1. Solve for x

$$(a)\quad \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \end{cases} \qquad (b)\quad \begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 3 \pmod 7 \end{cases}$$

$$(c)\quad \begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 3 \pmod 5 \end{cases} \qquad (d)\quad \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 6 \end{cases}$$

Solution. (a) The Bézout identity for $(3, 4)$ is $-1 \cdot 3 + 1 \cdot 4 = 1$. Hence the solution is

$$x = 1 \cdot 1 \cdot 4 + 2 \cdot (-1) \cdot 3 = 4 - 6 = -2 \equiv 10 \pmod{12} \ .$$

One can observe that $10 \bmod 3 = 1$ and $10 \bmod 4 = 2$.

(b) The Bézout identity for $(4, 7)$ is $2 \cdot 4 - 1 \cdot 7 = 1$. Hence the solution is

$$x = 3 \cdot 2 \cdot 4 + 0 = 24 \pmod{28} \ .$$

One can observe that $24 \bmod 4 = 0$ and $24 \bmod 7 = 3$.

(c) The Bézout identity for $(12, 5)$ is $-2 \cdot 12 + 5 \cdot 5 = 1$. Hence the solution is

$$x = 3 \cdot -2 \cdot 12 + 10 \cdot 5 \cdot 5 = -72 + 250 = 178 \equiv 58 \pmod{60} \ .$$

One can observe that $58 \mod 12 = 10$ and $58 \mod 5 = 3$.

(d) The Bézout identity for $(5, 6)$ is $1 \cdot 6 - 1 \cdot 5 = 1$. Hence the solution is

$$x = 5 \cdot 5 \cdot (-1) + 3 \cdot 6 \cdot 1 = -25 + 18 = -7 \equiv 23 \pmod{30} \ .$$

One can observe that $23 \bmod 5 = 3$ and $23 \bmod 6 = 5$.

2. Solve for x

$$(a)\quad \begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \qquad (b)\quad \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$

Solution. (a) We've got 3 moduli, hence $N = 2 \cdot 3 \cdot 5 = 30$ and

$$N_1 = \frac{30}{2} = 15 \ , \qquad N_2 = \frac{30}{3} = 10 \ , \qquad N_3 = \frac{30}{5} = 6 \ .$$

The Bézout identities for $\gcd(N_i, n_i)$ are

$$\begin{aligned} \gcd(15, 2) &= 1 \cdot 15 + (-7) \cdot 2 = 1 \ , \\ \gcd(10, 3) &= 1 \cdot 10 + (-3) \cdot 3 = 1 \ , \\ \gcd(6, 5) &= 1 \cdot 6 + (-1) \cdot 5 = 1 \ . \end{aligned}$$

Hence, $M_1 = M_2 = M_3 = 1$. We will use the formula

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{N} \ . \tag{1}$$

Therefore,

$$x = 0 + 2 \cdot 1 \cdot 10 + 3 \cdot 1 \cdot 6 = 38 \equiv 8 \pmod{30} \ .$$

To verify that 8 is indeed the solution, observe that

$$8 \bmod 2 = 0 \ , \qquad 8 \bmod 3 = 2 \ , \qquad 8 \bmod 5 = 3 \ .$$

(*b*) We've got 4 moduli, hence $N = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and

$$N_1 = \frac{210}{2} = 105 \ , \quad N_2 = \frac{210}{3} = 70 \ , \quad N_3 = \frac{210}{5} = 42 \ , \quad N_4 = \frac{210}{7} = 30 \ .$$

The Bézout identities for $\gcd(N_i, n_i)$ are

$$\begin{aligned} \gcd(105, 2) &= 1 \cdot 105 + (-52) \cdot 2 = 1 \ , \\ \gcd(70, 3) &= 1 \cdot 70 + (-23) \cdot 3 = 1 \ , \\ \gcd(42, 5) &= (-2) \cdot 42 + 17 \cdot 5 = 1 \ , \\ \gcd(30, 7) &= (-3) \cdot 30 + 13 \cdot 7 = 1 \ . \end{aligned}$$

Hence, $M_1 = M_2 = 1, M_3 = -2, M_4 = -3$. By (1), the solution is

$$x = 1 \cdot 1 \cdot 105 + 2 \cdot 1 \cdot 70 + 3 \cdot (-2) \cdot 42 + 5 \cdot (-3) \cdot 30 = -457 \equiv 173 \pmod{210} \ .$$

To verify that 173 is indeed the solution, observe that

$$173 \bmod 2 = 1 \ , \quad 173 \bmod 3 = 2 \ , \quad 173 \bmod 5 = 3 \ , \quad 173 \bmod 7 = 5 \ .$$

3. Modified RSA signature scheme. First, let's recall the regular RSA signatures.

   (a) Alice selects sufficiently large primes p and q and calculates $n = pq$.

   (b) Alice selects her public exponent $e \in \mathbb{Z}^{\times}_{\varphi(n)}$.

   (c) Alice calculates her private exponent $d \in \mathbb{Z}^{\times}_{\varphi(n)}$ such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

   (d) Alice publishes her public key (e, n) to the key server, and keeps her private key (d, n) to herself.

   (e) To sign a document $\hat{d}$, Alice takes a hash of it $m = H(\hat{d}) \in \mathbb{Z}_n$.

   (f) The signature of Alice is $m^d \bmod n$, she distributes it together with the document.

   (g) To verify the signature, Bob downloads Alice's public key (e, n) and computes

   $$\Big(m^d \bmod n\Big)^e \bmod n = m^{de} \bmod n = m \ .$$

   If $m = H(\hat{d})$, the signature is valid.

Now consider a modification to this scheme. Assume we do not need CRT to combine elements in $\mathbb{Z}_p^\times$ and $\mathbb{Z}_q^\times$ into one structure $\mathbb{Z}_{pq}^\times$. Instead, let's just work in one ring $\mathbb{Z}_n^\times$, where n is sufficiently large prime. The modified scheme works as follows.

(a) Alice selects a sufficiently large prime n and selects her public exponent $e \in \mathbb{Z}_{\varphi(n)}^\times$.

(b) Alice calculates her private exponent $d \in \mathbb{Z}_{\varphi(n)}^\times$ such that $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

(c) Alice publishes her public key (e, n) to the key server and keeps her private key (d, n) to herself. To sign a document $\hat{d}$, Alice takes a hash of it $m = H(\hat{d}) \in \mathbb{Z}_n$.

(d) The signature of Alice is $m^d \bmod n$, she distributes it together with the document.

(e) To verify the signature, Bob downloads Alice's public key (e, n) and computes

$$\Big(m^d \bmod n\Big)^e \bmod n = m^{de} \bmod n = m \ .$$

If $m = H(\hat{d})$, the signature is valid.

This scheme is not secure against passive adversary Carol. It turns out that Carol can obtain Alice's private key from her public key (e, n) and only just one sample of her signature $m^d \bmod n$. This will allow Carol to make as many fake signatures on behalf of Alice as she wants with Alice being completely unaware of it. How can Carol obtain Alice's private key (d, n)?

Solution. Since n is prime, Carol can easily calculate $\phi(n) = n - 1$. Given Alice's public exponent $e \in \mathbb{Z}_n^\times$, Carol can calculate Alice's private exponent in polynomial time using extended Euclidean algorithm as follows

$$e \in \mathbb{Z}_n^\times \implies \gcd(e, n) = 1 \ .$$

Then, by the Bezout identity there exist $\phi, \psi \in \mathbb{Z}$ such that $\phi \cdot e + \psi \cdot n = 1$, and hence Alice's private exponent d is $d = \phi = e^{-1}$ in $\mathbb{Z}_n^\times$.

4. Let Alice send a message M to bob. Let Bob's public key be (e, n). Adversary Carol sees the cryptogram $M^e \bmod n$. If $M^e < n$, can Carol recover M?

Solution. Carol can recover M by calculating $\sqrt[e]{M^e} = M$.