CHINESE REMAINDER THEOREM

- Used to solve a set of congruent equations with one variable but different moduli, which are relatively prime

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

Continued…

- Example
  - The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

  - The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is $x = 23$. This value satisfies all equations: $23 \equiv 2 \pmod{3}$, $23 \equiv 3 \pmod{5}$, and $23 \equiv 2 \pmod{7}$.

Continued…

- Solution To Chinese Remainder Theorem
  - Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
  - Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
  - Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
  - The solution to the simultaneous equations is

$$\boxed{x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M}$$

Continued…

- Example
  - Find the solution to the simultaneous equations:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

- Solution: We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$
3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

Continued…

- Example
  - Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.
- Solution ????

Continued...

- Example
  - Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.
- Solution
  - This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$
$$x = 3 \bmod 13$$
$$x = 0 \bmod 12$$

  - If we follow the four steps, we find x = 276. We can check that
    276 = 3 mod 7, 276 = 3 mod 13 and 276 is divisible by 12 (the quotient is 23 and the remainder is zero).

Continued…

- Assume we need to calculate z = x + y where x = 123 and y = 334, but our system accepts only numbers less than 100. These numbers can be represented as follows:

$$
\begin{array}{ll}
x \equiv 24 \pmod{99} & y \equiv 37 \pmod{99} \\
x \equiv 25 \pmod{98} & y \equiv 40 \pmod{98} \\
x \equiv 26 \pmod{97} & y \equiv 43 \pmod{97}
\end{array}
$$

- Adding each congruence in x with the corresponding congruence in y gives

$$
\begin{array}{lcl}
x + y \equiv 61 \pmod{99} & \rightarrow & z \equiv 61 \pmod{99} \\
x + y \equiv 65 \pmod{98} & \rightarrow & z \equiv 65 \pmod{98} \\
x + y \equiv 69 \pmod{97} & \rightarrow & z \equiv 69 \pmod{97}
\end{array}
$$

- Now three equations can be solved using the Chinese remainder theorem to find z. One of the acceptable answers is z = 457.

Continued…

Secret Sharing scheme in cryptography aims to distribute and later recover secret S among n parties. Secret S is distributed in form of shares which are generated from secret. Without cooperation of k no. of parties, the secret cannot be reconstructed from shares directly. Consider the following example:

Say our secret is S. The shares for n=4 no. of parties are generated taking modulus 11,13,17 and 19. They are respectively 1,12,2 and 3 and given by following equations:

Now, from four possible sets of k=3 shares (as k shares are necessary to reconstruct the secret), consider one possible set {1, 12, 2} and recover the secret S from it.

Continued…

Secret Sharing scheme in cryptography aims to distribute and later recover secret S among n parties. Secret S is distributed in form of shares which are generated from secret. Without cooperation of k no. of parties, the secret cannot be reconstructed from shares directly. Consider the following example:

Say our secret is S. The shares for n=4 no. of parties are generated taking modulus 11,13,17 and 19. They are respectively 1,12,2 and 3 and given by following equations:

$S \equiv 1 \bmod 11$,

$S \equiv 12 \bmod 13$,

$S \equiv 2 \bmod 17$,

$S \equiv 3 \bmod 19$.

Now, from four possible sets of k=3 shares (as k shares are necessary to reconstruct the secret), consider one possible set {1, 12, 2} and recover the secret S from it.

Continued…

Solution: The problem can be solved by Chinese remainder theorem.

For the set {1,12,2}, the equations available are,

S Ξ 1 mod 11,

S Ξ 12 mod 13,

S Ξ 2 mod 17,

Now solving this equation using CRT, M=11 *13*17 = 2431,

M1 = 2431/11=221,

M2 = 2431/13=187,

M3=2431/17=143

$M1^{-1}$, $M2^{-1}$ and $M3^{-1}$ can be calculated using Extended Euclidean Algorithm.

$M1^{-1}$ = 1

$M2^{-1}$ = 8

$M3^{-1}$= 5

Now, secret S= ((1*221*1) + (12*187*8) + (2*143*5)) mod 2431

S = 155 mod 2431

Continued…

In RSA, when the same message is encrypted for three people who happen to have same public key but different values of n, it is possible to get the value of message by using Chinese Remainder Theorem.

Can you formulate the problem statement ?

And how it leads to Chinese Remainder problem?