Sacred Heart University

Mathematics

Senior Seminar

Chinese Remainder Theorem

Author:

Nancirose Piazza

Mentor:

Dr. Gopalakrishnan

March 29, 2018

Abstract

The Chinese Remainder Theorem is one of the oldest theorems in mathematics. It states that a system of linear congruences with pairwise relatively prime moduli has a unique solution modulo the product of its pairwise relatively prime moduli. In this talk, we will prove the Chinese Remainder Theorem and illustrate with an example.

1 Introduction

The Chinese Remainder Theorem first came from the Chinese mathematical treatise, *Sun Tze Suan Ching* written by Sun Zi. Little is known about the author except that he may have been a Buddist monk who lived in the third or fourth century AD. From Volume 3 of his work, *Master Sun's Mathematical Manual*, the following is translated:

> "We have a number of things, but we do not know exactly how many. If we count them by threes we have two left over. If we count them by five we have three left over. If we count them by sevens we have two left over. How many things are there?" (Marshall, Odell, and Starbird, 2007)

The Chinese Remainder Theorem claims that if $n_1, n_2, \ldots n_L$ are positive integers that are pairwise relatively prime such that $gcd(n_i,\ n_j) = 1$ *for* $i \neq j,\ 1 \leq i, j \leq L$. Then the system of L congruences:

$$x \equiv a_1 \ (mod\ n_1)$$

$$x \equiv a_2 \ (mod\ n_2)$$

$$\vdots$$

$$x \equiv a_L \ (mod\ n_L)$$

has a unique solution modulo the product $n_1 n_2 n_3 ... n_L$.

We start with definitions in divisibility, congruence modulo n, and greatest common divisors. We will prove results leading to the Chinese Remainder Theorem.

1.1 Background

All definitions and statements of theorems in this paper are provided from [1]. The proofs of the theorems were derived through the method of inquiry.

2 Divisibility and Greatest Common Divisor

Divisibility is an essential concept and foundation to many theorems in number theory. We will start with the divisibility definition and work our way to the Diophantine equation and to the Chinese Remainder Theorem.

Definition 2.1. *(Divisibility) Let a and b* $\in \mathbb{Z}$*. We say a divides b, denoted as* $a|b$*, if there exists an integer k such that* $ak = b$*.*

2.1 Divisibility

Example 2.1. *Consider* $3 \mid 6$*. Then there exists an integer k, namely* $k = 2$*, such that* $3k = 6$*.*

We can continue with this example to explore other properties. It is true that if $3|6$ and $3|9$, then $3|(6 + 9)$. Also, if $3|6$, then 3 divides any multiple of 6 such as 12, 18, and so on. These properities of divisibility are true for integers in general and we therefore state them as theorems.

Theorem 2.1. *Let a, b, and $c \in \mathbb{Z}$. If $a|b$ and $a|c$ then $a|(b + c)$.*

Proof. Suppose $a|b$ and $a|c$. Then there exist integers k and m such that $ak = b$ and $am = c$. Adding both equations together we obtain $ak + am = b + c$. Since $(k + m) \in \mathbb{Z}$, then this implies that $a|(b + c)$ by Theorem 2.1. □

By subtracting the second equation from the first in the proof of Theorem 2.1, another theorem follows.

Theorem 2.2. *Let a, b, and $c \in \mathbb{Z}$. If $a|b$ and $a|c$ then $a|(b - c)$.*

Theorem 2.3. *Let a, b, and $c \in \mathbb{Z}$. If $a|b$ then $a|bc$.*

Proof. Suppose $a|b$, then there exists an integer k such that $ka = b$. We multiply by integer c to obtain $kac = bc$. Since $(kc) \in \mathbb{Z}$, then $a|(bc)$. □

Theorem 2.4. *Let a, b and $c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.*

Proof. Suppose $a|b$ and $b|c$. By Definition 2.1, there exist integers k and m such that $ka = b$ and $mb = c$. We substitute for b to obtain $(mk)a = c$. Since $(mk) \in \mathbb{Z}$, then again by Definition 2.1, we have $a|c$. □

For any integers a and b where $b > 0$, there is a linear relationship between a and b given by the Division Algorithm. We shall state and prove this algorithm for positive integers.

Theorem 2.5. *(Division Algorithm) Let m and $n \in \mathbb{N}$. Then there exist unique integers q, r such that $m = qn + r$, where $0 \leq r \leq n - 1$.*

Proof: (Existence) The Well-Ordering Axiom states every nonempty subset of positive integers contains a smallest element. Without loss of generality, assume $m > n$. If $n|m$, then there exists an integer q such that $m = qn = qn + 0$. Then $r = 0$. If n does not divide m, then let's construct a set S as followed: $S = \{m - kn \mid k \in \mathbb{Z}\ m - kn > 0\}$. If $k = 0$, then $m - kn = m$. Since m is greater than 0, then m must be an element in S. This proves that set S is non empty. Then by the Well-Ordering Axiom, there is a smallest element r in set S such that $r = m - qn$ for some integers q, $r > 0$. We want to prove $r \leq n - 1$, so let's assume $r > n - 1$. Since $r > n - 1$, then it is clear that $r \geq n$. Then $r = m - nq \geq n$ which implies $m - n(q - 1) \geq 0$. If $m - n(q - 1) = 0$, then $m = n(q - 1)$ implies that $n|m$ which is a contradiction. If $m - n(q - 1) > 0$, then $m - n(q - 1)$ is in S but $m - n(q - 1) = m - nq - n < m - nq = r$ which contradicts the fact that r is the smallest element in set S. Therefore $r \leq n - 1$. By combining both cases, it follows that given natural numbers n and m, there exist integers q and r such that $m = qn + r$, where $0 \leq r \leq n - 1$.

Proof: (Uniqueness) Suppose there exist integers q, q_1 r, r_1 such that $m = nq + r$ and $m = nq_1 + r_1$, where $0 \leq r$, $r_1 < n$. We want to show $q_1 = q$ *and* $r_1 = r$ to prove uniqueness. Without loss of generality, suppose $r_1 \geq r$. Since $m = nq + r$ and $m = nq_1 + r_1$, *where* $0 \leq r$, $r_1 < n$, we have $nq - nq_1 = r_1 - r$ which implies that $n|(r_1 - r)$. But since $0 \leq r_1 - r < n$, this implies that $r_1 - r = 0$. Thus $r_1 = r$. Then we have $nq - nq_1 = 0$ which implies that $nq = nq_1$. We divide by n to have $q_1 = q$. Thus, q and r are unique.

Theorem 2.6. *Let a, n, b, r and $k \in \mathbb{Z}$. If $a = nb + r$ and $k|a$ and $k|b$, then $k|r$.*

Proof. Since $k|b$, then $k|nb$ by Theorem 2.3. Since $k|a$ and $k|nb$, then $k|(a - nb)$ by Theorem 2.2. We know $a - nb = r$, therefore k also divides r. □

2.2 Greatest Common Divisor

Definition 2.2. *The Greatest Common Divisor (gcd) of two integers a and b, not both 0, is the largest, positive integer that divides a and b. It is denoted as (a, b).*

We will also note that $(a, 0) = a$, where a is an integer not 0, and $(0, 0)$ does not exist because there are infinitely many integers that divide 0.

Example 2.2. *$(-20, 5) = 5$ and $(12, 18) = 6$.*

Definition 2.3. *Two integers a and b are relatively prime if $(a, b) = 1$.*

Theorem 2.7. *Let a, n, b, and r* $\in \mathbb{Z}$*, where a and b are not both 0. If* $a = nb + r$*, then (a, b) = (b, r).*

Proof. Assume *(a,b) = d and (b,r)* $= d_1$. By definition of gcd, we have $d|a$ and $d|b$. Then by Theorem 2.6, d also divides r. Since d_1 is the gcd of b and r, then $d \leq d_1$. Conversely, we have $d_1|b$. By Theorem 2.3, we have $d|nb$. Since $d_1|r$ and $d_1|(nb + r)$ by Theorem 2.1, then $d_1|a$. Since $d_1|a$ and $d_1|b$, then d_1 is a common divisor of a and b. Since d is gcd of *(a, b)*, then $d_1 \leq d$. Therefore $d_1 = d$. □

Theorem 2.7 allows us to devise a procedure for finding the *gcd(a, b)*. This procedure is called the Euclidean Algorithm.

Euclidean Algorithm. Let a and b be integers not both 0. Since *(a, b) =* $(|a|, |b|)$, assume $a, b > 0$ without loss of generality. Then by applying the Division Algorithm to a and b, we obtain $a = q_1 b + r_1$ *with* $0 \leq r_1 < b$. Now by Theorem 2.7, we continue to apply the Divison Algorithm to b and r_1. Continuing thus, we obtain the sequence $r_1 > r_2 > r_3 > \ldots > r_n$. Since this sequence is decreasing, it must terminate after say n steps with $r_{n+1} = 0$. This idea is sequenced below for best illustration:

$a = q_1 b + r_1$ *with* $0 \leq r_1 < b$

$b = q_2 r_1 + r_2$ *with* $0 \leq r_2 < r_1$

$r_1 = q_3 r_2 + r_3$ *with* $0 \leq r_3 < r_2$

...

$r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}$ *with* $0 \leq r_{n-1} < r_{n-2}$

$r_{n-2} = q_n r_{n-1} + r_n$ *with* $0 \leq r_n < r_{n-1}$

$r_{n-1} = q_{n+1}r_n + 0$

By Theorem 2.7, we have $(a, b) = (b, r_1) = (r_1, r_2) = \ldots (r_{n-1}, r_n) = r_n$, since $r_n | r_{n-1}$.

Example 2.3. *We will find the gcd (24, 36). By the Division Algorithm, 36 = (24 · 1) + 12. Then 24 = (12 · 2) + 0. Then the gcd(24, 36) = 12.*

We can write $r_n = r_{n-2}$ - $q_n r_{n-1}$. By substituting for r_{n-1}, r_{n-2}, ... , r_2, r_1, gathering like terms and simplifying, we can express *gcd(a, b)* as a linear combination of a and b. We state this in the next theorem and illustrate with an example.

Theorem 2.8. *Let a and b* $\in \mathbb{Z}$ *not both 0. Then there exist x and y* $\in \mathbb{Z}$ *such that ax + by= (a, b).*

Example 2.4. *gcd(124, 144).*

144 = (124 · 1) + 20.

124 = (20 · 6) + 4.

20 = (4 · 5) + 0.

Then the gcd(124, 144) = 4.

Retracing our steps, we express the gcd as a linear combination of its terms 124 and 144:

4 = 124 - (20 · 6)

4 = 124 - ((144 - 124) · 6)

4 = 124 - (6 · 144) + (6 · 124)

4 = (- 6) · 144 + (7) · 124

Thus 4 - 144 · x + 124 · y where x = - 6 and y = 7.

In the next theorem we characterize *gcd(a, b)* in the special case of *(a, b) = 1.*

Theorem 2.9. *Let a, b ∈ ℤ. Then (a, b) = 1 if and only if there exist integers x and y such that ax + by = 1.*

Proof. Suppose *(a, b) = 1.* Then by Theorem 2.8, there exist integers *x, y* such that *ax + by = 1.* Conversely, assume there exist integers *x, y* such that *ax + by = 1.* Let *d = (a, b)* so that *d|a* and *d|b.* Then *d|(ax + by)* by Theorem 2.1 and Theorem 2.3, which implies that *d|1.* Then *d = 1* or *d = -1.* Since *d* is the gcd of *a* and *b*, then *d > 0* and therefore *(a,b) = 1.* □

Theorem 2.10. *Let a, b and c ∈ ℤ. If a|bc and (a,b) = 1, then a|c.*

Proof. Let *a, b,* and *c* be integers. Suppose *a|bc* and *(a, b) = 1.* Since *a* and *b* are relatively prime, then there exist integers *x* and *y* such that *ax + by = 1* from Theorem 2.9. We multiply by *c* to have *cax + cby = c.* Since *a|cax* and *a|bc*, then *a|(cax + cby)* by Theorem 2.1. Therefore *a|c.* □

Theorem 2.11. *Let a, b be integers. Then* $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$.

Proof. Let $(a, b) = d$. Then there exist integers x and y such that $ax + by = d$ by Theorem 2.8. We divide by d to obtain $\frac{a}{d}x + \frac{b}{d}y = 1$. Then $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$ by Theorem 2.9. □

3 A Linear Diophantine Equation

A linear Diophantine is a linear equation with integer solutions. We will define the conditions for a linear Diophantine equation with two variables to have a solution.

Theorem 3.1. *Let a, b, and $c \in \mathbb{Z}$ with a and b not both 0. Then there exist integers x and y that satisfy the equation $ax + by = c$ if and only if $(a, b)|c$.*

Proof. Suppose $ax + by = c$ and $(a,b) = d$. Then $d|a$ and $d|b$ which implies that $d|c$ by Theorem 2.3 and Theorem 2.1. Conversely, assume $d|c$. Then there exists an integer k such that $kd = c$. Since $d = (a, b)$, by Theorem 2.3, there exist integers x' and y' such that $ax' + by' = d$. By multiplying by k, we have $kd = k(ax' + by') = a(kx') + b(ky') = c$. Let $x = kx'$ and $y = ky'$. Therefore this satisfies the equation $ax + by = c$. □

The next theorem tells us how to generate infinitely many solutions given one solution (x_0, y_0) of the linear Diophantine equation $ax + by = c$.

Theorem 3.2. *Let a, b, c, x_0 and y_0 be integers with a and b, not both 0, such that $ax_0 + by_0 = c$. Then the integers $x = x_0 + k\frac{b}{(a,b)}$ and $y = y_0 - k\frac{a}{(a,b)}$ for $k \in \mathbb{Z}$ are also solutions to $ax + by = c$.*

Proof. Let k be an integer. By substituting $x = x_0 + k\frac{b}{(a,b)}$ and $y = y_0 - k\frac{a}{(a,b)}$ into the left hand side of the equation $ax + by = c$, then $a(x_0 + k\frac{b}{(a,b)}) + b(y_0 - k\frac{a}{(a,b)}) = ax_0 + k\frac{ab}{(a,b)} + by_0 - k\frac{ab}{(a,b)} = c$ which implies that $ax_0 + by_0 = c$. Then $x_0 = x$ and $y_0 = y$ is a solution to $ax + by = c$. □

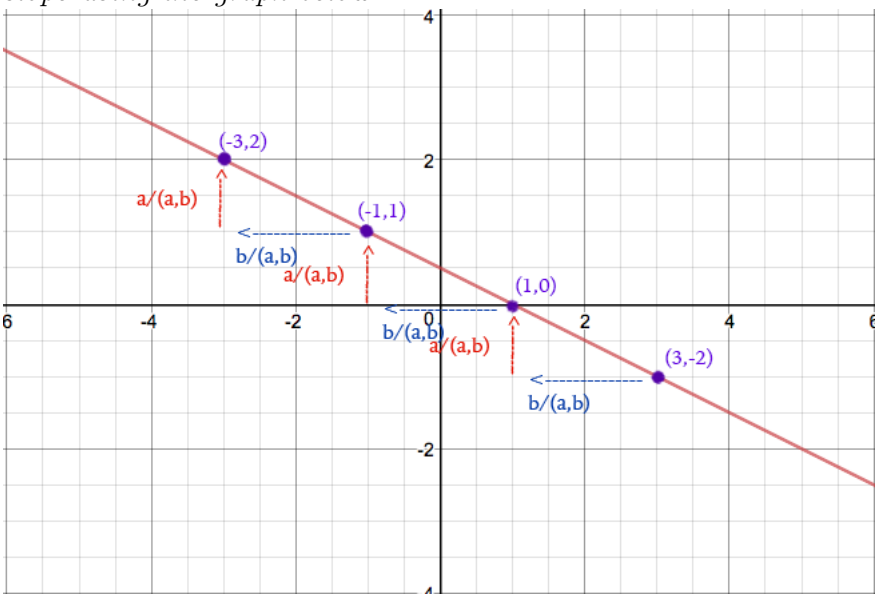
Since we can find solutions of a particular form, it is imperative to consider if we can find solutions that do not satisfy this form. There is no solution not of this form because all solutions are of this form. We shall prove this in the next theorem.

Theorem 3.3. *Let a, b, c, x_0 and y_0 be integers with a and b not both 0 such that $ax_0 + by_0 = c$. Then every solution is of the form $x = x_0 + \frac{kb}{(a,b)}$ and $y = y_0 - \frac{ka}{(a,b)}$ for $k \in \mathbb{Z}$.*

Proof. Suppose (x', y') is another solution such that $ax' + by' = c$. Since we are given $ax_0 + by_0 = c$, we have $a(x' - x_0) + b(y' - y_0) = 0$. This implies that $a(x' - x_0) = b(y_0 - y')$. Since $d = (a, b)$, we have $\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$. Then $\frac{a}{d} \mid \frac{b}{d}(y_0 - y')$. Since $(\frac{a}{d}, \frac{b}{d}) = 1$, by Theorem 2.11, then $\frac{a}{d} \mid (y_0 - y')$. This means that there exists an integer k such that $k\frac{a}{d} = y_0 - y'$. Thus $y' = y_0 - k\frac{a}{d}$. By substituting for $y_0 - y'$ with $k\frac{a}{d}$, we have $b(k\frac{a}{d}) = a(x' - x_0)$, giving us

$x' = x_0 + k\frac{b}{d}$. We were able to express any arbitrary x' and y' solution in this form, therefore this is true for all solutions. □

Example 3.1. *Consider the linear Diophantine $3x + 6y = 3$. Since $(3, 6) = 3$ and $3|3$, this equation has an integer solution (x_0, y_0). We start with any solution, say (1, 0). Then all solutions are of the form $x = 1 + 2k$ and $y = -k$ for some $k \in \mathbb{Z}$. It is clear that each integer solution differs from each other by a slope using the graph below.*



4 Congruence Modulo n, Primes, and Building Blocks

We discussed integer solutions of a linear Diophantine equation because of its similarities with the Chinese Remainder Theorem. Since the Chinese Remainder

Theorem is about solutions of linear congruences, we will first explore the properties of congruence modulo n.

Definition 4.1. *(Congruence mod n) Let a and b* $\in \mathbb{Z}$. *We say a congruent b modulo n, if n|(a - b). This is denoted as denoted as* $a \equiv b(\text{mod } n)$.

Theorem 4.1. *Let a and* $n \in \mathbb{Z}$ *with* $n > 0$, *then* $a \equiv a \ (\text{mod } n)$.

Proof. Let $a \in \mathbb{Z}$ and $n > 0$. Since 0 is an integer and $a - a = 0 = 0 \cdot n$, this implies that $n|(a - a)$. Thus by Definition 4.1, $a \equiv a \ (\text{mod } n)$. □

Theorem 4.2. *Let a, b, and* $n \in \mathbb{Z}$ *with* $n > 0$. *If* $a \equiv b \ (\text{mod } n)$ *then* $b \equiv a \ (\text{mod } n)$.

Proof. Suppose $a \equiv b \ (\text{mod } n)$. Then by Definition 4.1, we have $n|(a - b)$ which implies that there exists an integer k such that $nk = a - b$. We multiply the equation by -1 to obtain $n(-k) = b - a$ where $(-k) \in \mathbb{Z}$. Therefore, again by Definition 4.1, we have $n|(b - a)$ which implies that $b \equiv a(\text{mod } n)$. □

Theorem 4.3. *Let a, b, c and* $n \in \mathbb{Z}$ *with* $n > 0$. *If* $a \equiv b \ (\text{mod } n)$ *and* $b \equiv c \ (\text{mod } n)$, *then* $a \equiv c(\text{mod } n)$.

Proof. Suppose $a \equiv b \ (\text{mod } n)$ and $b \equiv c \ (\text{mod } n)$. Then by Definition 4.1, it follows that $n|(a - b)$ and $n|(b - c)$. By Theorem 2.1, this implies that $n|((a - b) + (b - c))$ which can be reduced to $n|(a - c)$. Therefore $a \equiv c(\text{mod } n)$ by Definition 4.1. □

We can also add, subtract, and multiply congruences with the same modulus much like the divisibility properties we discussed.

Theorem 4.4. *Let a, b, c, d and $n \in \mathbb{Z}$ with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.*

Proof. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|(a - b)$ and $n|(c - d)$. Then by Theorem 2.1, we have $n|((a - b) + (c - d))$. We rearrange the terms to have $n|((a + c) - (b + d))$. Therefore, $a + c \equiv b + d \pmod{n}$. □

The proof of the next theorem is similiar to that of Theorem 4.4. Instead of using Theorem 2.1, we can use Theorem 2.2 and rewrite the equation as $n|((a - c) - (b - d))$. This implies that $a - c \equiv b - d \pmod{n}$.

Theorem 4.5. *Let a, b, c, d and $n \in \mathbb{Z}$ with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.*

Theorem 4.6. *Let a, b, c, d and $n \in \mathbb{Z}$ with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*

Proof. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By the definition of congruence modulo n, this implies that $n|(a - b)$ and $n|(c - d)$. By Theorem 2.3, we have $n|(c(a - b))$ and $n|(b(c - d))$. Then by Theorem 2.1, $n|((a - b)(c) + (b)(c - d))$ which can be reduced to $n|(ac - bd)$. This implies that $ac \equiv bd \pmod{n}$. □

Theorem 4.7. *Given any integer a and any natural number n, there exists a unique integer t in the set* $\{0, 1, 2, \ldots, n - 1\}$ *such that* $a \equiv t \pmod{n}$.

Proof. Given any integer a and natural number n, by the Division Algorithm, there exist unique integers q and t such that $a = nq + t$, *where* $0 \leq t \leq n - 1$. By rearranging the equation, we obtain $a - t = nq$. Since $n|(a - t)$, we have $a \equiv t \pmod{n}$ by the definition of congruence. □

We introduce the definition of a prime number because the Chinese Remainder Theorem requires a system of linear congruences with pairwise relatively prime moduli.

Definition 4.2. *A natural number p greater than 1 is prime if p is not a product of natural numbers less than p.*

Definition 4.3. *A natural number n is composite if n is a product of natural numbers less than n.*

Theorem 4.8. *Let* $n \in \mathbb{N}$. *Then there exists a prime p such that* $p|n$.

Proof. Induction basis: Let $n = 2$, then there exists a prime p that divides 2, namely 2. Induction step: Suppose there exist a prime p such that $p|n$ for some natural number n. We shall prove there exists a prime q such that $q|(n + 1)$. If $n + 1$ is prime, then $q = n + 1$. If $n + 1$ is composite, then we will write $n + 1 = ab$, *where* $1 < a, b < n + 1$. Since a is less than $n + 1$, then there

exists a prime p_1 such that $p_1|a$. By Theorem 2.4, then $p_1|(n + 1)$. We let $p_1 = q$ such that $q|(n + 1)$. □

Theorem 4.9. *(Euclid's Lemma) Let p be a prime number. If $p|a_1 a_2$, then $p|a_1$ or $p|a_2$.*

Proof. Let p be a prime number. Suppose $p|a_1 a_2$. If $p|a_1$, then we are done. If $p \nmid a_1$, then $(a_1, p) = 1$. By Theorem 2.10, then $p|a_2$. □

Theorem 4.10. *(Generalized) Let p be a prime number and n be a natural number. If $p|a_1 ... a_n$ for integer n, then $p|a_i$ for some i, $1 \leq i \leq n$.*

Proof. Suppose p is a prime number and n is a natural number. Induction basis: Let $n = 2$ and $p|a_1 a_2$, then by Theorem 4.9, we have $p|a_1$ or $p|a_2$. Induction step: Suppose $p|a_1 ... a_n$, then $p|a_i$ for some i, $1 \leq i \leq n$. Then we shall prove if $p|a_1 ... a_{n+1}$, then $p|a_j$ for some j, $1 \leq j \leq n + 1$. Since $p|a_1 ... a_n a_{n+1}$, by Theorem 4.9 we have $p|a_1 .... a_n$ or $p|a_{n+1}$. If $p|a_{n+1}$, then $a_j = a_{n+1}$. If $p|a_1 ... a_n$, then $p|a_i$ for some i, $1 \leq i \leq n$ by the induction step. Thus this result holds for $n + 1$. □

The next few theorems connect solutions of a linear congruence to solutions of its linear Diophantine equation.

Theorem 4.11. *Let a, b, and n be integers with $n > 0$. The congruence $ax \equiv b \pmod{n}$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.*

Proof. Assume $ax \equiv b \pmod{n}$ has a solution, say x_0. By definition of congruence modulo n and Theorem 2.2, $n|(ax_0 - b)$ and $n| -(ax_0 - b)$. Then there exists an integer y_0 such that $ny_0 = b - ax_0$. By rearranging, we have $ax_0 + ny_0 = b$. Conversely, assume there exist integers x_0 and y_0 such that $ax_0 + ny_0 = b$. We rearrange the equation to obtain $ax_0 - b = n(-y_0)$. Since $n|(ax_0 - b)$, then $ax_0 \equiv b \pmod{n}$. Therefore $x = x_0$ is a solution. □

Theorem 4.12. *Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n)| b$.*

Proof. The congruence $ax \equiv b \pmod{n}$ has a solution if and only if $ax + ny = b$ has a solution by Theorem 4.11. The equation $ax + ny = b$ has a solution if and only if $(a, n)|b$ by Theorem 2.8. Thus $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n)|b$. □

Theorem 4.13. *Let a, b, and n be integers with $n > 0$. Let x_0 be a solution of $ax \equiv b \pmod{n}$. Then all solutions for $ax \equiv b \pmod{n}$ are of the form $x_0 + (m\frac{n}{(a,n)}) \pmod{n}$, $m = 0, 1, 2, \ldots (a, n) - 1$.*

Proof. Assume x' is any solution to $ax \equiv b \pmod{n}$. Then we have $ax' \equiv b \pmod{n}$ and $ax_0 \equiv b \pmod{n}$. Then by setting the equations together, we obtain $ax' \equiv ax_0 \pmod{n}$. By definition of congruence modulo n, then $n|(ax' - ax_0)$. Let $d = (a, n)$ so that $\frac{n}{d}|\frac{a}{d}(x' - x_0)$. Since $(\frac{a}{d}, \frac{n}{d}) = 1$, then $\frac{n}{d}|(x' - x_0)$ by Theorem 2.11. Assume $x' > x_0$ so that $x' - x_0 > 0$. By the

definition of divisibility, there exists a positive integer k such that $k\frac{n}{d} = x'$ - x_0. We rewrite the equation so that $x' \equiv x_0 + k\frac{n}{d}$ *(mod n).* Let's assume $k \geq d$. Then by the Division Algorithm, there exist integers q and r such that $k =$ $q \cdot d + r$, *where* $0 \leq r \leq d$ - *1.* Then $k \cdot \frac{n}{d} \equiv q \cdot d \cdot \frac{n}{d} + r \cdot \frac{n}{d} \equiv \frac{rn}{d}$, where $0 \leq r \leq d$ - *1.* This implies that $x' \equiv x_0 + m\frac{n}{d}$*(mod n)* for some integer m, $0 \leq m \leq d$ - *1.* By direct substitution we can verify that $x_0 + (m\frac{n}{(a,n)})$ *(mod n), m = 0, 1, 2, ..., (a, n)* - *1* are solutions to $ax \equiv b$ *(mod n).* Therefore all solutions for $ax \equiv b$ *(mod n)* are of the form $x_0 + (m\frac{n}{(a,n)})$ *(mod n), m = 0, 1, 2, ..., (a, n)* - *1.* □

5 The Chinese Remainder Theorem

The goal of this section is to prove the Chinese Remainder Theorem and illustrate it with an example.

Theorem 5.1. *Let a, b, m and n be integers with* $m > 0$ *and* $n > 0$*. Then the system* $x \equiv a$ *(mod n),* $x \equiv b$ *(mod m) has a solution if and only if* $(n, m)|(a - b)$*.*

Proof. Let *a, b, m* and *n* be integers with $m > 0$ and $n > 0$ and suppose there is a solution to the system $x \equiv a$ *(mod n)* and $x \equiv b$ *(mod m).* We know $n|(x - a)$ and $m|(x - b)$. Let $d = (n, m)$. Since $d|n$ and $d|m$, then by Theorem 2.4, we have $d|(x - a)$ and $d|(x - b)$. By Theorem 2.2, then $d|((x - b) - (x - a))$ which is reduced to $d|(a - b)$. Conversely, suppose $(n, m)|(a - b)$. By Theorem 4.12, there

exists integer x_0 such that $mx_0 \equiv (a - b) \pmod{n}$. By rewriting the equation, we obtain $mx_0 + b \equiv a \pmod{n}$. It is also clear that $mx_0 + b \equiv b \pmod{m}$, thus $x = mx_0 + b$ is a solution to the system. □

Theorem 5.2. *Let a, b, m and n be integers with $m > 0$, $n > 0$ and $(n, m) = 1$. Then the system $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$ has a unique solution modulo mn.*

Proof. *Since $(n, m) = 1$* and $(n , m) | (a - b)$, by Theorem 5.1, the system $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ has a solution say x_0. Let $x' \equiv a \pmod{n}$ and $x' \equiv b \pmod{m}$ be another solution to the system. Then we obtain $x_0 - x' \equiv 0 \pmod{n}$ and $x_0 - x' \equiv 0 \pmod{m}$. Since m and n both divide $x_0 - x'$ and $(m, n) = 1$, we have $mn | (x_0 - x')$ by Theorem 2.10. Therefore $x_0 \equiv x' \pmod{mn}$ is the unique solution. □

Lemma 5.3. *Suppose $(n_1, n_2, \ldots, n_k)$ are pairwise relatively prime, that is where $(n_i, n_j) = 1$ for all $1 \leq i \leq k$. Then $(n_1 n_2 \ldots n_{k-1}, n_k) = 1$.*

Proof. Suppose $(n_1 n_2 \ldots n_{k-1}, n_k) = d$. If $d > 1$, then there exists a prime p such that $p | d$. Then $p | n_k$ and $p | n_1 \ldots n_{k-1}$. By Theorem 4.9 , we have $p | n_j$ for some j, $1 \leq j \leq k - 1$. This implies that $(n_i, n_k) \geq p > 1$ which is a contradiction since n_i and n_k are relatively prime. Therefore $(n_1 \ldots n_{k-1}, n_k) = 1$. □

Theorem 5.4. *The Chinese Remainder Theorem. Suppose n_1, n_2 .... n_L are positive integers that are pairwise relatively prime, that is where $(n_i, n_j) = 1$ for i*

$\neq j$, $1 \leq i, j \leq L$. *Then the system of L congruences* $x \equiv a_1$ *(mod* n_1*),* $x \equiv a_2$ *(mod* n_2*), ...,* $x \equiv a_L$ *(mod* n_L*) has a unique solution modulo the product* $n_1 n_2 n_3 \ldots n_L$.

Proof. Suppose n_1, n_2, ..., n_L are positive integers that are pairwise relatively prime. We shall prove by induction. Induction basis: Let $L = 2$. Since $(n_1, n_2) = 1$, the system $x \equiv a_1$ *(mod* n_1*)* and $x \equiv a_2$ *(mod* n_2*)* has a unique solution modulo the product $n_1 n_2$ by Theorem 5.2. Induction step: Suppose the system of L - *1* congruences $x \equiv a_1$ *(mod* n_1*),* $x \equiv a_2$ *(mod* n_2*),* ..., $x \equiv a_{L-1}$ *(mod* n_{L-1}*)* has a unique solution modulo the product $n_1 \ldots n_{L-1}$ say x_0. Then we have $x \equiv x_0$ *(mod* $n_1 n_2 \ldots n_{L-1}$*).* We shall prove the result is true for L congruences $x \equiv a_1$ *(mod* n_1*),* $x \equiv a_2$ *(mod* n_2*),* ..., $x \equiv a_{L-1}$ *(mod* n_{L-1}*),* $x \equiv a_L$ *(mod* n_L*),* where $(n_i, n_j) = 1$ for all i, j such that $1 \leq i, i \leq L$. Since n_1, n_2,..., n_{L-1}, n_L are pairwise relatively prime, it follows that the product $n_1 n_2 \ldots n_{L-1}$ is relatively prime to n_L by Lemma 5.3. By applying Theorem 5.2 to the pairs of congruences $x \equiv x_0$ *(mod* $n_1 n_2 \ldots n_{L-1}$*)* and $x \equiv a_L$ *(mod* n_L*)*, it follows that this system has a unique solution modulo $n_1 n_2 \ldots n_{L-1} n_L$, say x'. Then x' is the unique solution modulo the product $n_1 n_2 \ldots n_L$ to the system: $x \equiv a_1$*(mod* n_1*),* $x \equiv a_2$ *(mod* n_2*), ...,* $x \equiv a_L$ *(mod* n_L*).* □

Let's illustrate the Chinese Remainder Theorem with an example.

Example 5.1. *Suppose it is Easter morning and the Easter Bunny has left*

behind eggs. By noon, all eggs are brought together by Sally, Billy, and Ann. Sally notices that all eggs can be sorted into groups of 13 with a remainder of 5. Billy observes that all eggs can be divided into groups of 12 with a remainder of 7. Then Ann sees that all eggs can be evenly distributed into groups of 11 with no remainder. What is the least amount of eggs? We see that 13, 12, and 11 are pairwise relatively prime so by the Chinese Remainder Theorem, the system $x \equiv 5 \pmod{13}$, $x \equiv 7 \pmod{12}$ *and* $x \equiv 0 \pmod{11}$ *has a solution modulo the product of (13)(12)(11), or 1716.*

We know $x \equiv 5 \pmod{13}$ *implies that* $13|(x - 5)$. *Using the definition of divisibility, there exists an integer k such that* $13k = x - 5$, *or if we rewrite it,* $x = 13k + 5$. *Now we can replace x so that* $13k + 5 \equiv 7 \pmod{12}$. *We reduce to have* $k \equiv 2 \pmod{12}$ *or* $k = 12m + 2$. *We substitute for k in the original equation* $x = 13k + 5$ *to obtain* $x = 13(12m + 2) + 5$ *which is reduced to* $x = 156m + 31$. *We substitute this equation into the last congruence to have* $156m + 31 \equiv 0 \pmod{11}$ *which is reduced to* $m \equiv 1 \pmod{11}$. *This implies that* $m = 1 + 11j$ *for some integer j. We substitute m into* $x = 156m + 31$ *to obtain* $x = 156(1 + 11j) + 31$ *or* $x = 1716j + 187$.

Any solution of the form $x = 1716j + 187$, *is a solution to the system of congruences. However the least solution is* $187 \pmod{1716}$. *Therefore, Sally, Billy and Ann must have at least 187 eggs!*

6 Applications and Further Research

For applications of the Chinese Remainder Theorem, we can simultaneously compute unique solutions to multiple systems of pairwise relatively prime congruences with pairwise relatively moduli. Any parallel process that use systems of linear congruences where all moduli are pairwise relatively prime can map data to each unique solution without data interception.

References

[1] David C. Marshall, E. O. and Starbird, M. (2007). *Number Theory Through Inquiry*, volume 1 of *1*. The Mathematical Association of America, Washington, DC 20090-1112, 1 edition.