Assignment 2

The Chinese Remainder Theorem — Nandan Madhuj

Project #4 — Roll: 210648

1 Solving for x.

$x \equiv 2 \mod 3, \qquad x \equiv 3 \mod 5, \qquad x \equiv 2 \mod 7$

or $x = b_i \mod n_i$.... for i $\in \{1,2,3\}$

where $n_1 = 3, n_2 = 5, n_3 = 7$ and similar relations for b_i

where $b_1 = 2, b_2 = 3, b_3 = 2$

and $N = n_1 \cdot n_2 \cdot n_3 = 105$

and $N_i = \frac{N}{n_i}$ for i $\in \{1,2,3\}$

So, $N_1 = 35, N_2 = 21, N_3 = 15$

We define x_i such that, $x_i \cdot N_i \equiv 1 \mod n_i$

So, $x_1 \cdot N_1 \equiv 1 \mod n_1$

$\implies x_1 \cdot 35 \equiv 1 \mod 3$

$\implies x_1 \cdot -1 \equiv 1 \mod 3$

$\implies x_1 \equiv -1 \mod 3 \equiv 2 \mod 3$

Similarly,

$x_2 \cdot N_2 \equiv 1 \mod n_2$

$\implies x_2 \cdot 21 \equiv 1 \mod 5$

$\implies x_2 \equiv 1 \mod 5$

Also,

$x_3 \cdot N_3 \equiv 1 \mod n_3$

$\implies x_3 \cdot 15 \equiv 1 \mod 7$

$\implies x_3 \equiv 1 \mod 7$

Using the CRT, we have,

$x = \sum_{1,2,3} x_i \cdot N_i \cdot b_i$

$\implies x = 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 2 = 233$

$\implies x \equiv 233 \mod 105 \equiv 23 \mod 105.$

Required solution is $x \equiv 23 \mod 105$

2 Given first relation: $x = 36 \cdot k + 11$

Taking $\mod 4$ and $\mod 9$, we get,

$x \equiv 11 \mod 4 \implies x \equiv 3 \mod 4$

$x \equiv 11 \mod 9 \implies x \equiv 2 \mod 9$

Similarly, the other two relations give

$x \equiv 7 \mod 8$

$x \equiv 2 \mod 5$

Also,

$x \equiv 7 \mod 25$

$x \equiv 2 \mod 3$

Hence, we have 6 relation.

Some are implied by the following 3 relations:

$x \equiv 2 \mod 9$

$x \equiv 7 \mod 8$

$x \equiv 7 \mod 25$

These can directly be solved using Chinese Remainder Theorem. We define $\{x_1, x_2, x_3\}$ inverses of 200,225 and 72 w.r.t modulo 9,8 and 25 respectively.

$x_1 \cdot 200 \equiv 1 \mod 9 \implies x_1 = 5.$

$x_2 \cdot 225 \equiv 1 \mod 8 \implies x_2 = 1.$

$x_3 \cdot 72 \equiv 1 \mod 25 \implies x_3 = 8.$

So by CRT we get $x = 5 \cdot 200 \cdot 2 + 1 \cdot 225 \cdot 7 + 8 \cdot 72 \cdot 7 = 7606 \equiv 407 \mod 1800.$

Or We directly use Code used in 6th problem to get

x=407 $\mod 1800$

3. Symbols have usual meaning.

$x^2 \equiv 1 \mod 3 \iff x \equiv 1 \mod 3$ or $x \equiv 2 \mod 3$.

System 1: $x \equiv 1 \mod 3$ and $x \equiv 2 \mod 4$

We define $N = 3 \cdot 4 = 12$

$N_i = \frac{N}{n_i}$

$N_1 = 4$ and $N_2 = 3$

We define x_i such that $x_i \cdot N_i \equiv 1 \mod n_i$

$x_1 \cdot 4 \equiv 1 \mod 3 \implies x_1 = 1.$

$x_2 \cdot 3 \equiv 1 \mod 4 \implies x_2 = 3$. Using the Chinese remainder theorem, $x = \sum x_i \cdot N_i \cdot b_i$

where b_i is the residue class of x w.r.t n_i

This gives,

$x = 1 \cdot 4 \cdot 1 + 3 \cdot 3 \cdot 2 \equiv 10 \mod 12$

System 2: $x \equiv 2 \mod 3$ and $x \equiv 2 \mod 4$

We define $N = 12$.

$N_1 = 4$ and $N_2 = 3$

We define x_i in a similar way.

$x_1 = 1$ and $x_2 = 3$

Hence,

$x = 1 \cdot 4 \cdot 2 + 3 \cdot 3 \cdot 2 \equiv 2 \mod 12$

Hence, the combined solution is $x \pm 2 \mod 12$

4

We note that for a number n to be p-safe,

$3 \leq n \mod p \leq p-3$

So $n \mod p$ may take values $\{3, 4, 5 \ldots p-3\}$

That is, total of p-5 values.

For 7-safe, permitted residue classes are $\{3, 4\}$.

For 11-safe, permitted residue classes are $\{3, 4, 5 \ldots 8\}$

For 13-safe, permitted residue classes are $\{3, 4, 5 \ldots 10\}$ Hence, to be 7-safe,11-safe,13-safe simultaneously, we have the system,

$x \equiv a_i \mod 7$

$x \equiv b_i \mod 11$

$x \equiv c_i \mod 13$

where a_i, b_i, c_i is one of the permitted residue classes for 7-safe,11-safe and 13-safe respectively.

We note that, gcd(7,11,13) $= 1$. $\implies$ we have unique solution modulo 1001 for each of a_i, b_i, c_i.

Hence, in modulo 1001, we have $2 \cdot 6 \cdot 8 = 96$ unique solution modulo 1001. (one corresponding to each choice of a_i, b_i, c_i.)

Since we need x $\leq$ 10000, upto 10010, we have $10 \cdot 96 = 960 solutions$. But some values may be greater than 10,000.

7-safes in range are $\{10, 006, 10, 007\}$

11-safes in range are {10002,10003,10004,10005...10007}

13-safes in are {10001,10002...10007}.

Common numbers are 10006 and 10007. So, we subtract these.

Hence total, $960 - 2 = 958$. (Total possibilities.)

5

The problem requires the residues of divisor m $\in \{2,3,5\}$ be repeated after m positions. So, for $m = 2$, we need only fix the remainders of a_1 and a_2. $\implies$ 2 ways.

Similarly, for $m = 3$ we fix remainders fora_1, a_2 and a_3. $\implies$ 3! ways.

And, for $m = 5$, we fix remainders for $a_1, a_2 \ldots a_5$ $\implies$ 5! ways.

Total: $2 \cdot 6 \cdot 120 = 1440$ ways.

After that, remainders are fixed w.r.t divisors 2,3 and 5 for all positions.

By CRT we obtain unique solutions modulo 30 at each of these positions.

Hence, after setting up the remainders at first 5 positions, we have fixed the required permutation as all places have unique solution modulo 30.

At one of these places, we have a 0, which we replace by 30.

Hence, we can conclude that N = 1440. $\implies$ $N \equiv 440 \mod 1000$

6 Implementing CRT on coprime Divisors.

Following code is in C language.

CRT in Action

Please download the file if its not loading.