdot (5^{-1}) x \equiv 20 \cdot (5^{-1}) \pmod 6$
$\Rightarrow x \equiv 4 \pmod 6$.
When III. $x \equiv 1 \pmod 2$; $x \equiv 0 \pmod 3$. gives $\exists k_3, l_3 \in \mathbb{Z}$. s.t. $x - 1 = 2k_3$ $(x = 2k_3 + 1)$; $x = 3l_3$. gives.
$\begin{cases} 3x = 6k_3 + 3 \\ 2x = 6l_3 \end{cases} \Rightarrow 5x = 6(k_3 + l_3) + 3 \Rightarrow 5x \equiv 3 \pmod 6. \Rightarrow 5x \equiv 15 \pmod 6. \Rightarrow 5 \cdot (5^{-1}) x \equiv 15 \cdot (5^{-1}) \pmod 6$
$\Rightarrow x \equiv 3 \pmod 6$.
When IV. $x \equiv 1 \pmod 2$; $x \equiv 1 \pmod 3$. gives. $\exists k_4, l_4 \in \mathbb{Z}$. s.t. $x - 1 = 2k_4$ $(x = 2k_4 + 1)$; $x - 1 = 3l_4$ $(x = 3l_4 + 1)$; gives.
$\begin{cases} 3x = 6k_4 + 3 \\ 2x = 6l_4 + 2 \end{cases} \Rightarrow 5x = 6(k_4 + l_4) + 5 \Rightarrow 5x \equiv 5 \pmod 6. \Rightarrow 5x \equiv 35 \pmod 6$.
$\Rightarrow 5 \cdot (5^{-1}) x \equiv 35 \cdot (5^{-1}) \pmod 6$.
$\Rightarrow x \equiv 7 \pmod 6. \Rightarrow x \equiv 1 \pmod 6$.
Therefore $x \equiv 0 \pmod 6$, $x \equiv 1 \pmod 6$, $x \equiv 3 \pmod 6$, $x \equiv 4 \pmod 6$.

c) Assume a prime number p is of the form $n^2 + 5$ for some natural number n. Prove that the last digit of p must be 1 or 9.

Let p is a prime number and $p = n^2 + 5$. for $n \in \mathbb{N}$.
WTP: $p \equiv 1 \pmod{10}$ or $p \equiv 9 \pmod{10}$. (according to hint).
Considering $n^2 \equiv \_ \pmod{10}$
Since $n \in \mathbb{N}$. when $n = 1$. $n^2 = 1$, $n^2 \equiv 1 \pmod{10}$.
when $n = 2$. $n^2 = 4$, $n^2 \equiv 4 \pmod{10}$.
when $n = 3$. $n^2 = 9$. $n^2 \equiv 9 \pmod{10}$.
when $n = 4$. $n^2 = 16$, $n^2 \equiv 6 \pmod{10}$.
when $n = 5$. $n^2 = 25$. $n^2 \equiv 5 \pmod{10}$.
when $n = 6$. $n^2 = 36$. $n^2 \equiv 6 \pmod{10}$.
when $n = 7$. $n^2 = 49$. $n^2 \equiv 9 \pmod{10}$.
when $n = 8$. $n^2 = 64$. $n^2 \equiv 4 \pmod{10}$.
when $n = 9$. $n^2 = 81$. $n^2 \equiv 1 \pmod{10}$.
Thus n^2 can congruent to 1 or 4 or 5 or 6 or 9 mod 10.
Considering $n^2 + 5 \equiv \_ \pmod{10}$.
when $n = 1$. $n^2 + 5 \equiv 6 \pmod{10}$.
when $n = 2$. $n^2 + 5 \equiv 9 \pmod{10}$.
when $n = 3$. $n^2 + 5 \equiv 4 \pmod{10}$.
when $n = 4$. $n^2 + 5 \equiv 1 \pmod{10}$.
when $n = 5$. $n^2 + 5 \equiv 0 \pmod{10}$.
when $n = 6$. $n^2 + 5 \equiv 1 \pmod{10}$.
when $n = 7$. $n^2 + 5 \equiv 4 \pmod{10}$.
when $n = 8$. $n^2 + 5 \equiv 9 \pmod{10}$.
when $n = 9$. $n^2 + 5 \equiv 6 \pmod{10}$.

Thus, $n^2 + 5$ can congruent to 0, 1, 4, 6, 9.
Since $p = n^2 + 5$ and p is a prime number. the last digit which are 0, 2, 4, 6, 8 can't be one possible p as they are even number and have a divisor, 2. (Since $n \in \mathbb{N}$. $p = n^2 + 5$. $p \geq 6$, $p \neq 2$). Thus, when $p = n^2 + 5$ and p is a prime number, p can congruent to 1 or 9 mod 10. which means. the last digit of p must be 1 or 9.

∎

d) Suppose the rightmost digit of a natural number n is 7. Prove that there exists a prime divisor of n with the rightmost digit equal to 3 or 7. (Hint: use congruency mod 10.)

WTP. $p \mid n$ and p is a prime number s.t. $p \equiv 3 \pmod{10}$ or $p \equiv 7 \pmod{10}$.

Let the rightmost digit of a natural number n be 7, which, from hint, $n \equiv 7 \pmod{10}$.

According to the definition, $\exists k \in \mathbb{N}$, s.t. $n - 7 = 10k$, which $n = 10k + 7$.

According to the lemma that, $\forall n \in \mathbb{N}$. $n = p' \cdot q'$, where p' is a prime number.

Since $n = 10k + 7$. gives. $p' \cdot q' = 10k + 7$.

Since when $k \in \mathbb{N}$, $10k + 7$ is an odd number, as $10k$ is an even number and 7 is an odd number, give both p' and q' should be odd number otherwise, the multiplication of $p' \cdot q'$ can't be an odd number, which. $p' \equiv 1 \pmod{10}$ or $p' \equiv 3 \pmod{10}$ or $p' \equiv 5 \pmod{10}$ or $p' \equiv 7 \pmod{10}$ or $p' \equiv 9 \pmod{10}$, so as q'.

Since $n = p' \cdot q'$ and $n \equiv 7$ (mod). there are only four combinations of p' and q'. which are $p_1' \equiv 1 \pmod{10}$, $q_1' \equiv 7 \pmod{10}$; $p_2' \equiv 7 \pmod{10}$, $p_2' \equiv 1 \pmod{10}$; $p_3' \equiv 3 \pmod{10}$. $q_3' \equiv 9 \pmod{10}$; $p_4' \equiv 9 \pmod{10}$, $q_4' \equiv 3 \pmod{10}$.

According to the canonical factorization, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_n^{\alpha_n}$ where each p_i is a prime and p_i is less then p_{i+1} and each α_i is a natural number.

Since $n \equiv 7 \pmod{10}$, there always exists at least one of the combination of describing above (1×7 or 3×9), i.e. if there is a $p_i^{\alpha_i} \equiv 1 \pmod{10}$. there is a $p_j^{\alpha_j} \equiv 7 \pmod{10}$, so does for 3×9), in order to get $n \equiv 7 \pmod{10}$.

Therefore. there exists a prime divisor of n with rightmost digit equal to 3 or 7. ∎