Problem 1. Find integers $a, b, c > 1$ satisfying the system of equations: $a \cdot c = 647701$, $b \cdot c = 690497$. Describe the method used.

Solution. We have: $a \cdot c = 647701$, $b \cdot c = 690497$, then $c$ is a common divisor of 647701 and 690497, so let it be the greatest common divisor.

To find $\text{gcd}(647701, 690497)$, we run the Euclidean Algorithm on input $a = 690497$ and $b = 647701$. The steps are as follows:

\[
\begin{align*}
690497 &= 647701 \cdot 1 + 42796 \quad \rightarrow q_1 = 1, \quad r_1 = 42796 \\
647701 &= 42796 \cdot 15 + 5761 \quad \rightarrow q_2 = 15, \quad r_2 = 5761 \\
42796 &= 5761 \cdot 7 + 2469 \quad \rightarrow q_3 = 7, \quad r_3 = 2469 \\
5761 &= 2469 \cdot 2 + 823 \quad \rightarrow q_4 = 2, \quad r_4 = 823 \\
2469 &= 823 \cdot 3 + 0 \quad \rightarrow q_5 = 3, \quad r_5 = 0
\end{align*}
\]

Since $r_5 = 0$, $\text{gcd}(690497, 647701) = r_4 = 823$. Hence, $c = \text{gcd}(690497, 647701) = 823$, $a = 647701/823 = 787$ and $b = 690497/823 = 839$
Problem 2. The Extended Euclidean Algorithm expresses \( \gcd(a,b) \) as \( d = as - bt \). Can these \( s, t \) be both odd? Both even? Explain.

Solution. \( s \) and \( t \) can be both odd. Proof of existence: \( \gcd(3,2) = 1 \) and running EEA on inputs \( a = 3 \) and \( b = 2 \) gives the linear combination \( 3 \cdot 1 - 2 \cdot 1 = 1 \) where \( s = 1 \) and \( t = 1 \) which are both odd.

However, \( s \) and \( t \) cannot be both even. Assume, for the sake of contradiction, that \( s \) and \( t \) are even, then we can express \( s = 2s' \) and \( t = 2t' \) for some integers \( s', t' \). This means that \( \gcd(s, t) > 1 \) as it is at least 2, which contradicts Theorem 4.3 (iii) which says \( \gcd(s, t) = 1 \).
Problem 3. Is the pair of congruences $x \equiv a \pmod{30}, \ x \equiv b \pmod{35}$ solvable for every $a, b$? Explain.

Solution. Observe that the prime factorisation of 30 is $2 \cdot 3 \cdot 5 = 30$. Therefore, by CRT, the congruence $x \equiv a \pmod{30}$ can be expressed as the following system:

$$
\begin{align*}
x & \equiv a \pmod{2} \\
x & \equiv a \pmod{3} \\
x & \equiv a \pmod{5}
\end{align*}
$$

Similarly, we can express $b \equiv a \pmod{35}$ as:

$$
\begin{align*}
x & \equiv b \pmod{5} \\
x & \equiv b \pmod{7}
\end{align*}
$$

This means that if the given system is solvable, then it must be the case that $a \equiv b \pmod{5}$ (by CRT), or simply $5 | (a - b)$.

Hence, the system is **not** solvable for every arbitrary $a$ and $b$, **unless** $5 | (a - b)$.
Problem 4. Describe a polynomial time algorithm to decide for prime $p$ and integers $a \in [0,p)$ if the equation $(x^2 \pmod{p}) = a$ has solution. Explain fully.

Solution. Observe that asking whether the equation $(x^2 \pmod{p}) = a$ has a solution is equivalent to asking whether $a \in (\mathbb{Z}_p^*)^2$. By Euler’s Criterion, if $a \in (\mathbb{Z}_p^*)^2$, then $a^{(p-1)/2} = 1$ and if $a \notin (\mathbb{Z}_p^*)^2$, then $a^{(p-1)/2} = -1$.

Thus, we can design an algorithm as follow: calculate $a^{(p-1)/2}$ in $\mathbb{Z}_p$ then check if the result equals to $-1$; if not, return a yes answer; else, return a no answer. By section 3.4, evaluating some $a^e$ in $\mathbb{Z}_n$ for any integer $n$ takes time $O(||e|| \cdot ||n||^2)$. In our case, evaluating $a^{(p-1)/2}$ in $\mathbb{Z}_p$ takes time $O(||(p-1)/2|| \cdot ||p||^2) \sim O(||p||^2)$ which is polynomial time.