1. Find the smallest positive integer $x$ satisfying the following system of congruences, should such a solution exist.

$$
x \equiv 0 \mod 3 \\
x \equiv 1 \mod 5 \\
x \equiv 2 \mod 8
$$

2. Find the smallest positive integer $x$ satisfying the following system of congruences, should such a solution exist.

$$
x \equiv 3 \mod 4 \\
x \equiv 6 \mod 12
$$

3. Find the smallest positive integer $x$ satisfying the following system of congruences, should such a solution exist.

$$
x \equiv 4 \mod 9 \\
x \equiv 10 \mod 12
$$

4. Users $A, B, C, D,$ and $E$ are friends of $S$. They have public keys $(e_A, n_A) = (5, 62857), (e_B, n_B) = (5, 64541), (e_C, n_C) = (5, 69799), (e_D, n_D) = (5, 89179),$ and $(e_E, n_E) = (5, 82583)$. You know that $S$ sends the same message to all of them and you observe the ciphertexts $c_A = 11529, c_B = 60248, c_C = 27504, c_D = 43997,$ and $c_E = 44926$. What was the message?

**Theorem 1 (Chinese Remainder Theorem)**

Let $r_1, \ldots, r_k \in \mathbb{Z}$ and let $0 \neq n_1, \ldots, n_k \in \mathbb{N}$ such that the $n_i$ are pairwise coprime. The system of equivalences

$$
X \equiv r_1 \mod n_1, \\
X \equiv r_2 \mod n_2, \\
\vdots \\
X \equiv r_k \mod n_k,
$$

has a solution $X$ which is unique up to multiples of $N = n_1 \cdot n_2 \cdots n_k$. The set of all solutions is given by $\{X + aN | a \in \mathbb{Z}\} = X + N\mathbb{Z}$.

If the $n_i$ are not all coprime the system might not have a solution at all. E.g. the system $X \equiv 1 \mod 8$ and $X \equiv 2 \mod 6$ does not have a solution since the first congruence implies that $X$ is odd while the second one implies that $X$ is even. If the system has a solution then it is unique only modulo lcm($n_1, n_2, \ldots, n_k$). E.g. the system $X \equiv 4 \mod 8$ and $X \equiv 2 \mod 6$ has solutions and the solutions are unique modulo 24. Replace $X \equiv 2 \mod 6$ by $X \equiv 2 \mod 3$; the system still carries the same information and we obtain $X = 8a + 4 \equiv 2a + 1 \equiv 2 \mod 3$, thus $a \equiv 2 \mod 3$ and $X = 8(3b + 2) + 4 = 24b + 20$. The smallest positive solution is thus 20.
We now present a constructive algorithm to find this solution, making heavy use of the extended Euclidean algorithm presented in the previous section. Since all \( n_i \) are coprime, we have \( \gcd(n_i, N/n_i) = 1 \) and we can compute \( u_i \) and \( v_i \) with

\[
u_i n_i + v_i (N/n_i) = 1.
\]

Let \( e_i = v_i (N/n_i) \), then this equation becomes

\[
u_i n_i + e_i = 1 \text{ or } e_i \equiv 1 \mod n_i.
\]

Furthermore, since all \( n_j | (N/n_i) \) for \( j \neq i \) we also have \( e_i = v_i (N/n_i) \equiv 0 \mod n_j \) for \( j \neq i \).

Using these values \( e_i \) a solution to the system of equivalences is given by

\[
X = \sum_{i=1}^{k} r_i e_i,
\]

since \( X \) satisfies \( X \equiv r_i \mod n_i \) for each \( 1 \leq i \leq k \).

**Example 2** Consider the system of integer equivalences

\[
X \equiv 1 \mod 3,
X \equiv 2 \mod 5,
X \equiv 5 \mod 7.
\]

The moduli are coprime and we have \( N = 105 \). For \( n_1 = 3, N_1 = 35 \) we get \( v_1 = 2 \) by just observing that \( 2 \cdot 35 = 70 \equiv 1 \mod 3 \). So \( e_1 = 70 \). Next we compute \( N_2 = 21 \) and see \( v_2 = 1 \) since \( 21 \equiv 1 \mod 5 \). This gives \( e_2 = 21 \). Finally, \( N_3 = 15 \) and \( v_3 = 1 \) so that \( e_3 = 15 \).

The result is \( X = 70 + 2 \cdot 21 + 5 \cdot 15 = 187 \) which indeed satisfies all 3 congruences. To obtain the smallest positive solution we reduce 187 modulo \( N \) to obtain 82.

For easier reference we phrase this approach as an algorithm.

**Algorithm 3** (Chinese remainder computation)

IN: *system of k equivalences as \((r_1, n_1), (r_2, n_2), \ldots, (r_k, n_k)\)* with pairwise coprime \( n_i \)

OUT: *smallest positive solution to system*

1. \( N \leftarrow \prod_{i=1}^{k} n_i \)
2. \( X \leftarrow 0 \)
3. for \( i = 1 \) to \( k \)
   \(\quad\quad\) (a) \( M \leftarrow N \div n_i \)
   \(\quad\quad\) (b) \( v \leftarrow ((N_i)^{-1} \mod n_i) \) (use XGCD)
   \(\quad\quad\) (c) \( e \leftarrow vM \)
   \(\quad\quad\) (d) \( X \leftarrow X + r_i e \)
4. \( X \leftarrow X \mod N \)