THE CHINESE REMAINDER THEOREM AND SOME APPLICATIONS

King Fahd University of Petroleum & Minerals

Student: Ali Aljanubi

Advisor: Dr. Abdullah Laradji

Department of Mathematics

May 23, 2024

Abstract

The Chinese Remainder Theorem is one of the most important and useful results in Number Theory and Algebra. In this report, we give a brief historical overview of the theorem, its generalization to commutative rings, and some of its applications. In particular, we will show how it can be used in remote coin-flipping.

Contents

Chapter 1

Brief History

Around the 3rd century A.D., Chinese mathematician Sun Zi gave and solved this problem:

Problem 1. *Now there are an unknown number of things. If we count by threes, there is a remainder 2; if we count by fives, there is a remainder 3; if we count by sevens, there is a remainder 2. Find the number of things.*

- CRT was essential for computing some calendars in ancient times.

- CRT may have been used to calculate the number of soldiers in an army.

Example 1. *A battle commander asks his soldiers to line up in rows of 11, then in rows of 17, 29, and 31, respectively. He is informed that the remainders are 8, 5, 16, and 24 respectively. Then he calculates the number of soldiers privately.*

Chapter 2

Linear Congruences

Theorem 1. *Let $a, b, m \in \mathbb{Z}$, $m > 0$, and $d = gcd(a, m)$. Then the congruence*

$$ax \equiv b \mod m$$

has a solution if and only if d is a divisor of b. If $d|b$, then there are exactly d solutions that are distinct mod m.

In general, let $d = gcd(a_1, a_2, ..., a_n, m)$. Then the congruence

$$a_1x_1 + a_2x_2 + ... + a_nx_n \equiv b \mod m$$

has

- No solution if $d \nmid b$
- Exactly dm^{n-1} solutions if $d|b$.

Definition 1. *We say that integers a and b are **multiplicative inverses** of each other mod m if*

$$ab \equiv 1 \mod m.$$

Corollary. *The integer a has an inverse* mod m *if and only if $gcd(a, m) = 1$.*

Chapter 3

Chinese Remainder Theorem (CRT)

Theorem 2. *Let $m_1, m_2, ..., m_r$ be positive integers that are pairwise relatively prime (that is, $gcd(m_i, m_j) = 1$ if $i \neq j$). Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

has a unique solution $\mod m_1 m_2 ... m_r$.

A Generalization of CRT: the system of congruences $x \equiv a_i \mod m_i$ $(1 \leq i \leq r)$ is solvable if and only if $gcd(m_i, m_j) | (a_i - a_j)$ whenever $1 \leq i \leq j \leq r$. The solution, if any, is unique $\mod lcm(m_1, m_2, ..., m_r)$.

Example 2. *Solve the system* $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$, $x \equiv 2 \mod 7$.

Solution*: The system has a solution because* 3, 5 *and* 7 *are pairwise relatively prime. Let* x *be a solution, then*

$$x = 2 + 7k \qquad \text{for some integer } k.$$

Hence

$$2 + 7k \equiv 3 \mod 5$$

so that

$$2k \equiv 1 \mod 5, \text{ i.e. } k \equiv 3 \mod 5.$$

Then

$$k = 3 + 5h \text{ for some integer } h.$$

Hence

$$2 + 7(3 + 5h) \equiv 2 \mod 3, \text{ i.e.}$$
$$h \equiv 0 \mod 3$$

This gives $h = 3t$ *for some integer* t. *We obtain* $k = 3+15t$, *i.e.* $x = 2+7(3+15t) = 23+105t$ *All integers congruent to* 23 $\mod 105$ *are solutions of the system.*

Example 3. *Solve the system*

$$x \equiv 1 \mod 6$$
$$x \equiv 4 \mod 15$$
$$x \equiv 3 \mod 5$$

Theorem 3. *Let* I *and* J *be two comaximal ideals of a commutative ring* R. *Then,*

$$\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}$$

Corollary. *Let* n *and* m *be two relatively prime integers. Then,*

$$\frac{\mathbb{Z}}{nm\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

Example 4.

$$\frac{\mathbb{Z}}{6\mathbb{Z}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$$

There is a ring isomorphism

$$\frac{\mathbb{Z}}{6\mathbb{Z}} \quad \to \quad \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$$

$x + 6\mathbb{Z} \mapsto (x + 2\mathbb{Z}, x + 3\mathbb{Z})$

Which sends

$$\bar{0} \mapsto (\bar{0}, \bar{0})$$

$$\bar{1} \mapsto (\bar{1}, \bar{1})$$

$$\bar{2} \mapsto (\bar{0}, \bar{2})$$

$$\bar{3} \mapsto (\bar{1}, \bar{0})$$

$$\bar{4} \mapsto (\bar{0}, \bar{1})$$

$$\bar{5} \mapsto (\bar{1}, \bar{2})$$

Corollary. *let n, m be positive integers ≥ 2 with $gcd(m, n) = 1$. Then Euler's function Φ satisfies*

$$\Phi(nm) = \Phi(n)\Phi(m).$$

Chapter 4

Systems of Linear Congruences

Consider the system (1) below

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &\equiv b_1 \mod m_1 \\
a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n &\equiv b_2 \mod m_2 \\
&... \\
&... \\
&... \\
a_{r1}x_1 + a_{r2}x_2 + ... + a_{rn}x_n &\equiv b_r \mod m_r.
\end{aligned}$$

4.1 Systems of Linear Congruences with Equal Modulo (Prime)

The system (1) with $m_1 = m_2 = ... = m_r = p$, where p is prime

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &\equiv b_1 \mod p \\
a_{21}x_1 + a_{22}x_2 + ... + a_{21}x_n &\equiv b_2 \mod p \\
&... \\
&... \\
&... \\
a_{r1}x_1 + a_{r2}x_2 + ... + a_{rn}x_n &\equiv b_r \mod p
\end{aligned}$$

can be solved by adapting methods from linear algebra.

Example 5. *We consider the system*

$$\begin{aligned} 2x_1 + 5x_2 + 6x_3 &\equiv 3 \mod 7 \\ 2x_1 + 6x_3 &\equiv 4 \mod 7 \\ x_1 + 2x_2 + 3x_3 &\equiv 1 \mod 7 \end{aligned}$$

this is equivalent to the matrix congruence

$$\begin{bmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 4 \\ 1 \end{bmatrix} \mod 7$$

$$\begin{bmatrix} 2 & 5 & 6 & 3 \\ 2 & 0 & 1 & 4 \\ 1 & 2 & 3 & 1 \end{bmatrix} r_2 \to r_2 - r_1 \begin{bmatrix} 2 & 5 & 6 & 3 \\ 0 & 2 & 2 & 1 \\ 1 & 2 & 3 & 1 \end{bmatrix} r_3 \to r_3 + 3r_1 \begin{bmatrix} 2 & 5 & 6 & 3 \\ 0 & 2 & 2 & 1 \\ 0 & 3 & 0 & 3 \end{bmatrix} r_2 \leftrightarrow r_3 \begin{bmatrix} 2 & 5 & 6 & 3 \\ 0 & 3 & 0 & 3 \\ 0 & 2 & 2 & 1 \end{bmatrix}$$

$$r_3 \to 2r_3 + r_2 \begin{bmatrix} 2 & 5 & 6 & 3 \\ 0 & 3 & 0 & 3 \\ 0 & 0 & 4 & 5 \end{bmatrix} r_1 \to 2r_1 - r_2 \begin{bmatrix} 4 & 0 & 5 & 3 \\ 0 & 3 & 0 & 3 \\ 0 & 0 & 4 & 5 \end{bmatrix} r_1 \to r_1 + 4r_2 \begin{bmatrix} 4 & 0 & 0 & 2 \\ 0 & 3 & 0 & 3 \\ 0 & 0 & 4 & 5 \end{bmatrix}$$

$$r_1 \to 2r_1, r_2 \to 5r_2, r_3 \to 2r_3 \begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

so the solution is

$$x_1 \equiv 4 \mod 7,\ x_2 \equiv 1 \mod 7,\ x_3 \equiv 3 \mod 7.$$

4.2 Systems of Linear Congruences with Equal Modulo m

Consider the system (2) below

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &\equiv b_1 \mod m \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n &\equiv b_2 \mod m \\ &... \\ &... \\ a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n &\equiv b_n \mod m \end{aligned}$$

Let A be the coefficient matrix of the system. If $\det(A)$ is relatively prime to m, then the system has a unique solution mod m.

Example 6. *Solve the system*

$$\begin{aligned} x + 3y + z &\equiv 1 \mod 8 \\ 4x + y + 5z &\equiv 7 \mod 8 \\ 2x + 2y + z &\equiv 3 \mod 8 \end{aligned}$$

the determinant of the coefficient matrix is 7 *which is relatively prime to* 8*, so there exists a unique solution* mod 8*. The augmented matrix is*

$$\begin{bmatrix} 1 & 3 & 1 & 1 \\ 4 & 1 & 5 & 7 \\ 2 & 2 & 1 & 3 \end{bmatrix} r_2 \to r_2 - 4r_1,\ r_3 \to r_3 - 2r_1 \begin{bmatrix} 1 & 3 & 1 & 1 \\ 0 & 5 & 1 & 3 \\ 0 & 4 & 7 & 1 \end{bmatrix} r_3 \to r_3 + 4r_2 \begin{bmatrix} 1 & 3 & 1 & 1 \\ 0 & 5 & 1 & 3 \\ 0 & 0 & 3 & 5 \end{bmatrix}$$

$$r_1 \to r_1 + r_2 \begin{bmatrix} 1 & 0 & 2 & 4 \\ 0 & 5 & 1 & 3 \\ 0 & 0 & 3 & 5 \end{bmatrix} \quad r_1 \to r_1 + 2r_3,\ r_2 \to 3r_2 - r_3 \begin{bmatrix} 1 & 0 & 0 & 6 \\ 0 & 7 & 0 & 4 \\ 0 & 0 & 3 & 5 \end{bmatrix} r_2 \to 7r_2,\ r_3 \to 3r_3 \begin{bmatrix} 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 7 \end{bmatrix}$$

the solution is $x \equiv 6 \mod 8$*,* $y \equiv 4 \mod 8$*,* $z \equiv 7 \mod 8$*.*

4.3 Multivariable Chinese Remainder Theorem

Consider the system (3) below with $gcd(m_i, m_j) = 1$ for all $i \neq j$

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &\equiv b_1 \mod m_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n &\equiv b_2 \mod m_2 \\ &... \\ &... \\ &... \\ a_{r1}x_1 + a_{r2}x_2 + ... + a_{rn}x_n &\equiv b_r \mod m_r. \end{aligned}$$

Theorem 4. *Let* $m_1, m_2, ..., m_r$ *be pairwise relatively prime integers and* $m = m_1 m_2 ... m_r$*. The system of congruences represented by (3) has a solution if and only if for each* $i \leq r$*,* $d_i | b_i$*, where* $d_i = gcd(a_{i1}, a_{i2}, ..., a_{in}, m_i)$ *and if this condition is satisfied, then there are* $m^{n-1} \prod_{i=1}^{r} d_i$ *solutions.*

Chapter 5

Some Applications

5.1 Square Roots mod pq

Definition 2. *Let $gcd(a, m) = 1$. We say that a is a **quadratic residue** mod m or (**square** mod m) if $x^2 \equiv a \mod m$ has a solution, and that it is a **quadratic nonresidue** mod m if it has no solution.*

Lemma 1. *Let p be an odd prime and $gcd(a, p) = 1$, then $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$.*

Euler's Criterion Let p be an odd prime and $gcd(a, p) = 1$, then $x^2 \equiv a \mod p$ has

$$\text{exactly 2 solutions if } a^{\frac{p-1}{2}} \equiv 1 \mod p$$

$$\text{no solution if } a^{\frac{p-1}{2}} \equiv -1 \mod p.$$

Let $p \equiv 3 \mod 4$ be prime. If $x^2 \equiv a \mod p$ has a solution, then we can find square roots easily.

Lemma 2. *Let $p \equiv 3 \mod 4$ be prime. If $x^2 \equiv a \mod p$ has a solution, then the solutions are given by*

$$x \equiv \pm a^{\frac{p+1}{4}} \mod m.$$

Proof. By Euler's Criterion $(\pm a^{\frac{p+1}{4}})^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} a \equiv 1a \equiv a \mod p$.

□

Theorem 5. *Let $n = pq$ where p and q are two distinct odd primes numbers and let a be an integer with $gcd(n, a) = 1$, then the congruence $x^2 \equiv a \mod n$ either has exactly 4 noncongruent solutions mod n or no solution.*

Proof. The congruence $x^2 \equiv a \mod n$ has a solution if and only if the system

$$x^2 \equiv a \mod p$$
$$x^2 \equiv a \mod q$$

has a solution. Let the system have a solution,
let $x \equiv \pm x_1 \mod p$ be the solutions of $x^2 \equiv a \mod p$
and $x \equiv \pm x_2 \mod q$ be the solutions of $x^2 \equiv a \mod q$.

Then we obtain four systems of congruences:

$$\text{(i)} \begin{array}{l} x \equiv x_1 \mod p \\ x \equiv x_2 \mod q \end{array} \qquad \text{(ii)} \begin{array}{l} x \equiv x_1 \mod p \\ x \equiv -x_2 \mod q \end{array}$$

$$\text{(iii)} \begin{array}{l} x \equiv -x_1 \mod p \\ x \equiv x_2 \mod q \end{array} \qquad \text{(iv)} \begin{array}{l} x \equiv -x_1 \mod p \\ x \equiv -x_2 \mod q \end{array}$$

By CRT each one of the systems has a unique solution modulo n satisfying the congruence $x^2 \equiv a \mod n$. The 4 solutions are noncongruent $\mod n$.

□

Let $n = pq$ where p and q are two distinct prime numbers each congruent to 3 modulo 4, and let a be an integer with $gcd(n, a) = 1$. Then finding the 4 solutions of the congruence $x^2 \equiv a \mod n$ (if any) is computationally equivalent to factoring n. We mean by this: if we know the four roots we can easily factor n; conversely, if we know the factors of n we can easily find the four roots.

Let $\pm u, \pm v$ be the four noncongruent square roots of $a \mod n$ i.e.
$u^2 \equiv a \mod n$ and $v^2 \equiv a \mod n$, then $u^2 - v^2 \equiv 0 \mod n$, hence $pq|(u - v)(u + v)$. Assume that $pq|(u - v)$ or $pq|(u + v)$, then that contradicts that they are noncongruent mod pq. Therefore,

$$gcd(u + v, n) = p \text{ and } gcd(u - v, n) = q \text{ or}$$
$$gcd(u + v, n) = q \text{ and } gcd(u - v, n) = p.$$

5.2 Remote Coin Flipping

Suppose A and B are two people who want to flip a coin to see who wins a certain prize. But they are far apart, talking on the telephone.

- A chooses two very large distinct primes p, q, where p and q are each congruent to 3 modulo 4, and computes $n = pq$. A then sends n to B.

- B chooses a natural number $x \in (0, n)$ with $gcd(x, n) = 1$, and computes $x^2 \equiv a \mod n$. B then sends a to A.

- A knows p and q, so he computes the four square roots of a: $\pm x$ and $\pm y$. Then he assigns $\pm x$ to one side of a coin and $\pm y$ to the other side. A tosses the coin: if he gets $\pm x$, he wins, and if he gets $\pm y$, he loses.

- If A wins, he sends $\pm x$ to B. If B denies that A won, then B should be able to factor n (compute p and q) since he knows the four square roots of a.

- If B wins (in case A has sent $\pm y$), then to prove that, either he sends the four square roots of a to A, or sends the prime numbers p and q to A.

5.3 Arbitrary Distance between Square-Free Numbers

Theorem 6. *There exist an arbitrarily large number of consecutive integers, none of which is prime.*
There exist arbitrarily large numbers of consecutive integers, none of which is square-free.

Proof. Let k be an arbitrary positive integer and let $p_1, p_2, ..., p_k$ be distinct primes, then consider the system

$$\begin{aligned} n+1 &\equiv 0 \mod p_1^2 \\ n+2 &\equiv 0 \mod p_2^2 \\ &\vdots \\ n+k &\equiv 0 \mod p_k^2 \end{aligned}$$

By CRT there exists a solution of the system. Therefore, $n+1, n+2, ..., n+k$ are consecutive integers none of which is square-free. □

5.4 Arbitrary Distance between Sums of Two Squares

Lemma 3. *There are infinitely many primes congruent to 3 mod 4.*

Fermat's Theorem on Sums of Two Squares Let n be a positive integer. Then n is a sum of two squares if and only if all primes that are congruent to 3 modulo 4 can only appear to even powers in its prime factorisation.

Theorem 7. *There exist an arbitrarily large number of consecutive integers, none of which is a sum of two squares.*

Definition 3. *A natural number n is a **powerful number** if for every prime p dividing n, p^2 divides n.*

Theorem 8. *There exist an arbitrarily large number of consecutive integers, none of which is powerful.*

We will show both theorems in one proof.

We construct a sequence of consecutive numbers such that for each number in that sequence, there exists at least one prime congruent to 3 mod 4 that is to power one in its prime factorization.

Note that if $n \equiv p \mod p^2$, then $p \mid\mid n$.

Proof. Let k be an arbitrary positive integer and let $p_1, p_2, ..., p_k$ be distinct primes each congruent to 3 modulo 4 , then consider the system

$$\begin{aligned} n+1 &\equiv p_1 \mod p_1^2 \\ n+2 &\equiv p_2 \mod p_2^2 \\ &\vdots \\ n+k &\equiv p_k \mod p_k^2 \end{aligned}$$

By CRT there exists a solution of the system. Therefore, $n+1, n+2, ..., n+k$ are consecutive integers neither of which is the sum of two squares nor a powerful number.

□

References

Kraft, J., Washington, L. (2018). An Introduction to Number Theory with Cryptography. Chapman and Hall/CRC.

Rosen, K. H. (2011). Elementary Number Theory. London: Pearson Education.

Schroeder, M. R. (2009). Number Theory in Science and Communication 5th edition. In Springer Series in Information Sciences.

Dickson, L. E. (2005). History of the Theory of Numbers, Volume II: Diophantine Analysis. Dover Publications, New York.

Lac, Jacquelyn Ha, "Chinese remainder theorem and its applications" (2008). Theses Digitization Project. 3373.

Knill, O. (2012). A multivariable Chinese remainder theorem. arXiv:1206.5114.

Babu, C. G., Bera, R., Sury, B. (2024). Linear congruences in several variables with congruence restrictions. arXiv:2403.01914.

Sury, B. (2015). Multivariable Chinese remainder theorem. Resonance 20, 206-216.

Kangsheng, S. (1988). Historical development of the Chinese remainder theorem. Archive for history of exact sciences 38, 285-305.