12-2021

The Chinese Remainder Theorem

Carol S. Jackson

THE CHINESE REMAINDER THEOREM

By

Carol S. Jackson

B.A., University of St. Francis, 2014

Thesis

Submitted In partial fulfillment of the requirements

For the Degree of Master of Science,
With a Major in Mathematics

Governors State University

University Park, IL 60484

2021

Acknowledgements

I would like to express my sincerest gratitude to Dr. Jing Zhang for her continued patience, support and guidance in the completion of this project. I would also like to extend my appreciation to Dr. Tamulis and Dr. Lyne for being on the committee to review this project.

Special thanks are due to my wonderful husband, Kendall Jackson for his love, encouragement and assistance while I pursued my educational goals.

Abstract

The oldest remainder problems in the world date back to 3rd century China. The Chinese Remainder Theorem was used as the basis in calendar computations, construction, commerce and astronomy problems. Today, the theorem has advanced uses in many branches of mathematics and extensive applications in computing, coding and cryptography. The Chinese Remainder Theorem is an excellent example of how mathematics that emerged in the 3rd century AC has developed and remains relevant in today's world. This paper will explore the historical development of the Chinese Remainder Theorem along with central properties of linear congruences. In addition to providing a historical overview of the Chinese Remainder Theorem, this paper will examine several modern applications of the Chinese Remainder Theorem.

Contents

Acknowledgement …… iii.

Abstract ……. iv.

List of Symbols ……. vi.

1 Introduction 1

1.1 Origins of the Chinese Remainder Theorem ……..... 1

1.2 Migration of the Chinese Remainder Theorem to India ……. 5

1.3 Migration of the Chinese Remainder Theorem to Europe ……... 6

2 Properties of Congruences and Congruence Classes 8

3 Proof of the Chinese Remainder Theorem 13

4 Applications of the Chinese Remainder Theorem 19

4.1 The RSA Cryptosystem and the Chinese Remainder Theorem …… 20

4.2 Chinese Remainder Theorem Based Threshold Cryptography …… 27

4.3 Illustration of Asmuth Bloom Threshold Secret Sharing Scheme …… 30

5 Conclusion 32

6 References 34

List of Symbols

Symbol	Definition
$\mathbb{N}$	Set of Natural Numbers
$\mathbb{Z}$	Set of Integers
$\mathbb{Q}$	Set of Rational Numbers
$\mathbb{R}$	Set of Real Numbers
$\mathbb{C}$	Set of Complex Numbers
(a, b)	The greatest common divisor of a and b
$a\|b$	a divides b

1. Introduction

A vital problem in elementary number theory concerns the solution to systems of congruence equations. Congruence, or modular arithmetic is a simple, powerful and enormously useful tool in the study of number theory. The method for solving systems of linear congruences, or the Chinese Remainder Theorem (CRT), provides unique solutions to simultaneous linear congruences with coprime moduli. Today, the CRT has applications in every area of mathematics. In particular, it is used extensively in computer science. For example, internet cryptography encodes numbers using mathematics that has its origins in the Chinese Remainder Theorem. This paper will examine the Chinese Remainder Theorem, the concept of a congruence and congruence classes along with their properties and some cryptography applications that utilize the CRT.

1.1 Origins of the Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) was formulated in ancient China and first recorded in the 3rd century (Kangsheng, 1987). The CRT was developed to assist with practical problems that arose in astronomy, construction and commerce. The Chinese used the algorithm to calculate calendars, compute the number of soldiers when lined up in different configurations, or constructing the wall of a building or the base of a house. The earliest example of the Chinese Remainder Theorem appeared in the 3rd century book Sun Zi Suanjing (*Master Sun's Mathematical Manual)* by Chinese mathematician Sun Zi Suanjing (Kangsheng,1987, p.1).

According to Shen Kangsheng (1987), a translated problem from *Master Sun's Mathematical Manual (problem 26, Volume 3)* reads as follows:

> "There are certain things whose number is unknown. A number is repeatedly divided by 3, the remainder is 2; divided by 5, the remainder is 3, and divided by 7, the remainder is 2. What will the number be?"

From the given information we can construct three equations:

$$x = 3n + 2\,, \qquad x = 5m + 3\,, \qquad x = 7l + 2$$

The equations form the following congruences:

$$x \equiv 2\ (mod\ 3)\ , x \equiv\ 3\ (mod\ 5)\ , x \equiv 2\ (mod\ 7)$$

For a system of equations such as these, the Chinese Remainder Theorem provides a unique solution up to a certain modulus. The Chinese Remainder Theorem (CRT) can determine an integer from its residues modulo by a set of pairwise relatively prime moduli.

One of the earliest applications of the CRT arose from the computation of calendars in ancient China. The Chinese calendar which marks seasons and holidays in China, is based on lunar and solar elements. The Chinese calendar considers both the moon's orbit around the earth and the earth's 365-day orbit around the sun. The winter solstice typically marks the shortest day of the year and the longest night. The winter solstice occurs in the Northern Hemisphere when the height of the sun is the smallest in the northern hemisphere where China is located, shines directly on the Tropic of Capricorn, and is most oblique to the northern hemisphere. In the Northern Hemisphere, it takes place between December 20 and 23, depending on the year. The winter solstice is the turning point of the sun's southward journey. After this day, it will go "turning back". The direct sun will begin to move northward from the Tropic of Capricorn (23°26′S), and daytime in the northern hemisphere will increase day by day. The winter solstice, as an important node of China's twenty-four solar terms, is the day with the shortest day and the longest night in

the region north of the earth's equator. Even though in astronomy, the winter solstice is a moment when the path of the sun in the sky is farthest south in the Northern Hemisphere, ancient Chinese considered the entire day as the winter solstice, called "Dong Zhi" (冬至, which means Winter Arrives).

In modern astronomy an epoch is an instant of time or date selected as a point of reference. The assumption of ancient Chinese almanacs before 1281 was that celestial motions were cyclic, and an epoch was chosen to be the beginning of a grand cycle (Liu, 2018). *Shàngyuán* was an epoch at midnight on a day in a year and when a lunar conjunction, winter solstice, the beginning of an eclipse cycle occurred. A lunar conjunction is an astronomical event which the earth, moon and sun lie approximately in a straight line and it is often referred to as the new moon. Chinese almanacs typically took the winter solstice as the beginning of a calendar year (Liu, 2018). In ancient time, Chinese used 60 days (or years) as a period to record days (or years) starting from Jiazi to the end of Guihai. Sixty days are a period (or a week), and the recording was repeated. "If Winter Solstice of a certain year occurred r_1 days after *shangyuan* and r_2 days after the new moon, then that year was N years after *shangyuan*; hence arose the system of congruences:

$$aN \equiv r_1 \ (mod\ 60) \qquad aN \equiv r_2 \ (mod\ b)$$

where *a* is the number of days in a tropical year and *b* the number of days in a lunar month" (Ding et al., 1996, p.13).

The CRT offered a simple method of determining the solution to this type of simultaneous congruences. While the CRT appeared in ancient texts as early as the 3rd century, a complete solution for solving linear congruences was not given until much later. A generalized solution for the CRT appeared in the mid thirteenth century (Joyce, 2000). The generalized method for solving

systems of linear congruences was written by Qin Jiushao in 1247 and published in a comprehensive book of Chinese mathematics titled, *Mathematical Book in Nine Chapters*. "In the first section he presents a remarkable generalization of the Chinese Remainder Theorem, which allowed for congruences to be solved even if the moduli were not relatively prime. Qin's method (which he claimed he learned from calendar experts… would be independently invented in the west nearly six hundred years later by Gauss and Legendre" (China and India, 2009, P.66). The CRT algorithms worked on a counting board with rods that represented numbers, to find the modular multiplicative inverse of a given congruence. For cases where the moduli were not relatively prime, his method looked for common factors to reduce the moduli. Qin Jiushao then applied a method of continued division (Euclidian algorithm) to solve the resulting system of congruences (Joyce, 2000). The Euclidian algorithm is a computational process that computes the greatest common divisor of two positive integers. It's a very old method that first appeared in Euclid's Elements, which was written approximately 300 BC. In this method, long division is repeated, using the quotient and remainder. The method is exhausted when the remainder is zero and the greatest common divisor is the last non-zero remainder (Burton, D. 2011, P.34) The Euclidian algorithm has been used for centuries to find solutions to Diophantine equations.

1.2 Migration of Chinese Remainder Theorem to India

Chinese mathematics eventually migrated to surrounding Indian and Islamic cultures (Films Media Group, 2008). Between 500 A.D. and 1200 A.D. Hindu mathematicians used the CRT to make advances in their study of intermediate analysis (Kangsheng, 1987). Ibn Tahir (930 -1087 A.D), an Islamic mathematician, was the first to explain that when solving systems of congruences, a

necessary and sufficient condition on the moduli was that they be pairwise relatively prime (Ing, 2003).

In the 6th century, Aryabhata, the first of great Hindu mathematicians, gave what amounts to a complete algorithm for solving pairwise relatively prime systems of linear congruences. Aryabhata, used the algorithm to explore positive integer solutions to equations of the form $ax + c = by$, where $a, b, c \in \mathbb{Z},\ a > b$ and $(a, b) = 1$. The Aryabhata algorithm requires a repeated division method, (Euclidian algorithm), to arrive at a solution to the proposed equations. The method was called kuttaka, which translates as "pulverize" in reference to the continued division that is needed to obtain successively smaller remainders (Kangsheng, 1987, p.287). It is Aryabhata's algorithm that more closely resembles the modern form of the Chinese Remainder Theorem found in undergraduate textbooks. Aryabhata's algorithm was essential in the development of Hindu intermediate analysis, more commonly referred to today as the method of continued fractions (Matkovic, 1988).

Continued fractions express an arbitrary real number as an integer plus a series of nested fractions. Continued fractions have the general form $a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_4}{a_4 + \ddots}}}}$, where a_i and b_i are either rational numbers or real numbers. If $a_i \in \mathbb{Z}\ and\ b_i = 1\ \forall\ i$, then the expression is called a simple continued fraction. If the expression contains finitely many terms, then it is called a finite continued fraction; otherwise, it is called an infinite continued fraction (Collins, 1999).

Continued fractions date back to 300 BC, around the time of Euclid and have many applications, one of which involves the solutions to a Pell's equation. Pell's equations are a type of Diophantine

equation of the form $x^2 - dy^2 = 1$. Continued fractions can be used to represent a rational approximation for a real number and in solving linear Diophantine equations.

1.3 Migration of Chinese Remainder Theorem to Europe

The CRT made its way to Europe via India and Persia where it spread into the works of European mathematicians. "The Chinese Remainder Theorem became widely known in Europe through an article published in 1853 and written by Alexander Wylie, titled "Jottings on the science of Chinese arithmetic" (Singh, 2010).

In 1809, while conducting research on the newly discovered Ceres, the largest object in the asteroid belt, Carl Friedrich Gauss rediscovered the Chinese Remainder Theorem (Films Media Group, 2008). One of Gauss' many important contributions to mathematics is his development of the idea of a congruence. On the 1st page of his seminal work on number theory, *Disquisitiones Arithmeticae*, Gauss introduced the concept of congruence and the notation which makes it such a powerful technique. We define division as follows: if *a* and *b* are integers, *a* divides *b* if there is an integer *c* such that $ac = b$. The notation $a|b$ means *a* divides *b*. The greatest common divisor of *a* and *b* is defined as follows: let *a* and *b* be integers such that $a \neq 0$ or $b \neq 0$ then the greatest common divisor of *a* and *b* denote gcd (*a, b*), is a positive integer *d* such that:

$d|a$ and $d|b$ and if $c|a$ and $c|b$, then $c \leq d$. Two integers *a* and *b* are coprime or relatively prime if their greatest common divisor is 1, written $(a, b) = 1$.

Gauss's definition of congruence given below:

$If\ a\ and\ b\ are\ integers\ and\ m > 0, then\ a\ is\ congruent\ to\ b\ modulo\ m\ iif\ m|(a - b).$
$This\ is\ written\ \ a \equiv b\ (mod\ m).$

Two integers are said to be congruent modulo m if their difference is divisible by m. A congruence class of an integer a modulo m is defined to be a set of integers which are congruent to a modulo m. There are exactly m distinct congruence classes given by $0, 1, 2, \ldots, m-1$.

Each integer belongs to one of m congruence (or residue) classes modulo m. An equivalent definition of a congruence, useful for proofs involving congruences is:

$$If\ m|(a-b), then\ there\ exists\ k \in \mathbb{Z}\ such\ that\ a-b=km\ or\ a=b+km.$$

Gauss used congruences to study approximation methods relevant to orbital mechanics (Films Media Group, 2008). Using Gauss's congruence definition, the Chinese Remainder Theorem can be written as:

$Let\ n_1, n_2, \cdots, n_r\ be\ positive\ integers\ such\ that\ gcd(n_i, n_j) = 1\ , \forall\ i \neq j.$
$Then\ the\ system\ of\ linear\ congruences$

$$x \equiv c_1 (mod\ n_1)$$
$$x \equiv c_2 (mod\ n_2)$$
$$x \equiv c_3 (mod\ n_3)$$
$$\cdots$$
$$x \equiv c_r (mod\ n_r)$$

$has\ a\ simultaneous\ solution\ which\ is\ unique\ modulo\ n_1 n_2 \cdots n_r.$

The Chinese Remainder Theorem provides the following solution x to the system of linear congruences:

$Let\ N = n_1 n_2 \cdots n_r\ , then\ a\ solution\ to\ the\ system\ of\ linear\ congruences$:

$x \equiv c_1 (mod\ n_1)$
$x \equiv c_2 (mod\ n_2)$

$x \equiv c_3 (mod\ n_3)$

…

$x \equiv c_r (mod\ n_r)$

$is\ x = c_1 N_1 d_1 + c_2 N_2 d_2 + \cdots + c_r N_r d_r (mod\ N), where\ N_i = \frac{N}{n_i} and\ each\ d_i\ is\ a\ solution$

$of\ the\ equation\ \ N_i x \equiv 1 (mod\ n_i)$.

In section III, a proof of this theorem is derived.

2. Properties of Congruence and Congruence Classes

A congruence of the form $ax \equiv b\ (mod\ m)$, where x is an unknown integer is called a linear congruence in one variable. If x_0 is a solution for a linear congruence, then all integers x_i such that $x_i \equiv x_0\ (mod\ m)$ are solutions of the linear congruence. Also, $ax \equiv b\ (mod\ m)$ is equivalent to a linear Diophantine equation i.e., there exist an integer *y* such that $ax - my = b$.

A congruence modulo m also forms an equivalence relation. That is, for all $a, b, c \in \mathbb{Z}$, the following hold:

1. $Reflexive$: $a \equiv a\ (mod\ m)$
2. $Symmetric$: $if\ a \equiv b\ (mod\ m)\ , then\ b \equiv a\ (mod\ m)$
3. $Transitive$: $if\ a \equiv b\ (mod\ m)\ and\ b \equiv c\ (mod\ m)\ , then\ a \equiv c\ (mod\ m)$

Proof:

1. m|(a − a) since a − a = 0 and 0 is divisible by any nonzero integer. Therefore, a ≡ a(mod m).

2. Suppose a ≡ b (mod m) ⇒ m|(a − b). Therefore, m|(−1)(a − b) or m|(b − a). ⇒ b ≡ a (mod m).

3. Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow m|(a-b)$ and $m|(b-c)$.

   Now, using the linear combination theorem $\Rightarrow m|(a-b+b-c)$ or $m|(a-c)$
   $\Rightarrow a \equiv c \pmod{m}$.

Congruences of the same modulus share many of the same properties as equalities. They can, to a large extent, be manipulated like ordinary equations. Congruences of the same moduli can be added, multiplied, taken to a fixed positive integral power and obey the transitive law (Childs, 2009, p.67), i.e., for any $a, b, c, d \in \mathbb{Z}$ and $m > 0$ we have:

- **Adding/subtraction congruences**:

$If\ a \equiv b\ (mod\ m)\ and\ c \equiv d\ (mod\ m), then\ \ a + c \equiv b + d\ (mod\ m)$.

- **Multiplying congruences:**

$If\ a \equiv b\ (mod\ m)\ and\ c \equiv d\ (mod\ m), then\ \ ac \equiv bd\ (mod\ m)$.

- **Taking congruences to the k-th power:**

$If\ a \equiv b\ (mod\ m)\ and\ k \in \mathbb{N}, then\ a^k \equiv b^k\ (mod\ m)$.

Congruence Modulo m Addition Proof:

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then by definition $\exists\ k_1, k_2 \in \mathbb{Z}$
s.t. (i) $a - b = k_1 m$ and (ii) $c - d = k_2 m$.
Adding equations (i) and (ii) $\Longrightarrow (a + c) - (b + d) = (k_1 + k_2)m$.
Now, let $k = k_1 + k_2 \Longrightarrow (a + c) - (b + d) = km \ \Longrightarrow\ a + c \equiv b + d \pmod{m}$. ■

Congruence Modulo m Multiplication Proof:

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then by definition $\exists, k_1, k_2 \in \mathbb{Z}$ s.t.
(i) $a - b = k_1 m$ and (ii) $c - d = k_2 m$.
Now consider $ac - bd = ac - cb + cb - bd$

$$= c(a - b) + b(c - d)$$
$$= ck_1 m + ck_2 m$$

$= m(ck_1 + ck_2)$, where $c, k_1, k_2 \in \mathbb{Z}$.

Let $k = (ck_1 + ck_2)$ for the above $c, k_1, k_2 \in \mathbb{Z}$,

$\Longrightarrow ac - bd = mk \Longrightarrow ac \equiv bd \pmod{m}$, where $a, b \in \mathbb{Z}$. ■

Congruence Modulo m to the k-th Power Proof:

Suppose $a \equiv b \pmod{m}$, where $a, b \in \mathbb{Z}$, then $\exists\ k_1 \in \mathbb{Z}$ s.t. $a - b = k_1 m$.

Now consider $(a^k - b^k) = (a - b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + b^{k-1}\right)$ … (1)

Substitute $a - b = k_1 m$ into equation (1)

$\Longrightarrow (a^k - b^k) = k_1 m\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + b^{k-1}\right)$

Let $r = k_1\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + b^{k-1}\right), r \in \mathbb{Z}$

$\Longrightarrow (a^k - b^k) = rm$, therefore $m \mid (a^k - b^k)$

$\Longrightarrow a^k \equiv b^k \pmod{m}$. ■

Another important property of congruence modulo m is the following;

If $a \equiv b \pmod{m}$ *and* $n \mid m \Rightarrow m = n \cdot k$ where $k \in \mathbb{Z}$, *then* $a \equiv b \pmod{n}$.

Proof:

Suppose $a \equiv b \pmod{m}$ and $n \mid m$, then by the definition of congruence and divisibility

$\Longrightarrow \exists\ k_1, k_2 \in \mathbb{Z}$ such that $a - b = mk_1$ and $m = nk_2$; by subsitution

$\Longrightarrow a - b = (nk_2)k_1$ or $a - b = nk$, where $k = k_1 k_2 \Longrightarrow a \equiv b \pmod{n}$. ■

Example: $5 \equiv 1 \pmod{4}$ and since $2 \mid 4 \Rightarrow 5 \equiv 1 \pmod{2}$.

The existence of an inverse in ordinary arithmetic, can similarly be found in modular arithmetic, under certain constraints. In basic arithmetic, the multiplicative inverse of a non-zero real number *x* is defined as another number x^{-1}, such that $x \cdot x^{-1} = 1$.

Generally, except for 0, multiplicative inverse exists over the real numbers. For example, the inverse of 2 is $\frac{1}{2}$ since $2 \cdot \frac{1}{2} = 1$. Conversely, inverses generally do not exist over the integers.

For example, 3 cannot be multiplied by another integer to give 1. However, inverses exist for modulo a relatively prime number. The multiplicative inverse of "*a* modulo *m*" exists if and only if *a* and *m* are relatively prime (i.e., if gcd (*a*, *m*) = 1). The multiplicative inverse of an integer *a* modulo *m*, is defined as an integer *b*, such that $ab \equiv 1 \ (mod\ m)$.

Modular Multiplicative Inverses:

$Let\ a, m\ be\ positive\ integers\ such\ that\ gcd(a, m) = 1.$

$Then\ a\ has\ a\ multiplicative\ inverse\ modulo\ m, and\ it\ is\ unique\ modulo\ m.$

$In\ other\ words, a \in \mathbb{Z}\ is\ invertable\ mod\ m, if\ and\ only\ if\ the\ gcd(a, m) = 1.$

Proof:

$\Rightarrow$

Suppose a is invertable mod m and $m > 1$, then $\exists\ x \in \mathbb{Z}$ s. t. $ax \equiv 1 (\text{mod } m)$.

$\Rightarrow m | ax - 1$

$\Rightarrow ax - my = 1$ for $y \in \mathbb{Z}$.

Let $d = \gcd(a, m)$, then $d|a$ and $d|m$ so,

$d|(ax - my)$

$\Rightarrow d|1$

$\Rightarrow \gcd(a, m)|1$

$\Rightarrow \gcd(a, m) = 1$.

$\Leftarrow$

Now, Bezout's Identity states:

If the greatest common divisor of a and m is d, then $ax + my = d$ for x and $y \in \mathbb{Z}$: (Childs, 2009, P.37).

Suppose $\gcd(a, m) = 1$, then by Bezout's Identity $\exists\ x, y \in \mathbb{Z}$ s. t. $ax + my = 1$

$\Rightarrow ax = 1 - my$

$\Rightarrow ax - 1 = (-y)m$

$\Rightarrow m|ax - 1$

$\Rightarrow ax \equiv 1 \pmod{m}$. ■

Multiplicative inverses play a key role in the CRT algorithm.

Finally, we end with this important cancellation proposition of congruence modulo m;

$\forall\, a, b, c \in \mathbb{Z}, ca \equiv cb \pmod{m} \Leftrightarrow a \equiv b \left(mod \frac{m}{gcd(c,m)}\right)$.

Proof:

$\Rightarrow$

Suppose $ca \equiv cb \pmod{m} \Rightarrow m|c(a-b)$

$\Rightarrow c(a-b) = mk,\ k \in \mathbb{Z}$. Now let $d = \gcd(c, m)$,

$\Rightarrow d|c$ and $d|m \Rightarrow c = dr, m = ds;\ r, s \in \mathbb{Z}$, also $\gcd(r, s) = 1$.

By substitution, $c(a-b) = mk$ reduces to $r(a-b) = ks$.

$\Rightarrow r|ks$ and $s|r(a-b)$.

$s|r(a-b)$ and $\gcd(r, s) = 1$

$\Rightarrow s|(a-b)$ or $(a-b) = sq, q \in \mathbb{Z}$

$\Rightarrow a \equiv b \pmod{s}$

$\Rightarrow a \equiv b \left(\mod \frac{m}{d}\right)$

$\Rightarrow a \equiv b \left(\mod \frac{m}{\gcd(c,m)}\right)$.

$\Leftarrow$

If $a \equiv b \left(\mod \frac{m}{\gcd(c,m)}\right)$, let $d = \gcd(c, m)$ and $e = \frac{m}{\gcd(c,m)}$.

$\Rightarrow m = de$ and $c = df, f \in \mathbb{Z}$

$\Rightarrow (e, f) = 1$.

$\Rightarrow \mathrm{e}|(a-b)$

$\Rightarrow \mathrm{de}|d(a-b)$

$\Rightarrow \mathrm{m}|d(a-b)$

$\Rightarrow \mathrm{m}|df(a-b)$

$\Rightarrow \mathrm{m}|c(a-b)$

$\Rightarrow \mathrm{c}a \equiv \mathrm{cb} \pmod{m}$. ■

From this result, we can cancel a common factor in the linear congruence only if we modify the modulus as prescribed. An application of this result is that if *c* and *m* are relatively prime, we can cancel common factors in the linear congruence and it does not affect the modulo; this result is particularly useful when finding solutions to linear congruences. The statement $ca \equiv cb\ (mod\ m)$, reduces to $a \equiv b\ (mod\ m)$, if the gcd $(c, m) = 1$.

3. Proof of the Chinese Remainder Theorem

Recall the Chinese Remainder Theorem:

Let $n_1, n_2, \cdots, n_r$ *be positive integers such that* $gcd(n_i, n_j) = 1,\ \forall\ i \neq j.$

Then the system of linear congruences

$$x \equiv c_1 (mod\ n_1)$$
$$x \equiv c_2 (mod\ n_2)$$
$$x \equiv c_3 (mod\ n_3)$$
$$\cdots$$
$$x \equiv c_r (mod\ n_r)$$

has a simultaneous solution which is unique modulo N, *where* $N = n_1 n_2 \cdots n_r$.

The following proof, taken from an undergraduate text in elementary number theory (Burton, 2011, p.79), is a constructive proof. The proof allows us to show why the theorem holds and provides an explicit formula for the solution. To construct a solution unique up to the modulo equivalence $n_1 n_2 \cdots n_r$, we begin with *r* natural numbers that are pairwise relatively prime in the stated system of linear congruences.

Proof:

Let $n_1, n_2, \cdots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1 \ , \forall \ i \neq j$.

Suppose $N = n_1 n_2 \cdots n_r$ and for each $k = 1,2,3, \ldots, r$, let $N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$.

N_k is the product of all the integers n_i except n_k. Since by construction n_k is not a factor of the product N_k, we have the $\gcd(N_k, n_k) = 1$.

Now given that $\gcd(N_k, n_k) = 1$, we know that N_k has an inverse modulo n_k. Therefore, it is

Possible to solve the following congruence $N_k x \equiv 1 (\mathrm{mod}\ n_k)$, and we call the unique solution to this congruence x_k. So, by construction we have $x_k N_k \equiv 1 (\mathrm{mod}\ n_k)$.

Now observe $x_k N_k \equiv 0 (\mathrm{mod}\ n_j)$ for $j \neq k$. This is because N_k is the product of all the

n_i except n_k, which means it is a multiple of n_j and therefore congruent to 0 modulo $n_j \ \forall \ j \neq k$.

Let $x = x_1 N_1 c_1 + x_2 N_2 c_2 + \cdots + x_r N_r c_r$. If we compute x modulo n_k, then every term where the subscript $\neq k$, will be 0 from our previous observation. Therefore, $x = 0 + 0 + \cdots + x_k N_k c_k + \cdots + 0 \equiv x_k N_k c_k (\mathrm{mod}\ n_k)$. However, x_k was chosen to satisfy the congruence

$N_k x \equiv 1 (\mathrm{mod}\ n_k)$. Therefore, $x \equiv c_k (\mathrm{mod}\ n_k), \ \forall \ 1 \leq k \leq r$.

This shows that $x = x_1 N_1 c_1 + x_2 N_2 c_2 + \cdots + x_r N_r c_r$ is a solution of the system.

We will prove the uniqueness now.

Proof: Suppose x and y are solutions of the proposed system of congruences.

$\Rightarrow x \equiv c_k (\mathrm{mod}\ n_k)$ and $y \equiv c_k (\mathrm{mod}\ n_k)$, $\forall\ 1 \leq k \leq r$

Using the arithmetic properties of equivalences, we have:

$x - y \equiv 0\ (\mathrm{mod}\ n_k)$, $\forall\ 1 \leq k \leq r$

$\Rightarrow n_k | x - y$

$\Rightarrow (x - y)$ is a multiple of n_k , $\forall\ 1 \leq k \leq r$.

Recall that $N = n_1 n_2 \cdots n_r$, where $n_1, n_2, \cdots, n_r$ are pairwise relatively prime.

$\Rightarrow (x - y)$ is a multiple of N.

$\Rightarrow N | x - y$.

$\Rightarrow x \equiv y (\mathrm{mod}\ N)$. Therefore, the initial pair of congruences are the same modulo N. ■

Thus, given the following system of equations:

$x \equiv c_1 (mod\ n_1)$
$x \equiv c_2 (mod\ n_2)$
$x \equiv c_3 (mod\ n_3)$

c_i	N_i	$^*x_i$	$c_i N_i x_i$
c_1	$N_1 = n_2\, n_3$	x_1	$c_1 N_1 x_1$
c_2	$N_2 = n_1\, n_3$	x_2	$c_2 N_2 x_2$
c_3	$N_3 = n_1\, n_2$	x_3	$c_3 N_3 x_3$

And $N = n_1 n_2 n_3$ with x_i's that satisfy $N_i\, x_i \equiv 1 (mod\ n_i)$; the solution *x* is given by:

$x = \sum_{i=1}^{3} c_i N_i x_i$ modulo *N*.

The following is an illustration of the CRT.

Example 1.

Consider the following congruences:

$$\begin{cases} x \equiv 5(mod\ 11) \\ x \equiv 4\ (mod\ 29) \\ x \equiv 15\ (mod\ 31) \end{cases}$$

Because the moduli are pairwise relatively prime, a unique solution is given by the CRT:

We have $N = 11 \cdot 29 \cdot 31 = 9889$; $c_1 = 5,\ c_2 = 4,\ c_3 = 15;$

$N_1 = 29 \cdot 31 = 899,\ N_2 = 11 \cdot 31 = 341,\ N_3 = 11 \cdot 29 = 319$

Solving the following linear congruences：

$899x_1 \equiv 1\ (mod\ 11)\quad 341x_2 \equiv 1\ (mod\ 29)\quad 319x_3 \equiv 1\ (mod\ 31)$

$\Rightarrow 8x_1 \equiv 1\ (mod\ 11)\quad 22x_2 \equiv 1\ (mod\ 29)\quad 9x_3 \equiv 1\ (mod\ 31)$

$\Rightarrow\quad x_1 \equiv 7\ (mod\ 11),\quad x_2 \equiv 4\ (mod\ 29)\quad x_3 \equiv 7\ (mod\ 31)$

The solution x is as follows:

c_i	N_i	$*x_i$	$c_i N_i x_i$
5	899	7	$5 \cdot 899 \cdot 7 = 31465$
4	341	4	$4 \cdot 341 \cdot 4 = 5456$
15	319	7	$15 \cdot 319 \cdot 7 = 33495$

$$x = c_1 N_1 x_1 + c_2 N_2 x_2 + c_3 N_2 x_2 \ = 31465 + 5456 + 33495$$

$$x = 70416$$

Therefore, 70416 will be a solution to the system of linear congruences. However, the solution is unique modulo 9889.

$\Rightarrow x \equiv 70416\ (mod\ 9889)\ \ or\ \ x \equiv 1193\ (mod\ 9889)$. Therefore, 1193 is the smallest possible positive solution to the system of linear congruences.

Example 2.

Another Chinese remainder problem taken from Burton's Elementary Number Theory textbook (Burton, 2011) reads as follows:

> "A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, 1 pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again, an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?"

From the problem we construct the following linear congruences:

$x \equiv 3\ (mod\ 17),\ x \equiv\ 10\ (mod\ 16),\ x \equiv 0\ (mod\ 15)$.

Because 17, 16 and 15 are pairwise relatively prime, the CRT can be used to solve the system of congruences.

We have $\mathrm{N} = 17 \cdot 16 \cdot 15 = 4080$; $c_1 = 3,\ c_2 = 10,\ c_3 = 0$;

$N_1 = 16 \cdot 15 = 240,\ N_2 = 17 \cdot 15 = 255,\ N_3 = 17 \cdot 16 = 272$

Solving the following linear congruences :

$240x_1 \equiv 1\ (mod\ 17)\quad 255x_2 \equiv 1\ (mod\ 16)\quad 272x_3 \equiv 1\ (mod\ 15)$

$\Rightarrow 2x_1 \equiv 1\ (mod\ 17)\quad 15x_2 \equiv 1\ (mod\ 16)\quad 2x_3 \equiv 1\ (mod\ 15)$

$\Rightarrow x_1 \equiv 9\ (mod\ 17),\ \ x_2 \equiv 15\ (mod\ 16)$ and $\ x_3 \equiv 8\ (mod\ 15)$

The solution x is as follows:

c_i	N_i	$*x_i$	$c_i N_i x_i$
3	240	9	6480
10	255	15	38250
0	272	8	0

$x = c_1 N_1 x_1 + c_2 N_2 x_2 + c_3 N_2 x_2 = 6480 + 38250 + 0 = 44730$

44730 will be a solution to the system of linear congruences. However, our solution is unique modulo 4080; $x \equiv 44730 \ (mod\ 4080)$ or $x \equiv 3930 \ (mod\ 4080)$. Therefore, the pirates stole at least 3930 coins.

If we need to solve a system of congruences where some coefficients on x are not 1, such as:

$$a_1 x \equiv c_1 \ (mod\ n_1)$$
$$a_2 x \equiv c_2 \ (mod\ n_2)$$
$$a_3 x \equiv c_3 \ (mod\ n_3)$$
$$\dots$$
$$a_r x \equiv c_r \ (mod\ n_r),$$

we first need to change the system to the standard form so that all coefficients of x are 1 in the system then apply the formula in CRT.

Example 3.

Solve.

$$2x \equiv 1 \ (mod\ 3)$$
$$4x \equiv 3 \ (mod\ 5)$$
$$5x \equiv 2 (mod\ 7)$$

Recall that $ax \equiv b(mod\ n)$ has a solution iff gcd $(a, n)|b$. Also, if the gcd $(a, n) = c$ and $c|b$ then $c =$ number of solutions for $ax \equiv b(mod\ n)$. Since $(a, n) = 1$ for each of the above congruence equations and 1,2, and 3 are divisible by 1, each equation has one solution. To solve $ax \equiv$

$b\ (mod\ n)$ we need to find the inverse of a modulo n, then multiply both sides of the congruence by that factor.

Congruence	Scalar multiple	Congruence
$2x \equiv 1\ (mod\ 3)$	$2 \cdot 2x \equiv 2 \cdot 1 (mod\ 3)$	$4x \equiv 2\ (mod\ 3) \Rightarrow \quad x \equiv 2\ (mod\ 3)$
$4x \equiv 3\ (mod\ 5)$	$4 \cdot 4x \equiv 4 \cdot 3 (mod\ 5)$	$16x \equiv 12 (mod\ 5) \Rightarrow \quad x \equiv 2\ (mod\ 5)$
$5x \equiv 2\ (mod\ 7)$	$3 \cdot 5x \equiv 3 \cdot 2 (mod\ 7)$	$15x \equiv 6 (mod\ 7) \Rightarrow \quad x \equiv 6\ (mod\ 7)$

4. Applications of the Chinese Remainder Theorem

The CRT has numerous applications in computing, coding and cryptography. Cryptography is a branch of mathematics concerned with protecting information from unauthorized parties through the use of encryption techniques. Secret sharing schemes are a fundamental tool in cryptography and information security. In any secret sharing scheme, the chosen encryption process transforms the communication into a ciphertext before sending to a receiver; the receiver can then recover the secure information by use of a decryption process. One of most popular encryption systems in use today, is the RSA cryptosystem and the Chinese Remainder Theorem plays an important role in its algorithm.

The RSA cryptosystem is commonly used to authenticate digital signatures and protect data such as customer information and transaction data. It can be used to create key exchanges that establish a secure, encrypted communication channel. It has numerous applications in banking, telecommunications and ecommerce. The RSA cryptosystem was created in 1977 by MIT

professors, Ron Rivest, Adi Shamir, and Leonard Adleman; their last names form the acronym RSA. The RSA cryptosystem is one of the first public-key or asymmetric cryptosystems. The algorithm is based on the mathematics of modular exponentiation and relies on the computational difficulty of factoring large integers. Asymmetric cryptosystems require a pair of related keys to operate; the two different but mathematically linked keys are used for the encryption and decryption process (Rivest, R. L., Shamir, A., & Adleman, L., 1978). The publicly disclosed key is accessible by everyone and the private key is known only to the receiver. Using the public key, messages can be encrypted by anyone but can only be decoded with the use of the private key. The public and private keys are based on the product of two relatively large prime integers. The product of two large prime integers, known as semi primes, are easy to construct, but computationally difficult to factor. The RSA method is secure because it is difficult to factor the products of two large primes. "RSA encryption works under the premise that the algorithm is easy to compute in one direction, but almost impossible to reverse" (Lake, 2021). There are three steps in the RSA algorithm: key generation, encryption and decryption. The Chinese Remainder Theorem plays an integral role in the final phase, the decryption or private key process.

4.1 RSA Cryptosystem and the Chinese Remainder Theorem

The function Φ is an important theoretical function called Euler's Phi function. Euler's totient $\Phi(n)$ is defined as the number of positive integers not exceeding *n* that are relatively prime to *n*.

The following definition was taken from Child's *A concrete introduction to higher algebra*:

For each $n \geq 2,\ \Phi(n)$ denotes the number of integers a with $1 \leq a \leq n$ that are coprime to n.

Euler's theorem:

If n is a natural number and a is an integer such that gcd $(a, n) = 1$, then $a^{\Phi(n)} \equiv 1\ (mod\ n)$.

Proof:

Let *a* and *n* be positive integer such that $(a, n) = 1$. Construct a set $\mathcal{S}$ that contain all $x_i \in \mathbb{Z}$ such that $1 \leq x_i < n$ and $x_i's$ are coprime to $n \Longrightarrow \mathcal{S} = \{x_1, x_2, x_3, \dots, x_{\Phi(n)}\}$. Compare $\mathcal{S}$ with the set obtained by multiplying elements of $\mathcal{S}$ by $a \in \mathbb{Z} \Longrightarrow a\mathcal{S} = \{ax_1, ax_2, ax_3, \dots, ax_{\Phi(n)}\}$. Since $(a, n) = 1$, a can be reduced modulo n and a modulo n is invertible. Also, since all $x_i's$ are coprime to *n* and *a* is coprime to *n* so each ax_i is also coprime to *n*. Therefore $a\mathcal{S}$ can also be reduced modulo n.

Construct a set $\mathcal{T}$ such that $\mathcal{T} = \{ax_1(mod\ n), ax_2\ (mod\ n), ax_3\ (mod\ n), \dots, ax_{\Phi(n)}(mod\ n)\}$

If $i \neq j$ and $ax_i \equiv ax_j\ (mod\ n)$, then $x_i \equiv x_j\ (mod\ n)$ since *a* is invertible modulo *n*. We show that the set $\mathcal{T}$ contains exactly $\varphi(n)$ elements. $\mathcal{S}$ and $\mathcal{T}$ have the same number of elements and $\mathcal{T}$ is a subset of $\mathcal{S}$, therefore, $\mathcal{S} = a\mathcal{S} = \mathcal{T}$. Thus, the product of all the elements in the set $\mathcal{T}$ is:

$a^{\Phi(n)}(x_1x_2x_3 \dots x_{\Phi(n)}) \equiv x_1x_2x_3 \dots x_{\Phi(n)}\ (mod\ n)$. Cancelling $(x_1x_2x_3 \dots x_{\Phi(n)})$, we have $a^{\Phi(n)} \equiv 1(mod\ n)$.

A special case of Euler's theorem is Fermat's theorem: $\Phi(n) = n - 1$ iff *n* is prime. This is Euler's theorem when *n* is prime. The proof follows along the same line as the proof of Euler's theorem.

RSA encryption algorithm

- Step 1 (Key Generating Process):

Choose two large prime numbers p and q. Then generate a modulus n such that $n = p \cdot q$. Next generate $\Phi(n)$, where $\Phi(n) = \Phi(pq) = (p-1)(q-1)$.

We choose an exponent e, such that: $1 < e < \Phi(n)$ and the gcd $(e, \Phi(n)) = 1$; e is chosen to be smaller than $\Phi(n)$ to optimize the encryption time. Choosing an e value less than $\Phi(n)$, maximizes the time needed to encipher and thus speeds up decryption. Since e is a freely chosen parameter with the above-mentioned constraints, we know that the inverse of e modulo $\Phi(n)$ exists. The private key d is generated by computing the inverse of e; calculate d such that $ed \equiv 1(\ mod\ \Phi(n))$. To find such a d, the Euclidean algorithm can be used. The public key is made of e and n and the private key consists of d and n, therefore the two keys e and d are the inverse of each other modulo $\Phi(n)$.

Step 2 (Encryption Process):

In phase two, the initial message is converted to numbers. The message can be translated into decimal, binary or hexadecimal notation. One standard method for converting a message to a numerical form is the ASCII encoding system. The ASCII is an encoding system for letters on a keyboard that uses 7-bits. The following is a conversion chart for the ASCII system:

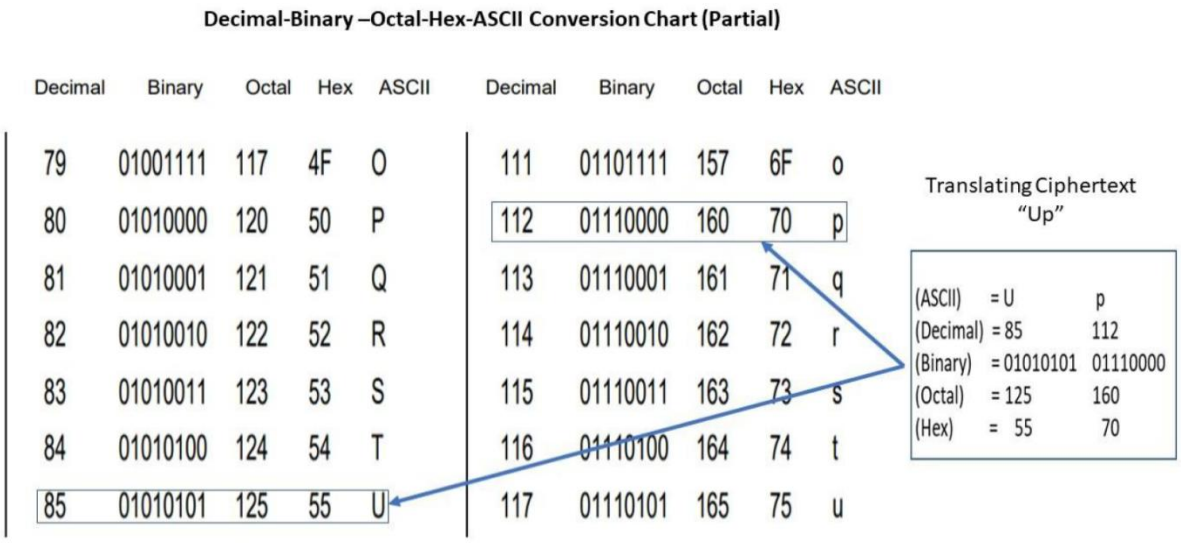

Figure 1

Note: Table of Decimal Binary Octal Hex ASCII Conversion Chart (http://web.alfredstate.edu/faculty/weimandn/miscellaneous/ascii/ASCII%20Conversion%20Chart.pdf)

Once the plaintext is converted into a number or series of numbers *m*, where $0 < m < n$, the number *m* is then transformed into an unreadable ciphertext *C*. The ciphertext *C* is calculated using the encryption equation: $C \equiv m^e (mod\ n)$.

- Step 3 (Decryption Process):

Since (e, $\Phi(n)) = 1$, by Bezout's Identity, there is an integer x such that $ed + \Phi(n)x = 1$.

We can write:

$ed = 1 - \Phi(n)x$. Choosing p and q such that (m, n) =1, by Euler's Theorem,

$m^{\Phi(n)} \equiv 1\ (mod\ n)$. Now, $C^d = m^{ed} = m^{\Phi(n)(-x)}\ m \equiv m\ (mod\ n)$.

In phase three the receiver is given *C*, and must recover *m*. Since the receiver knows the factorization on *n* with the use of the private key (*d*), *m* is recovered using the decryption equation: $m \equiv C^d (mod\ n)$. "By taking advantage of the Chinese Remainder Theorem, the computational effort of the RSA decryption can be reduced significantly. If the two prime numbers P and Q of the modulus *n* are known, it is possible to calculate the modular exponentiation $m \equiv C^d (mod\ n)$ separately by computing m (mod *p*) and m (mod *q*) with shorter exponents. The RSA crypto chip can compute two exponentiations in parallel, as the 1024-bit multiplier core can be split into two 512 bit multipliers. Running the two 512-bit multipliers in parallel allows both CRT related exponentiations to be computed simultaneously. Compared to the non-CRT based RSA decryption performed on an n bit hardware, utilizing the CRT results in a speed-up factor of approximately 3.5" (Grossschadl, 2000).

The RSA algorithm requires two large prime number *p* and *q* to generate the encryption and decryption keys, longer keys provide better security. The current minimum RSA system requirement or lower bound is $p, q > 2^{2048}$ bits and $n > 4096$ bits. Each bit can be represented by a 0 or 1. For a 4096-bit public key $\Longrightarrow 2^{4096} = 10^x$ and $x = 4096 \cdot log\ 2 \approx 1233$. Therefore, a 4096-bit public key contains 1234 digits. This large of an integer is extremely difficult to factor and thus, provides a high degree of security for the encryption process. If $n = p \cdot q$ is known, it is possible to calculate $C = m^e (mod\ n)$ separately by computing *C* (mod *p*) and *C* (mod *q*) with shorter exponents. Then we can use the Chinese Remainder Theorem to solve the resulting system of linear congruences and retrieve m. The following is an illustration of the RSA secret sharing scheme.

Example 4.

Step 1 (Key Generating Process):

John sets up an RSA system with:

Public modulus $n = 19837$ and public encryption key $e = 3$.

He tells no one the unique factorization of 19837. Such that, $p = 83$ and $q = 239$

$\Longrightarrow n = p \cdot q = 19837$ and calculates $\Phi(n)$.

$\Phi(n) = (83 - 1)(239 - 1) = 19516.$

$John's$ private key is found by evaluating ; $3 \cdot d \equiv 1\, mod(19516)$.

Using Euclid's Algorithm, John can calculate *d*. John's private key is $d = 13011$.

Public key (*e*, *n*)	Private key (*d*, *n*)
(3, 19837)	(13011, 19837)

Step 2 (Encryption Process):

Mary sends John the message 307.

The ciphertext *C* is calculated using the public modulus and encryption key and the encryption equation: $C = 307^3\ (mod\ 19837) = 12097$.

John must decrypt Mary's message by evaluating: $m \equiv 12097^{13011}\ (mod\ 19837)$.

Step 3 (Decryption Process):

To decrypt Mary's message efficiently, John uses the CRT:

Restatement of the Chinese Remainder Theorem

$Suppose\ p, q\ are\ relatively\ prime.$

$Then\ x \equiv a\ (mod\ pq)\ \ if\ and\ only\ if$

$x \equiv a\ (mod\ p)$

$x \equiv a\ (mod\ q)$.

John must evaluate $m \equiv 12097^{13011}\ (mod\ 19837)$, however, since he knows $19837 = 83 \cdot 239$, to speed the decryption process, he solves:

$m \equiv 12097^{13011} (mod\ 83)$ and $m \equiv 12097^{13011}\ (mod\ 239)$.

To simplifying the first congruence:

$12097 \equiv 62\ (mod\ 83)$. Using Euler's theorem which states $a^{\varphi(N)} \equiv 1\ (\ mod\ N)$, further reduces the exponent mod $\varphi(83) = 82$.

$\Longrightarrow\ 62^{13011} = 62^{82 \cdot 158} 62^{55}\ (mod\ 83)$

$\Longrightarrow\ 62^{55}\ (mod\ 83)$

A similar argument is made to reduce the second congruence.

$m \equiv 12097^{13011} (mod\ 83)$	$m \equiv 12097^{13011} (mod\ 239)$
$\equiv 62^{13011}\ (mod\ 83)$	$\equiv 147^{13011}\ (mod\ 239)$
$\equiv 62^{55} (mod\ 83)$	$\equiv 147^{159}\ (mod\ 239)$
$\equiv 58\ (mod\ 83)$	$\equiv 68\ \ (mod\ 239)$

Therefore, to decrypt Mary's message, John needs to solve the following system of congruences:

- $m \equiv 58\ (mod\ 83)$

- $m \equiv 68\ (mod\ 239)$

Applying the Chinese Remainder Theorem:

The solution m is as follows:

c_i	N_i	$*x_i$	$c_i N_i x_i$
58	239	58	803996
68	83	72	406368

$m = c_1 N_1 x_1 + c_2 N_2 x_2 \ = 803996 + 406368 = 1210364.$ However, the solution is unique modulo 19837.

$m \equiv 1210364\ (mod\ 19837)$

$\Longrightarrow m \equiv 307\ (mod\ 19837)$

$\Longrightarrow m = 307.$

4.2 Chinese Remainder Theorem Based Threshold Cryptography

Another application of the CRT is the design of threshold cryptography. Threshold cryptography or threshold secret sharing schemes (SSS) plays a vital role in cloud computing, electronic voting and the multi-signature requirements of Bitcoin transactions. In a threshold SSS the secret is compartmentalized or split into parts and distributed among participants. Each piece of the secret is called a share and the person creating the shares is called the dealer. The secret can only be recovered when a predetermined number of shares come together. "Let $\mathcal{K}$ be the set of secrets, $\mathcal{S}$ the set of shares, and $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of *n* participants in secret sharing. When a dealer $\mathcal{D} \notin \mathcal{P}$ wants to share a secret $s_0 \in \mathcal{K}$, he will give each participant $P_i \in \mathcal{P}$ a share $s_i \in \mathcal{S}$.

Later, an authorized subset of participants $\mathcal{A} \subseteq \mathcal{P}$ can determine the secret from the shares they jointly hold" (Liu, Y. 2017). Classified or sensitive information, such as military images, trade secrets, financial reports etc. are typically transmitted using a threshold secret sharing algorithms. One threshold SSS, which utilizes the CRT is the Asmuth-Bloom secret sharing scheme. This scheme was presented in 1983 by Charles Asmuth and Charles Bloom (Asmuth, C., & Bloom, J. 1983). The Asmuth-Bloom SSS uses a special sequence of integers as its parameters which allows for a more robust secret sharing scheme, and is therefore generally considered a more resilient SSS. The Asmuth-Bloom SSS uses a weighted threshold access structure. The weighted threshold allows for a more perfect privacy, meaning no unqualified group of participants can obtain information about the secret. The weighted threshold schemes are essentially a way of modifying the qualified sets of the access structure. In the Asmuth-Bloom SSS, sharing and reconstruction of the secret are done as follows:

Share Distribution:

The dealer shares a secret $\mathcal{S} \in \mathbb{Z}_{m_0}$ among n participants with an authorized threshold value *k*, needed to recover the secret. The dealer selects a prime number $m_0 > \mathcal{S}$ and pairwise relatively prime integers m are chosen for *n* number of shares, such that $m_0 < m_1 < m_2 < \cdots < m_n$.

The following constraints must be satisfied:

$$\beta < \mathcal{S} + \alpha m_0 < \gamma \ ,$$

where $\gamma = m_1 \cdot m_2 \cdot \cdots m_k$, $\beta = m_{k+1} \cdot m_{k+2} \cdot \cdots m_n$ and $\alpha \in \mathbb{Z}$ is a random integer such that the inequality $\beta < \mathcal{S} + \alpha m_0 < \gamma$ is satisfied.

Share of the i^{th} user is calculated as follows:

$$s_i \equiv \mathcal{S} + \alpha m_0 \ (mod\ m_i)$$

Since $m_1, m_2, \cdots, m_n$ are pairwise relatively prime, when the prerequisite number of shares are brought together, we can apply the Chinese Remainder Theorem to solve the system of congruences.

Secret Reconstruction:

Now, for a coalition of t different shares, we consider the system of congruences:

$$\begin{cases} s_i \equiv \mathcal{S} + \alpha m_0 \left(mod\ m_{i_1}\right) \\ \vdots \\ s_t \equiv \mathcal{S} + \alpha m_0 \left(mod\ m_{i_t}\right) \end{cases}$$

By the Chinese Remainder Theorem, since $m_{i_1}, \ldots, m_{i_t}$ are pairwise relatively prime, the system has a unique solution $\mathcal{S}_0$ modulo $m_{i_1}, \ldots, m_{i_t}$. By the construction of our shares, the secret $\mathcal{S}$ is the reduction modulo m_0 of $\mathcal{S}_0$. For example, given a threshold of three, we can use the CRT to solve:

$$s_1 \equiv \mathcal{S} + \alpha m_0 \ (mod\ m_1)$$
$$s_2 \equiv \mathcal{S} + \alpha m_0 \ (mod\ m_2)$$
$$s_3 \equiv \mathcal{S} + \alpha m_0 \ (mod\ m_3)$$

for a solution of the system of equations. Finally, taking the residue modulo m_0 will give us $\mathcal{S}$, thus reconstructing the original secret.

4.3 Illustration of Asmuth-Bloom Secret Sharing Scheme

The following is an example of the Asmuth-Bloom secret sharing scheme.

Example 5.

In this example, 6 secret shares are generated with a recovery threshold of 4 and the chosen secret is $\mathcal{S} = 75$. The prime numbers chosen by the dealer are:

$m_0 = 113$
$m_1 = 127$
$m_2 = 131$
$m_3 = 137$
$m_4 = 139$
$m_5 = 149$
$m_6 = 151$

$\beta = 149 \cdot 151 = 22499$
$\gamma = 127 \cdot 131 \cdot 137 \cdot 139 = 316818291$

α is then chosen to be 3000 thus satisfying the Asmuth-Bloom sequence constraints:

$$\beta < \mathcal{S} + \alpha m_0 < \gamma$$

$$22499 < 75 + 3000 \cdot 113 = 339075 < 316818291$$

The secret shares are computes as follows:

$s_1 = 75 + 3000 \cdot 113 \equiv 112 \ (mod\ 127)$

$s_2 = 75 + 3000 \cdot 113 \equiv 47 \ (mod\ 131)$

$s_3 = 75 + 3000 \cdot 113 \equiv 0 \ (mod\ 137)$

$s_4 = 75 + 3000 \cdot 113 \equiv 54 \ (mod\ 139)$

$s_5 = 75 + 3000 \cdot 113 \equiv 100 \ (mod\ 149)$

$s_6 = 75 + 3000 \cdot 113 \equiv 80 \ (mod\ 151)$

Given C(n, r) = C(6,4) = 15 we consider one possible combination of secret shares among the 15 possible sets of 4:

$s_1 \equiv 112\ (mod\ 127)$

$s_2 \equiv 47\ (mod\ 131)$

$s_3 \equiv 0\ (mod\ 137)$

$s_5 \equiv 100\ (mod\ 149)$

Since 127, 131, 137 and 149 are pairwise relatively prime the CRT can be used to find a unique solution *x* to the system of congruences modulo 339611081. The solution x is as follows:

c_i	N_i	$*x_i$	$c_i N_i x_i$
112	2674103	14	4192993504
47	2592451	47	5726724259
0	2478913	47	0
100	2279269	28	6381953200

$x = c_1 N_1 x_1 + c_2 N_2 x_2 + c_3 N_3 x_3 + c_4 N_4 x_4$

$= 4192993504 + 5726724259 + 0 + 6381953200 = 16301670963$

$x \equiv 16301670963$ modulo 339611081

$x \equiv 339075\ (mod\ 339611081)$

Finally, the residue $(mod\ m_0)$ will give us the original secret.

$s \equiv 339075\ (mod\ 113)$

$s \equiv 75\ (mod\ 113)$; thus, the original secret is 75.

As demonstrated by the following, the secret cannot be determined from a share coalition < 4.

Given:

$s_4 \equiv 54\ (mod\ 139)$
$s_5 \equiv 100\ (mod\ 149)$
$s_6 \equiv 80\ (mod\ 151)$

The CRT yields a unique solution modulo $139 \cdot 149 \cdot 151 = 3127361$

$s \equiv 339075\ (mod\ 3127361)$ or $s \equiv 145686\ (mod\ 3127361)$

Finally, the residue $(mod\ m_0)$ will give us $s \equiv 145686\ (mod\ 113)$

$s \equiv 29\ (mod\ 113)$; whose residue is not the original secret of 75.

In the Asmuth Bloom SSS, m_0 need not be prime, and the scheme works correctly for a composite m_0 as long as m_0 is relatively prime to m_i , $1 \leq i \leq n$ (Kaya, 2007). The Asmuth Bloom schemes works because of the initial sequence constraint on the pairwise relatively prime m_i integers. The lower and upper bound on the modulo inequality, establishes the threshold needed for secret recovery. Any residues retrieved from secret shares less than the designated recovery interval, fall outside the modulo inequality solution region and thus will not recover the secret. That is to say, with an authorized threshold value k, the secret cannot be recovered with $k - 1$ shares.

5. Conclusion

The Chinese Remainder Theorem first appeared in the 3rd century as a method for solving problems involving calendar computations, commerce, astronomy and solider counting. It has evolved to become one of the most useful tools in number theory. The CRT can be extended from its original definition involving integers to other fields such as Rings and integral domains. It has many modern-day uses in computer science and plays an integral role in signal processing as well as information security. Here we have discussed a brief history of the theorem, some properties of congruences as well as a few cryptography applications using the CRT. This topic is interesting and there are many more applications of the CRT. The Chinese Remainder Theorem is an excellent example of how mathematics that emerged from the 3rd century has developed and remained relevant and impactful in today's world. Ron Rivest, Adi Shamir, and Leonard Adleman

won the 2002 A. M. Turing Award, the “Nobel Prize of Computing”, for their contributions to public key cryptography which is an application of Euler’s Theorem and Chinese Reminder Theorem (Notices, 2003).

References

Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE transactions on information theory*, *29*(2), 208-210.

Burton, D. (2011). *Elementary number theory*. McGraw-Hill.

Childs, L. (2009). *A concrete introduction to higher algebra*. Springer.

China and India. (2009). In Mathematics in Historical Context (pp. 55–82). The Mathematical Association of America. https://doi.org/10.5948/UPO9781614445029.004379. https://doi.org/10.1007/s00407-019-00243-x

Collins, D.C. (1999). Continued fractions. The MIT Undergraduate Journal of Mathematics, I, 11-20.

Ding, C., Pei, D., & Salomaa, A. (1996). *Chinese Remainder Theorem Applications in Computing, Coding, Cryptography*. World Scientific Publishing.

Films Media Group. (2008). *The genius of the east: Mathematics during the Middle Ages*. *Films On Demand*. https://fod.infobase.com/PortalPlaylists.aspx?wID=96609&xtid=40030.

Grossschadl, J. (2000, December). The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip. In *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)* (pp. 384-393). IEEE.

Ing, L. H. (2003). *The History of the Chinese Remainder Theorem*. Https://Sms.Math.Nus.Edu.Sg/Smsmedley/Vol-30-1/The%20History%20of%20the%20Chinese%20Reminder%20Theorem%20(Law%20Huang%20lng).Pdf

Joyce, D. (2000) Clark University. *Qin Jiushao's algorithm for finding one*. Retrieved March 12, 2021, from https://mathcs.clarku.edu/~djoyce/ma105/findingone.html.

Kaya, K., & Selçuk, A. A. (2007). Threshold cryptography based on Asmuth–Bloom secret sharing. *Information sciences*, *177*(19), 4148-4160.

Kangsheng, S. (1987). Historical Development of the Chinese Remainder Theorem. *Archive for History of Exact Sciences*, *38*(4), 285-305. Retrieved April 17, 2021, from https://www.jstor.org/stable/41133837

Lake, J. (2021, March 18). *What is RSA encryption and how does it work?* Comparitech. https://www.comparitech.com/blog/information-security/rsa-encryption/

Liu, Y.-H., & Chen, R.-J. (2017). An asymptotically perfect secret sharing scheme based on the Chinese Remainder Theorem. International Journal of Computer Mathematics, 94(9), 1890–1915. https://doi.org/10.1080/00207160.2016.1274738

Liu, Y. (2018). *Shangyuan Astronomical System*. Shàngyuán System in Ancient Chinese Astronomical Systems. Retrieved September 16, 2021, from http://ytliu0.github.io/ChineseCalendar/Shangyuan.html

Matkovic, D. (1988). The Chinese Remainder Theorem: A Historical Account. *Pi Mu Epsilon Journal*, *8*(8), 493-502. Retrieved November 22, 2020, from http://www.jstor.org/stable/24339970

Notices of the American Mathematical Society. (2003),

Rivest, Shamir, and Adleman Receive 2002 Turing Award. Retrieved December 6, 2021, from http://www.ams.org/notices/200307/comm-turing.pdf

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

Singh, S., & Agarwal, G. (2010). Use of Chinese Remainder Theorem to generate random numbers for cryptography. *International Journal of Applied Engineering Research*, 1(2). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.374.8163&rep=rep1&type=pdf