KING SAUD UNIVERSITY

COLLEGE OF COMPUTER & INFORMATION SCIENCES
DEPT OF COMPUTER SCIENCE

CSC281 Discrete Mathematics for Computer Science Students
First Semester 1442 AH
Due: Tue, December 8, 2020 (before midnight)
Instructors: Prof. Aqil Azmi and Dr. Yousef Alohali

Group Term Project

The objective of this project is to find the unique solution to *n* linear congruencies. Consider the following *n* equations,

$$\begin{aligned} a_1 x &\equiv b_1 \bmod m_1 \\ a_2 x &\equiv b_2 \bmod m_2 \\ a_3 x &\equiv b_3 \bmod m_3 \\ &\vdots \\ a_n x &\equiv b_n \bmod m_n \end{aligned}$$

where all the variables are integers. Each of the linear congruencies has a unique solution if a_i and m_i (for all $i \le n$) are relatively prime. Moreover, according to the Chinese Remainder Theorem (CRT), these *n* equations have a unique solution modulo $m_1 \times m_2 \cdots \times m_n$ if m_i and m_j (for $i \neq j$) are pairwise relatively prime.

Let $m = \prod_{i=1}^{n} m_i$, and $M_i = m / m_i$ for all $i \le n$. Then the solution of this set of linear congruencies is given by,

$$x = a_1' b_1 M_1 y_1 + a_2' b_2 M_2 y_2 + \cdots + a_n' b_n M_n y_n \bmod m,$$

where $a_1', a_2', \ldots, a_n'$ are the inverses of $a_1, a_2, \ldots, a_n$ in the modulo $m_1, m_2, \ldots, m_n$ (respectively); and y_i are such that $M_i y_i \equiv 1 \bmod m_i$.

Project

Write a program that accepts the input in the following format,

n
a_1 b_1 m_1
a_2 b_2 m_2
.
.
a_n b_n m_n

Then outputs the unique solution *x* or say "No solution".

Instructions

This is a group project. Each four students will work as a team. You are free to use any convenient programming language. This project is worth 10 points.

What to submit

(a) Write-up of the project (brief description of your algorithm; the data structure used; cost analysis; sample runs and the conclusion). Each group should email the PDF of the report and the executable (e.g., .jar file for java).
(b) When executed, the program should show the name of all members of the group.
(c) Each group will get to demo their code in a zoom session. We will supply the data during demo.