CHINESE REMAINDER THEOREM

Weiwei Breakwell, Civil Engineering
Mentor: Dr. Berit Givens
Kellogg Honors College Capstone Project

INTRODUCTION

The Chinese Remainder Theorem is first published in the 3rd century by the Chinese mathematician Sun Tzu. This theorem is a method used for solving systems of linear congruences with integers. In its basic form, the Chinese remainder theorem will determine the remainder of a number *n* when divided by a given integer.

Example
An old woman goes to the market and a horse steps on her basket crashing the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

$x \equiv 1 \bmod 2$	$(a_1 = 1, m_1 = 2)$
$x \equiv 1 \bmod 3$	$(a_2 = 1, m_2 = 3)$
$x \equiv 1 \bmod 4$	$(a_3 = 1, m_3 = 4)$
$x \equiv 1 \bmod 5$	$(a_4 = 1, m_4 = 5)$
$x \equiv 1 \bmod 6$	$(a_5 = 1, m_5 = 6)$
$x \equiv 0 \bmod 7$	$(a_6 = 0, m_6 = 7)$

There is a known formula called the Chinese Remainder Theorem such that x = 301.

OBJECTIVE

The Chinese Remainder Theorem only solves the question type above. However, by modifying the equations, we scaled one of the x's down by multiplying by a rational number p/q. Since the Chinese Remainder Theorem cannot be used to solve these modified equations, the project's objective was to come up with methods that can solve these modified equations.

General Equations:
$x \equiv a \bmod m$ (equation 1)
$\frac{p}{q} x \equiv b \bmod n$ (equation 2)

Assumptions:
$\gcd(m,n) = 1$
$\gcd(p,q) = 1$
$0 < \frac{p}{q} < 1$
$\gcd(q,m) = 1$
$\gcd(p,n) = 1$

Questions:
1) Create an algorithm, implement in Excel spreadsheet.
2) For what types of a, b, m, n, p, q, are there solutions for x?
3) Given one solution, how to find more solutions?
4) What is an upper bound for a minimum positive solution?

EXCEL SPREADSHEET DEVELOPMENT

Started with x = qk + r, where 0 ≤ r < q
Substituted x into Equations 1 and 2

qk ≡ (a - r) mod m (equation 3)
pk ≡ b - $\left\lfloor \frac{p}{q} r \right\rfloor$ mod n (equation 4)

Using excel, we found the linear combination of q and m, and p and n. From there we solved Equations 3 and 4 for k resulting in the terms equivalent to a_1 and a_2 in the Chinese Remainder Theorem. Similarly we found the inverse modular for m and n which allowed us to solve for k. we considered each of the r values.

Once we simplified equations 3 and 4, we were left with one variable, k, and two equations. This brings us back to the Chinese Remainder Theorem, where we then solved for k. Once we obtained k, we plugged that value back into x = qk + r and found the different x values for each r.

EXCEL EXAMPLE

An Excel spreadsheet was developed to test the effect of changing different parameters. From which, other results were also conjectured when different parameters were changed.

$x \equiv 2 \bmod 5$
$\frac{3}{7} x \equiv 3 \bmod 8$

Where,
a = 2 | n= 8
b = 3 | p = 3
m = 5 | q = 7

Check,
gcd(m,n) = gcd(5,8) = 1
gcd(p,q) = gcd(3,7) = 1
gcd(q,m) = gcd(7,5) = 1
gcd(p,n) = gcd(3,8) = 1
$0 < \frac{p}{q} = \frac{3}{7} < 1$

x = 7k + r, 0 ≤ r < 7
For this example we picked r = 1. We can do this because r has finite number of values and it will eventually repeat, in our case, starting at 7.

r = 1
7k + 1 ≡ 2 mod 5
3k + $\left\lfloor \frac{3}{7} \right\rfloor$ ≡ 3 mod 8

From Excel
k ≡ 3 mod 5
k ≡ -15 mod 8

From Chinese Remainder Theorem k = 33

By plugging k back into equation x = 7k + r, we obtain a value of 232.

	Equation 3	Equation 4				
r	a-r (mod m)	b-pr/q (mod n)	Solns to pk ≡ a-r (mod m)	**x**	**mod (m)**	**mod (n)**
0	6	-15	1	7	TRUE	TRUE
1	3	-15	33	232	TRUE	TRUE
2	0	-15	25	177	TRUE	TRUE
3	-3	-10	22	157	TRUE	TRUE
4	-6	-10	14	102	TRUE	TRUE
5	-9	-5	11	82	TRUE	TRUE
6	-12	-5	3	27	TRUE	TRUE
7	-15	0	0	7	TRUE	TRUE
8	-18	0	32	232	TRUE	TRUE
9	-21	0	24	177	TRUE	TRUE

RESULTS

Theorem 1
If $\gcd(m,q) = \gcd(m,n) = \gcd(p,n) = \gcd(p,q) = 1$, $a < m$, and $b < n$, then solutions for x are guaranteed.

Theorem 2
If $x = x_0$ is one solution then more solutions can be found by $x = x_0 + lcm(m,n)qt$, where t is any integer.

Example,
If $m = 5, n = 4, q = 7$, and $x_0 = 8$ is one solution then so are $8 + 140t$, which is 148, 288,...etc.

Theorem 3
Let x_0 be the minimum positive solution.
1) $x_0 \le q \cdot lcm(m,n)$
$\frac{x_0}{lcm(m,n)} \le q$
2) If $a = 1, m = 2, b = n - 1, q = n, p = 1$, and n must be odd.
Then $x_0 = n(n-1) + 1$
So $\frac{x_0}{lcm(m,n)} \ge \frac{q-1}{2} + \frac{1}{2q}$