NAMANGAN DAVLAT UNIVERSITETI
ILMIY AXBOROTNOMASI, [2026-6]
ISSN:2181-1458
ISSN:2181-0427

01.00.00-FIZIKA-MATEMATIKA
journal.namdu.uz
PHYSICS AND MATHEMATICS

THE GENERALIZED CHINESE REMAINDER THEOREM: HANDLING NON-COPRIME MODULI

Tukhtabaev Akbarkhuja Mamajonovich
Senior lecturer (PhD) at the department of Mathematics, Namangan state university
Email: akbarxoja.toxtaboyev@mail.ru
Saylitdinova Hilola Khusniddin kizi
Student of Namangan state university
Email: saylitdinovah@gmail.com

Abstract. *Present paper is devoted to the generalization of the Chinese Remainder Theorem for non-coprime moduli. A criterion for the existence of a solution to a system of congruences in the non-coprime case is provided. Furthermore, a general formula for a system of two congruences and an iterative formula for systems involving more than two congruences are derived.*

Keywords: *Congruence, Chinese Remainder Theorem, residue, coprime.*

QOLDIQ HAQIDAGI XITOY TEOREMASINING O'ZARO TUB BO'LMAGAN MODULLAR UCHUN UMUMLASHLASHMASI

Annotatsiya. *Ushbu maqola qoldiq haqidagi Xitoy teoremasini o'zaro tub bo'lmagan modullar uchun umumlashtirishga bag'ishlangan. Taqqoslamalar sistemasi o'zaro tub bo'lmagan holatda yechimga ega bo'lishining zaruriy va yetarli sharti keltirilgan. Bundan tashqari, ikkita taqqoslamalar sistemasi uchun umumiy formula hamda ikkitadan ortiq taqqoslamalardan iborat sistemalar uchun itaratsion formula keltirib chiqarilgan.*

Kalit so'zlar: *Taqqoslama, Qoldiq haqidagi Xitoy teoremasi, qoldiq, o'zaro tub.*

ОБОБЩЕННАЯ КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ: РАБОТА С НЕ ВЗАИМНО ПРОСТЫМИ МОДУЛЯМИ

Аннотация. *Данная статья посвящена обобщению китайской теоремы об остатках для случая не взаимно простых модулей. Приводится критерий существования решения системы сравнений для не взаимно простых модулей. Кроме того, выведена общая формула для системы из двух сравнений и итерационная формула для систем, состоящих из более чем двух сравнений.*

Ключевые слова: *Сравнение, Китайская теорема об остатках, остаток, взаимно простые*

Introduction

The Chinese Remainder Theorem (CRT) [1] is a fundamental result in number theory with broad applications in cryptography, computational mathematics, and abstract algebra. In its classical form, the theorem guarantees that a system of simultaneous congruences has a unique solution, provided that the moduli (divisors) are pairwise coprime. However, what happens when these moduli share common factors? This article explores the behavior of congruences when the moduli are not relatively prime, presenting the generalized forms of the theorem and the algorithms used to find their solutions. Similar problems have also been studied in [2].

I. Preliminaries

I.1. Divisibility in integers and its main properties.

Definition 1. An integer a is said to be *divisible* by an integer b ($b \neq 0$) if there exists an integer k such that:

$$a = b \cdot k. \quad (1)$$

In this case, we write $b \mid a$ (read as b divides a). Here, b is called a divisor (or factor) of a, and a is called a multiple of b.

The divisibility relation in the set of integers ( ) satisfies the following properties:

1.**Reflexivity:** For any non-zero integer a, $a \mid a$

2.**Transitivity:** $b \mid a$ and $c \mid b$, then $c \mid a$.

3.**Divisibility of linear combinations:** If $m \mid a$ and $m \mid b$, then for any integers x and y $m \mid (ax+by)$.

4.**Multiplication property:** If $b \mid a$, then $bc \mid ac$ for any integer c.

5.**Comparison property:** If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

6.Antisymmetry: If $b \mid a$ and $a \mid b$, then $|a| = |b|$ (i.e., $a = b$ or $a = -b$).

For any integer a (the dividend) and a positive integer b (the divisor), there exist unique integers q (the quotient) and r (the remainder or residue) such that:

$$a = bq + r, \quad 0 \leq r < b. \tag{2}$$

If $r = 0$, then a is exactly divisible by b.

I.2. Greatest Common Divisor (GCD) and Least Common Multiple (LCM).

Definition 2. The GCD of two integers a and b is the largest positive integer that divides both a and b. It is denoted as $\gcd(a,b)$.

If $\gcd(a,b) = 1$, the integers a and b are said to be *relatively prime* (or *coprime*).

Definition 3. The LCM of two integers a and b is the smallest positive integer that is a multiple of both a and b. It is denoted as $\operatorname{lcm}(a,b)$.

It has the following property

$$|a \cdot b| = \gcd(a,b) \cdot \operatorname{lcm}(a,b). \tag{3}$$

Euclid's Algorithm. This is an efficient method for computing the GCD of two numbers. It is based on the principle that the GCD of two numbers does not change if the larger number is replaced by its remainder when divided by the smaller number, i.e. if $a = bq + r, \quad 0 \leq r < b$ then

$$\gcd(a,b) = \gcd(b,r). \tag{4}$$

This process is repeated until the remainder becomes zero. The last non-zero remainder is the GCD.

I.3. Important Theorems related to Divisibility.

Bézout's identity: For any integers a and b, there exist integers x and y such that:

$$ax + by = \gcd(a,b). \tag{5}$$

a and b are coprime if and only if there exit integers x and y such that

$$ax + by = 1. \tag{6}$$

If $\gcd(c,a) = 1$ and c divides ab, then c must divide b.

I.4. Congruence.

Definition 4. Two integers a and b are said to be *congruent modulo* m if their difference $a-b$ is an integer multiple of m. This is written as $a \equiv b \pmod{m}$.

Proposition 1[1]. If a, b, c, d, l, k and m are integers such that $m > 0$, $d = (k,m)$, $a \equiv b \pmod{m}$, and $c \equiv l \pmod{m}$ then

1) $a + c \equiv b + l \pmod{m}$,
2) $ac \equiv bl \pmod{m}$,
3) $ak \equiv bk \pmod{m}$,
4) if $k \neq 0$ then $ak \equiv bk \pmod{m|k|}$ (here $|k|$ is absolute value of k),
5) if $k \neq 0$, $ak \equiv bk \pmod{m}$ then $a \equiv b \left(\bmod \frac{m}{d} \right)$.

Proposition 2 [1]. Let a and b are integers with $d = (a,b)$. The equation $ax + by = c$ has no integer solutions if $d \not| c$. If $d \mid c$, then there are infinitely many integer solutions. Moreover, if $x = x_0$, $y = y_0$ is a particular solutions of the equation, then all solutions are given by

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n \tag{7}$$

where n is an integer.

Theorem 1 [1]. Let a, b and m are integers such that $m > 0$, $d = (a,m)$.

If $d \nmid b$ then the linear congruence

$$ax \equiv b(\bmod m) \tag{8}$$

has no solutions. If $d \mid b$ then the linear congruence (8) has exactly d incongruent solutions modulo m.

Corollary [1]. Let a and m are relatively prime integers with $m > 0$ and b is an integer, then the linear congruence (8) has a unique solution modulo m.

Theorem 2(Fermat's Little Theorem) [1]. If p is a prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{9}$$

II. Main results

We now present the main theorem concerning the solution of systems of linear congruences in one unknown. This theorem is called the *Chinese remainder theorem*, most likely because of the contributions of Chinese mathematicians such as Ch'in Chiu-Shao to its solution.

Theorem 3 (The Chinese Remainder Theorem) [1]. Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers. Then the system of congruences

$$\begin{cases} x \equiv a_1 (\bmod m_1) \\ x \equiv a_2 (\bmod m_2) \\ \quad \vdots \\ x \equiv a_r (\bmod m_r) \end{cases} \tag{10}$$

has a unique solution modulo $M = m_1 m_2 \ldots m_r$. Moreover,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r, \tag{11}$$

where $M_k = \dfrac{M}{m_k}$, y_k is a solution of the linear congruence $M_k y \equiv 1 (\bmod\ m_k)$, $k = \overline{1, r}$.

Example 1. Solve the following system of congruences:

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

Solution. $a_1 = 2, a_2 = 3, a_3 = 2$, $m_1 = 3, m_2 = 5, m_3 = 7$. The moduli $\{3, 5, 7\}$ are pairwise coprime.

$M = 3 \times 5 \times 7 = 105$, $M_1 = M / m_1 = 105/3 = 35$, $M_2 = M / m_2 = 105/5 = 21$, $M_3 = M / m_3 = 105/7 = 15$.

Finding the modular inverse (y_i) for each M_i such that $M_i y_i \equiv 1 \pmod{m_i}$, we have

For M_1: $35 y_1 \equiv 1 \pmod 3 \Rightarrow 2 y_1 \equiv 1 \pmod 3$. Here, $y_1 = 2$ (since $2 \times 2 = 4 \equiv 1 \pmod 3$).

For M_2: $21 y_2 \equiv 1 \pmod 5 \Rightarrow 1 y_2 \equiv 1 \pmod 5$. Here, $y_2 = 1$.

For M_3: $15 y_3 \equiv 1 \pmod 7 \Rightarrow 1 y_3 \equiv 1 \pmod 7$. Here, $y_3 = 1$.

$x = \sum a_i M_i y_i \pmod M$, $x = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1)$, $x = 140 + 63 + 30 = 233$.

$x \equiv 233 \pmod{105}$, $233 = 2 \times 105 + 23$, $x \equiv 23 \pmod{105}$.

If the moduli are not coprime ($\gcd(m_1, m_2) > 1$), a solution is not guaranteed. A specific compatibility condition must be satisfied.

Theorem 4 (Generilized Chinese Remainder Theorem). A system of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2}' \end{cases} \tag{12}$$

has a solution if and only if the following condition holds:

$$a_1 \equiv a_2 \pmod{d}, \tag{13}$$

here $d = gcd(m_1, m_2)$.

Moreover, (12) has a unique solution modulo M as folows:

$$x \equiv x_0 \pmod M, \tag{14}$$

where $M = lcm(m_1, m_2)$,

$$x_0 = a_1 + \left(\frac{a_2 - a_1}{d}\right) \cdot u \cdot m_1, \quad (15)$$

$$u \equiv \left(\frac{m_1}{d}\right)^{-1} \quad \left(mod\left(\frac{m_2}{d}\right)\right). \quad (16)$$

Proof. *Necessity.* Assume a solution x exists. By the definition of congruences, we can write

$x = a_1 + k_1 m_1$,

$x = a_2 + k_2 m_2$,

for some integers k_1 and k_2.

Setting these equal gives

$$a_1 + k_1 m_1 = a_2 + k_2 m_2 \Rightarrow a_1 - a_2 = k_2 m_2 - k_1 m_1$$

Let $d = \gcd(m_1, m_2)$. Since d divides both m_1 and m_2, it must also divide the right side of the equation ($k_2 m_2 - k_1 m_1$). Therefore, d must divide the left side, meaning d divides $(a_1 - a_2)$. It follows that

$a_1 \equiv a_2 \quad (mod \quad d)$.

Sufficiency. Assume the condition $a_1 \equiv a_2 \quad (mod \quad d)$ holds.

We must solve (12) .

$a_1 + k_1 m_1 = x = a_2 + k_2 m_2$ (17)

gives that

$k_1 m_1 = a_2 - a_1 + k_2 m_2$.

Dividing the last equality by d, we have

$\frac{k_1 m_1}{d} = \frac{a_2 - a_1}{d} + \frac{k_2 m_2}{d}$ (18)

Taking the congruence modulo $\frac{m_2}{d}$ from equality (18), we obtain the following

$k_1 \equiv \left(\frac{m_1}{d}\right)^{-1} \frac{a_2 - a_1}{d} \left(mod \frac{m_2}{d}\right)$. (19)

Note that $gcd\left(\frac{m_1}{d}, \frac{m_2}{d}\right) = 1$, then $u: \equiv \left(\frac{m_1}{d}\right)^{-1} \left(mod \frac{m_2}{d}\right)$ exists. First, both sides of (19) multiple by m_1, and adding a_1 we have

$a_1 + k_1 m_1 \equiv a_1 + m_1 u \frac{a_2 - a_1}{d} \left(mod \frac{m_2 m_1}{d}\right)$. (20)

Taking account $M = lcm(m_1, m_2) = \frac{m_2 m_1}{d}$, (17) and (20) give

$x \equiv a_1 + \frac{a_2 - a_1}{d} \cdot u \cdot m_1 (mod\, M)$. (21)

Using notation $x_0 = a_1 + \left(\frac{a_2 - a_1}{d}\right) \cdot u \cdot m_1$, we have (14). Theorem is proved.

Corollary 2. Let M is a multiple of m (i.e., $m \mid M$), a system of congruences

$$\begin{cases} x \equiv a (mod\, M) \\ x \equiv b (mod\, m) \end{cases}$$

is solvable if and only if $a \equiv b (mod\, m)$. Moreover, then the system of congruences is redundant, and the solution is $x \equiv a (mod\, M)$.

By applying Theorem 4 first to the initial two congruences, then applying the obtained result to the third, then to the fourth, and so on, we arrive at the following result.

Corollary 3 (Generalized Chinese Remainder Theorem). A system of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad (22)$$

has a solution if and only if the following condition holds for all $1 \le i < j \le k$:

$$a_i \equiv a_j \pmod{d_{i,j}}, \quad (23)$$

here $d_{i,j} = \gcd(m_i, m_j)$.

Moreover, the system has a unique solution modulo M as follows:

$$x \equiv X_k \pmod{M}, \tag{24}$$

where $M = \operatorname{lcm}(m_1, m_2, \ldots, m_k)$, and the specific solution X_k is determined recursively. Setting the base case as $X_1 = a_1$ and $M_1 = m_1$, for each step $i = 2, 3, \ldots, k$, the value X_i is defined as:

$$X_i = X_{i-1} + \left(\frac{a_i - X_{i-1}}{d_i}\right) \cdot u_i \cdot M_{i-1}, \tag{25}$$

where $d_i = \gcd(M_{i-1}, m_i)$, the running modulus is updated as $M_i = \operatorname{lcm}(M_{i-1}, m_i)$, and u_i is the modular inverse satisfying:

$$u_i \equiv \left(\frac{M_{i-1}}{d_i}\right)^{-1} \pmod{\frac{m_i}{d_i}}. \tag{26}$$

The following result follows directly from Corollary 3.

Corollary 4. A system of congruences

$$\begin{cases} x \equiv a \pmod{m_1} \\ \ldots \\ x \equiv a \pmod{m_k} \end{cases} \tag{27}$$

is always solvable and $x \equiv a (mod\ M)$, where $M = \operatorname{lcm}(m_1, m_2, \ldots, m_k)$.

Example 2. Solve the following system of congruences:

$$\begin{cases} x \equiv 3 (mod\ 6), \\ x \equiv 7 (mod\ 10). \end{cases}$$

Solution. Here $a_1 = 3$, $m_1 = 6$ and $a_2 = 7$, $m_2 = 10$. The moduli are not coprime.

First, we check the condition for the existence of a solution: $d = \gcd(m_1, m_2) = \gcd(6,10) = 2$

$a_2 - a_1 = 7 - 3 = 4$. Since 4 is divisible by 2 ($2 \mid 4$), a solution exists.

We solve it using the formulas from the theorem 4, Find the modular inverse u according to formula (16).

$u \equiv \left(\frac{m_1}{d}\right)^{-1} \left(mod\ \frac{m_2}{d}\right)$, $u \equiv \left(\frac{6}{2}\right)^{-1} \left(mod\ \frac{10}{2}\right)$, $u \equiv 3^{-1} (mod\ 5) \equiv 2 (mod\ 5)$.

Calculate the specific solution x_0 according to formula (15). $x_0 = a_1 + \left(\frac{a_2 - a_1}{d}\right) \cdot u \cdot m_1$, $x_0 = 3 + \left(\frac{7-3}{2}\right) \cdot 2 \cdot 6$,

$x_0 = 3 + \left(\frac{4}{2}\right) \cdot 12 = 3 + 24 = 27$, $x \equiv 27 (mod\ 30)$.

Example 3. Solve the following system of congruences:

$$\begin{cases} x \equiv 1 (mod\ 4), \\ x \equiv 5 (mod\ 6), \\ x \equiv 7 (mod\ 10), \\ x \equiv 2 (mod\ 15). \end{cases}$$

Solution. It is straightforward to verify that the condition $\gcd(m_i, m_j) \mid (a_i - a_j)$ holds true for all pairs (for example, $\gcd(6,10) = 2$ and $7 - 5 = 2$). Thus, a solution definitely exists. We apply the iterative formula step-by-step. We take the first congruence as our initial working solution:

1) $X_1 = 1$, $M_1 = 4$, $x \equiv 1 \pmod{4}$.

2) $d_2 = \gcd(M_1, m_2) = \gcd(4,6) = 2$, $u_2 \equiv \left(\frac{M_1}{d_2}\right)^{-1} \left(mod\ \frac{m_2}{d_2}\right) \Rightarrow u_2 \equiv \left(\frac{4}{2}\right)^{-1} \left(mod\ \frac{6}{2}\right) \Rightarrow 2u_2 \equiv 1 (mod\ 3)$. Thus, $u_2 = 2$. $X_2 = X_1 + \left(\frac{a_2 - X_1}{d_2}\right) \cdot u_2 \cdot M_1 = 1 + \left(\frac{5-1}{2}\right) \cdot 2 \cdot 4 = 1 + 2 \cdot 8 = 17$. New modulus: $M_2 = \operatorname{lcm}(4,6) = 12$.

We reduce 17 modulo 12: $17 \equiv 5 \pmod{12}$. Current solution: $x \equiv 5 \pmod{12}$.

3) $d_3 = \gcd(M_2, m_3) = \gcd(12,10) = 2$, $u_3 \equiv \left(\frac{12}{2}\right)^{-1} \left(mod\, \frac{10}{2}\right) \Rightarrow 6u_3 \equiv 1(mod\, 5) \Rightarrow 1 \cdot u_3 \equiv 1(mod\, 5)$. Thus, $u_3 = 1$.

$$X_3 = X_2 + \left(\frac{a_3 - X_2}{d_3}\right) \cdot u_3 \cdot M_2 = 5 + \left(\frac{7-5}{2}\right) \cdot 1 \cdot 12 = 5 + 1 \cdot 12 = 17.$$

New modulus: $M_3 = \text{lcm}(12,10) = 60$. Current solution: $x \equiv 17 \pmod{60}$.

4) According to Corollary 2, $x \equiv 2(mod\, 15)$ and $x \equiv 17(mod\, 60)$ gives $x \equiv 17(mod\, 60)$.

Example 4. Solve the following system of congruences:

$$\begin{cases} x \equiv 3(mod\, 4), \\ x \equiv 5(mod\, 6), \\ x \equiv 9(mod\, 10), \\ x \equiv 14(mod\, 15). \end{cases}$$

Solution. We rewrite given system as follows

$$\begin{cases} x \equiv -1(mod\, 4), \\ x \equiv -1(mod\, 6), \\ x \equiv -1(mod\, 10), \\ x \equiv -1(mod\, 15). \end{cases}$$

Thanks to Corollary 4, $x \equiv -1(mod\ \ lcm(4,6,10,15)) \equiv -1(mod\, 60)$, i.e. $x \equiv 59(mod\, 60)$.

Conclusion

The Generalized Chinese Remainder Theorem provides a robust framework for solving systems of linear congruences where the moduli are not necessarily coprime. A solution is guaranteed to exist if and only if every pair of equations satisfies the necessary compatibility condition based on their greatest common divisor. For systems with multiple equations, an iterative step-by-step approach is the most effective way to systematically find the unique solution. Additionally, the process can be significantly optimized by applying the absorption property to quickly identify and eliminate redundant congruences. Together, these methods offer a complete and computationally efficient strategy for tackling complex problems in modular arithmetic.

Foydalanilgan adabiyotlar

1. Rosen K.H., Elementary Number Theory and Its Applications. Pearson, (2011).

2. To'xtabayev A.M., Bunazarov X.K. Q_p maydonda kvadrat ildizga doir ayrim masalalar, Matematika Instituti Byulleteni, 2021, Vol. 4, 3, 37-41 b.