Group 2

2/16/20

**CECS 229 Lab 3 Report**

The Chinese Remainder Theorem (CMT) can be used to solve the solution of a system of congruences **(x\_1 = a\_1modm\_2 , x\_2 = a\_2modm\_2….)** The first step of the Chinese Remainder Theorem is to calculate M, which can be found by multiplying all m\_’s together. **M = m\_1\*m\_2….** From there we can calculate M\_1, M\_2…. by dividing M by their respective a\_ and performing their respective mod\_.  **Ex: M\_1 = (M/a\_1)modm\_1.** Afterwards, we calculate the inverse of each M\_. To ensure that there is an inverse, the greatest common divisor (GCD) of (M/a\_1) and m\_1 has to be 1. An inverse to M\_ is a number that is multiplied to M\_ that will result in a remainder of 1 when modded. In our code, we incorporated a “while loop” initializing a counter **x = 1**. The loop will terminate when x exceeds m\_ (**x > m\_)**. In the loop, a number y is generated through multiplying x by M\_ (**y = x \* M\_**). This number y is checked to see if modded by m\_, the result will be 1. (**y % m\_ == 1**) If it equals 1, then y is deemed the inverse of M\_. If it does not equal 1, x is incremented by 1 and the process repeats. Now that we have our inverses we can calculate X\_ which is derived from **X\_1 = a\_1\*(M/a\_1)\*inverse\_1**. Finally we can add up all respective X\_’s and mod the sum by M. Ex: (**X\_1+X\_2+....= SUMmodM**). The resulting remainder is the solution to the system of congruences.

A close up of text on a white background

Description automatically generated

A close up of text on a white background

Description automatically generated