

After receiving the inputs n , a_i , b_i , and m_i , we apply these steps in order to find the solution:

1 - Check to see whether a_i and m_i are relatively prime

1A - $\text{GCD}(a_i, m_i) = 1$ for all $i \leq n$

2 - Check to see whether all the m_i are pairwise relatively prime with each other.

2A - $\text{GCD}(m_i, m_{i+1}, m_{i+2} \dots, m_n) = 1$ for all $i \leq n$

3 - If not, then it has no unique solution.

4 - If so, we get the value of m_{Product} which is the product of all given m s

5 - We get the value of M_i which is m/m_i for all $i \leq n$

6 - We get all the inverses for all a_i in all m_i using the Extended Euclidean Algorithm

7 - We output " x " as the unique solution for the set of the given linear congruencies as per the following equation:

$$x = (a_1^{b_1} M_1 y_1 + a_2^{b_2} M_2 y_2 + \dots + a_n^{b_n} M_n y_n) \bmod m$$

Pseudocode:

Main

Ask user for number of equations n

Ask user for values of a_i, b_i, m_i // $a_n x \equiv b_n \pmod{m_n}$

IF (for each a_i and m_i relatively prime) and (for each m_i are pairwise relatively prime) then

$$M = \prod_{i=1}^n m_i$$

FOR i in n Do $M_i = \frac{M}{m_i}$ ENDFOR

FOR i in n Do $a y_i = \text{mod inverse } a_i, m_i$ ENDFOR

$$x_1 = \sum_{i=1}^n [a y_i * b_i * M_i * \text{mod inverse } M_i, m_i]$$

$$\text{solution} = x_1 \pmod{M}$$

ENDIF

END

Mod inverse

Input a, m

If $m == 1$ then return 0

FOR i in m Do

IF $a * i \pmod{m} == 1$ then return i ENDIF

ENDFOR

END

Data structure used: Array

Cost Analysis: Time complexity of $O(n^2)$ for the pairwise relatively prime checking.

Sample runs:

```
Enter the number of equations
3
Only positive non-zero numbers are allowed
6 82 61
86 54 19
47 33 26
The solution is: 14491
Members of the group are:
Abdullah Alminqah      (Serial Number: 4)
Saad Al Dosari         (Serial Number: 3)
Khalid Alqahtani       (Serial Number: 20)
Ahmad Alsohail         (Serial Number: 9)
Ahmed Alfaifi          (Serial Number: 12)
```

```
Enter the number of equations
2
Only positive non-zero numbers are allowed
52 36 14
44 85 20
No solution because m is not 1
Members of the group are:
Abdullah Alminqah      (Serial Number: 4)
Saad Al Dosari         (Serial Number: 3)
Khalid Alqahtani       (Serial Number: 20)
Ahmad Alsohail         (Serial Number: 9)
Ahmed Alfaifi          (Serial Number: 12)
```

```
Enter the number of equations
3
Only positive non-zero numbers are allowed
9 7 2
13 7 3
19 11 9
No solution because modulus are not pairwise relatively prime
Members of the group are:
Abdullah Alminqah      (Serial Number: 4)
Saad Al Dosari         (Serial Number: 3)
Khalid Alqahtani       (Serial Number: 20)
Ahmad Alsohail         (Serial Number: 9)
Ahmed Alfaifi          (Serial Number: 12)
```

Conclusion: We learned to work and communicate better as a team. We understood the importance of brainstorming before jumping into the code. We ordered the steps we were going to take, and we then put the steps into appropriate code form. This led us to appreciate CRT more and helped us gain a deeper understanding of it.

Members of the group are:

Abdullah Alminqah (Serial Number: 4)

Saad Al Dosari (Serial Number: 3)

Khalid Alqahtani (Serial Number: 20)

Ahmad Alsohail (Serial Number: 9)

Ahmed Alfaifi (Serial Number: 12).