MATHEMATICAL SCIENCES AND APPLICATIONS JOURNAL

Volume 5, Number 1 | ISSN: 2986-4180

https://online-journal.unja.ac.id/msa

Article

Metode Pemecahan Sistem Kongruensi Linear

Muhammad Arief Budiman, Edi Kurniadi, Sukono, Sisilia Sylviani*

Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran, Sumedang, Jawa Barat 45363, Indonesia

*Corresponding author e-mail: sisilia.sylviani@unpad.ac.id

Article Info

Received October 2024
Accepted December 2024
Published December 2024

Keyword:
Linear Congruence System
Chinese Remainder Theorem
Intelligent Inspection Algorithm type-I and II

Abstract

A linear congruence system is a system that has more than one linear congruence. The solution of linear congruence systems has an important role in the concept of number theory. Various ways of settlement can be applied in different cases. This study discusses the problem solving of linear congruence systems with *the Chinese Remainder Theorem*, *Intelligent Inspection* Algorithm type-I and II and its application.

1. Pendahuluan

Kongruensi merupakan aspek dasar yang penting untuk berbagai penyelesaian dalam masalah teori bilangan. Konsep dari kongruensi adalah memahami pola berulang pada suatu sistem bilangan yang melibatkan pembagian dan sisa. Solusi penyelesaiannya dapat ditemukan dengan berbagai cara. Kongruensi linear dapat diselesaikan dengan metode aljabar. Metode aljabar yang digunakan adalah penggunaan algoritma pembagian dikolaborasikan dengan berbagai sifat pada kongruensi linear [1, 2]. Konsep kongruensi juga mengalami perkembangan seiring waktu. Konsep kongruensi linear terbatas dengan menggunakan konsep jumlah Ramanujan telah diperkenalkan [3, 4]. Penerapan dari konsep ini dapat dilakukan diberbagai masalah kehidupan sehari – hari. Contohnya adalah penentuan kongruensi pada lampu lalu lintas, penentuan ISBN pada suatu karya tulis, dan pelaksanaan tryout pada aplikasi website [5–7].

Sistem kongruensi linear adalah sebuah sistem yang terdiri dari lebih satu kongruensi linear yang saling berkorespondensi. Berbagai cara untuk menyelesaikan sistem kongruensi linear, salah satunya yaitu algoritma intelligent inspection dengan memanfaatkan algoritma pembagian [8, 9]. Selain itu, Chinese Remainder Theorem juga dapat menyelesaikan permasalahan sistem kongruensi linear. Tetapi pada konsepnya, diharuskan untuk faktor persekutuan terbresar (FPB) dari setiap bilangan modulusnya adalah satu [10, 11]. Sistem kongruensi linear memiliki penerapan yang luas, sebagai contoh pada bidang kriptografi, teori permainan, dan dunia komputer. Pada bidang kriptografi, konsep sistem kongruensi linear dapat dijumpai Algoritma Rivest Shamir Adleman (RSA). Konsep algoritma RSA adalah penggunaan dua kunci yang berbeda (private key dan public key) [12–15]. Pada teori permainan, berbagai permainan yang ada di Indonesia mengambil konsep dari sistem kongruensi linear. Sebagai contoh, Permainan lagu daerah, NIM, dan Hangaroo berbasis android [16–18]. Pada dunia komputer juga dapat diaplikasikan berbagai konsep dari sistem kongruensi linear. Pembuatan ujian online dan pengenalan berbasis android sebagai contohnya [19, 20].

Penelitian ini membahas mengenai konsep awal dalam pemecahan sistem kongruensi linear pada berbagai contoh permasalahan. Pemecahan kongruensi linear dapat dilakukan dengan berbagai cara. Pada penelitian ini, cara yang digunakan adalah Chinese Remainder Theorem, Algoritma Intelligent Inspection tipe-I dan Algoritma Intelligent Inspection tipe-II beserta penerapannya. Penerapan dari berbagai cara tersebut

https://doi.org/10.22437/msa.v5i1.38085

dikombinasikan dengan penggunaan konsep dari Fermat Little's Theorem dan Wilson Theorem.

2. Metode Penelitian

2.1. Kongruensi

Definisi 1. [8] *Untuk bilangan bulat b, q, dan untuk $x, y \in \mathbb{Z}$, dikatakan kongruen ke b modulo q jika $q|(x-y)$ serta tulis $x \equiv y \pmod{q}$. Jika $q \nmid (x-y)$, maka tulis $x \not\equiv y \pmod{q}$.*

Catatan: Relasi $x \equiv y \pmod{q}$ dinamakan relasi kongruensi atau lebih simpelnya kongruensi. Nilai q muncul dalam kongruensi tersebut dinamakan modulus kongruensi.

Contoh 1. $19 \equiv 3 \pmod{4}$ karena $4|(19-3)$ dan $19 \not\equiv 3 \pmod{5}$ karena $5 \nmid (19-3)$

Teorema 1. [8, 21]*Misalkan x, y, z, dan r bilangan bulat, maka*

i. Sifat refleksif: jika x adalah bilangan bulat, maka $x \equiv x \pmod{q}$.
ii. Sifat simetris: jika $x \equiv y \pmod{q}$, maka $y \equiv x \pmod{q}$.
iii. Sifat transitif: jika $x \equiv y \pmod{q}$ dan $y \equiv z \pmod{q}$, maka $x \equiv z \pmod{q}$.
iv. Sifat simplifikasi: jika r membagi x, y, dan q, maka $x \equiv y \pmod{q}$ konguren ke $x/r \equiv y/r \pmod{q/r}$.
v. Sifat kanselasi: jika $\text{FPB}(q,r) = 1$, maka $xr \equiv yr \pmod{q}$ berlaku jika dan hanya jika kongruen $x \equiv y \pmod{q}$. Lebih umum lagi, jika $d = \text{FPB}(q,r)$ maka $xr \equiv yr \pmod{q}$berlaku jika dan hanya jika $x \equiv y \pmod{q/r}$.
vi. Sifat penjumlahan: jika $x \equiv y \pmod{q}$, maka $x + r \equiv y + r \pmod{q}$
vii. Sifat pengurangan: jika $x \equiv y \pmod{n}$, maka $x - r \equiv y - r \pmod{q}$
viii. Sifat invers: untuk x bilangan bulat positif dan $q \in \mathbb{Z}$, misalkan $x^{-1} \in \mathbb{Z}$ adalah invers perkalian dari x modulo q jika $xx^{-1} \equiv 1 \pmod{q}$.

Contoh 2. Di bawah ini merupakan contoh dari Teorema 3

i. Pilih $x = 5 \in \mathbb{Z}$, maka $5 \equiv 5 \pmod{19}$.
ii. Pilih $x = 7, y = 1 \in \mathbb{Z}$, $7 \equiv 1 \pmod{2}$ maka $1 \equiv 7 \pmod{2}$.
iii. Pilih $x = 19, y = 7, z = 1 \in \mathbb{Z}$, $19 \equiv 7 \pmod{2}$ dan $7 \equiv 1 \pmod{2}$ maka $19 \equiv 1 \pmod{2}$.
iv. Pilih $r = 2, x = 20, y = 16, c = 4$, maka $20 \equiv 16 \pmod{4}$ kongruen ke $10 \equiv 8 \pmod{2}$.
v. Pilih $r = 3, x = 20, y = 16, q = 4, \gcd(3,4) = 1$, maka $20 \times 3 \equiv 16 \times 3 \pmod{4}$ kongruen ke $20 \equiv 16 \pmod{4}$.
vi. Pilih $r = 2, x = 20, y = 16, q = 4$, maka $20 + 2 \equiv 16 + 2 \pmod{4}$ kongruen ke $22 \equiv 18 \pmod{4}$.
vii. Pilih $r = 2, x = 20, y = 16, q = 4$, maka $20 - 2 \equiv 16 - 2 \pmod{4}$ kongruen ke $18 \equiv 14 \pmod{4}$.
viii. Pilih $x = 9, x^{-1} = 3, q = 26$ maka $xx^{-1} \equiv 9 \cdot 3 \pmod{26} \equiv 1 \pmod{26}$

Teorema 2. (Teorema Pembagian) [22] *Misalkan $x \neq 0, y \in \mathbb{Z}$. Terdapat bilangan-bilangan $q, r \in \mathbb{Z}$ sedemikian sehingga $y = xq + r$ dengan $0 \leq r < |x|$. Dalam hal ini, $|x|$ adalah nilai mutlak dari x. Lebih jauh, notasi $y = xq + r$ equivalen dengan $y \equiv r \pmod{q}$.*

2.2. Penyelesaian kongruensi linear

Kongruensi linear merupakan aspek yang penting dalam sistem kongruensi linear. Pada dasarnya, kongruensi linear adalah bentuk persamaan yang melibatkan hubungan modulus antara kedua bilangan bulat, yang mana bertujuan untuk menemukan solusi yang memenuhi kondisi kongruensi modulo tertentu.

Teorema 3. [8] *Misalkan $x, q \in \mathbb{Z}$ dengan $q > 0$. x memiliki invers perkalian modulo q jika dan hanya jika x dan q relatif prima.*

Eksistensi invers perkalian dari x modulo q hanya bergantung pada nilai modulo q. Yaitu, jika $x \equiv y \pmod{q}$, maka x memiliki invers jika dan hanya jika y juga punya invers. dengan sifat invers, jika $x \equiv y \pmod{q}$, maka untuk setiap x^{-1} berlaku $xx^{-1} \equiv 1 \pmod{q}$ jika dan hanya jika $yx^{-1} \equiv 1 \pmod{q}$

Teorema 4. [8] *Misalkan $x, y, z, q \in \mathbb{Z}$ dengan $q > 0$, dan misalkan $s = \text{FPB}(x, q)$. Jika $s|y$ atau $y/s \in \mathbb{Z}$ kongruensi $xz \equiv y \pmod{q}$ mempunyai solusi z_0 untuk suatu bilangan bulat z_0. Lebih jauh, untuk setiap bilangan bulat z memiliki solusi jika dan hanya jika $z \equiv z_0 \pmod{q/s}$ suatu bilangan bulat z_0. Jika $s \nmid y$, maka kongruensi $xz \equiv y \pmod{q}$ sehingga kongruensi tidak memiliki solusi suatu bilangan bulat z_0.*

Akibat 1. [8] *Misalkan $x, y, q \in \mathbb{Z}$ dengan $q > 0$. Jika x relatif prima dengan q, maka kongruensi $xz \equiv y \pmod{q}$ memiliki solusi z_0. Lebih jauh, untuk setiap bilangan bulat z memiliki solusi jika dan hanya jika $z \equiv z_0 \pmod{q}$.*

Teorema 5. (*Fermat's Little Theorem*) [21] *Untuk setiap bilangan bulat z dan p prima,* $z^{p-1} \equiv 1\ (mod\ p)$.

Bukti. Misalkan z bilangan bulat dan p bilangan prima maka $z^{p-1} \equiv 1 \pmod p$ kongruen ke $z^p \equiv z \pmod p$. Pembuktian dengan menggunakan induksi matematika,

1. Langkah Basis
   Untuk $z = 1$. Maka $1^p \equiv 1 \pmod p$ benar. Jadi, terbukti langkah basis.
2. Langkah Induksi
   Asumsikan bahwa $z = k$ atau $z^p \equiv z \pmod p$ bernilai benar. Akan dibuktikan untuk $z = k + 1$ atau $(k+1)^p \equiv (k+1) \pmod p$ benar. Dengan menggunakan teorema binomial,
   $$(k+1)^p = k^p + \binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + \cdots + \binom{p}{p-1} k + 1$$
   Catatan p membagi semua koefisien binomial karena $p \mid \binom{p}{k}$ untuk $1 \le k \le p-1$. Karena p bilangan prima, maka p membagi pembilang dari $\binom{p}{k}$. Maka diperoleh,
   $$(k+1)^p \equiv \left[k^p + \binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} + \cdots + \binom{p}{p-1} k + 1\right] \pmod p$$
   $$\equiv (k^p + 1) \pmod p$$
   Karena $k^p \equiv k \pmod p$ maka $(k+1)^p \equiv (k+1) \pmod p$. Jadi, terbukti langkah induksi.

Berdasarkan 1 dan 2 terbukti untuk setiap z bilangan bulat dan p bilangan prima, $z^p \equiv 1 \pmod p$. ■

Contoh 3. Bentuk sederhana dari $5^{2017} \pmod 7$ adalah

$$5^{2017} \pmod 7 \equiv 5^{6.336+1} \pmod 7$$
$$\equiv (5^{336})^6 . 5 \pmod 7$$

dengan menggunakan *Fermat's Little Theorem*,

$$(5^6)^{336} . 5 \pmod 7 \equiv (1)^{336} . 5 \pmod 7 \equiv 5 \pmod 7.$$

Teorema 6. (*Wilson Theorem*) [21] *Jika f adalah bilangan prima, maka* $(f-1)! \equiv -1\ (mod\ f)$.

Bukti. Kasus $f = 2$ diperoleh $2! \equiv 2 \pmod 1 \equiv -1 \pmod 1$. Untuk bilangan prima lebih dari sama dengan 3, misalkan g dan z adalah suatu bilangan bulat yang memenuhi kondisi $gz \equiv 1 \pmod f$ dengan sifat keberadaan invers g^{-1} yang berlaku $gg^{-1} \equiv 1 \pmod f$, di mana $g, g^{-1} \in \{2,3,\dots,p-1\}$. Terdapat tepat $\frac{1}{2}(f-3)$ pasangan bilangan yang kongruen dengan 1 modulo f. Oleh karena itu, kita dapat tuliskan,

$$1.2.3 \dots (f-2) \equiv 1 \pmod f$$
$$1.2.3 \dots (f-2)(f-1) \equiv (f-1) \pmod f$$
$$(f-1)! \equiv -1 \pmod f$$

Terbukti bahwa, jika f adalah bilangan prima, maka $(f-1)! \equiv -1 \pmod f$. ■

3. Hasil dan Pembahasan

Sistem kongruensi linear adalah sebuah sistem yang terdiri dari lebih satu kongruensi linear yang saling berkorespondensi. Bentuk umum dari sistem kongruensi linear adalah

$$\begin{cases} z \equiv p_1 \pmod{q_1} \\ z \equiv p_2 \pmod{q_2} \\ \vdots \\ z \equiv p_r \pmod{q_r} \end{cases}$$

Di mana:

z : nilai yang ingin dicari yang memenuhi seluruh kongruensi tersebut.
p_r : sisa dari pembagian z terhadap modulus q_r.
q_r : bilangan modulus dari masing-masing kongruensi.

3.1. Chinese Remainder Theorem

Misalkan $q_1, q_2, \dots, q_r$ adalah bilangan bulat positif sehingga $FPB(q_i, q_j) = 1$ untuk $i \neq j$. Sehingga sistem kongruensi linearnya adalah

$$\begin{cases} z \equiv p_1 \pmod{q_1} \\ z \equiv p_2 \pmod{q_2} \\ \vdots \\ z \equiv p_r \pmod{q_r} \end{cases}$$

Memiliki solusi yang simultan (solusi yang berlaku untuk semua kongruensi), yang unik dalam modulus bilangan $q_1 q_2 \dots q_r$

Contoh 4. Diberikan suatu sistem kongruensi linear

$$\begin{cases} z \equiv 3^{2024} \pmod 5 \\ z \equiv 3^{2024} \pmod 7 \\ z \equiv 3^{2024} \pmod{11} \end{cases}$$

Sistem kongruensi di atas dapat disederhakan menggunakan *Fermat's Litte Theorem*.

$$z \equiv 3^{2024} \pmod{11} \equiv (3^{10})^{202} . 3^4 \pmod{11}$$
$$\equiv (1)^{202} . 81 \pmod{11} \equiv 4 \pmod{11}.$$

Dengan cara yang sama, kasus kongruensi lainnya diperoleh $z \equiv 3^{2024}\ (mod\ 5) \equiv 1\ (mod\ 5)$ dan $z \equiv 3^{2024} \pmod 7 \equiv 2 \pmod 7$. Karena $FPB(5,7) = FPB(5,11) = FPB(7,11) = 1$ maka sistem kongruensi linear di atas dapat diselesaikan dengan menggunakan *Chinese Remainder Theorem*. Pilih $q = 5 \cdot 7 \cdot 11 = 385$ dan

$$Q_1 = \frac{q}{5} = 77 \qquad Q_2 = \frac{q}{7} = 55 \qquad Q_3 = \frac{q}{11} = 35$$

Maka kongruensi linearnya akan menjadi

$$77z \equiv 1 \pmod 5 \quad 55z \equiv 1 \pmod 7 \quad 35z \equiv 1 \pmod{11}$$

Nilai z yang memenuhi adalah $z_1 = 3$, $z_2 = 6$, dan $z_3 = 6$. Sehingga diperoleh solusi dari sistem kongruensi linear adalah

$$z = 1 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 4 \cdot 35 \cdot 6 = 1731$$

Diperoleh solusi yaitu $z = 1731 \equiv 191 \pmod{385}$.

3.2. Algoritma intelligent Inspection Tipe-I

Misalkan $\begin{cases} z \equiv p_1 \pmod{q_1} \\ z \equiv p_2 \pmod{q_2} \\ \vdots \\ z \equiv p_r \pmod{q_r} \end{cases}$ adalah sistem kongruensi linear, dimana $p_1, p_2, \dots, p_r$ bilangan bulat dan $q_1, q_2, \dots, q_r$ adalah bilangan bulat positif dengan $q_1 < q_2 < \cdots < q_r$. Misalkan $Q = \text{KPK}(q_1, q_2, \dots, q_r)$.

Langkah 1 : Cari nilai Q,

Langkah 2 : Mulai dengan solusi awal dari $z \equiv p_r \pmod{q_r}$,

Langkah 3 : Cari semua solusi berurutan dari kongruensi linear lainnya hingga solusi terbesar, yang kurang dari Q,

Langkah 4 : Uji apakah masing-masing solusi kongruensi tersebut memenuhi $r - 1$ kongruensi linear lainnya dalam sistem, atau tidak. Jika diperoleh satu solusi yang memenuhi, maka solusi tersebut adalah solusi umum khusus dari sistem tersebut. Setelah itu, kita berhenti. Jika tidak kita melanjutkan dengan cara yang sama sampai kita mendapatkan solusi yang diinginkan yang kurang dari Q.

Catatan : Ketika solusi tidak ada, maka dapat disimpulkan bahwa sistem tersebut tidak memiliki solusi.

Contoh 5. Diketahui suatu sistem kongruensi linear memenuhi kondisi berikut

$$\begin{cases} 2z \equiv 2 \pmod 7 \\ 4z \equiv 5 \pmod 9 \end{cases}$$

Penyelesaian awal dari sistem kongruensi linear menggunakan sifat kanselasi, sistem di atas menjadi

$$\begin{aligned} 2z &\equiv 2 \pmod 7 \\ z &\equiv 2 \pmod 7 \cdot 2^{-1} \pmod 7 \\ z &\equiv 1 \pmod 7 \end{aligned}$$

dan

$$\begin{aligned} 4z &\equiv 5 \pmod 9 \\ z &\equiv 5 \pmod 9 \cdot 4^{-1} \pmod 9 \\ z &\equiv 8 \pmod 9 \end{aligned}$$

Dengan algoritma *intelligent inspection tipe*-I, Nilai kpk$(7,9) = 63$. Pilih $z_0 = 2$ sebagai solusi awal dari $z \equiv 1 \pmod 7$. Dengan substitusi ke dalam sistem, $z_0 = 2$ bukan solusi dari kongruensi tersebut. Semua solusi z berdasarkan teorema pembagian memiliki bentuk $z = 1 + 7k$ dimana $k = 0,1,2, \dots$ dan $z < 63$.

Berdasarkan Tabel 1. dapat disimpulkan bahwa $z = 8$ salah satu solusi dari sistem. Lebih jauh lagi $z \equiv 15 \ (mod\ 63)$ merupakah solusi dari sistem kongruensi linear di atas.

Tabel 1. Solusi sistem kongruensi linear dengan algoritma *intelligent inspection tipe*-I

k	$z = 1 + 7k$	Apakah z solusi dari $z \equiv 8 \pmod 9$?	Catatan
0	1	Tidak	Bukan solusi dari sistem
1	8	Ya	Solusi dari sistem
2	15	Tidak	Bukan solusi dari sistem
3	22	Tidak	Bukan solusi dari sistem
4	29	Tidak	Bukan solusi dari sistem
5	36	Tidak	Bukan solusi dari sistem
6	43	Tidak	Bukan solusi dari sistem
7	50	Tidak	Bukan solusi dari sistem
8	57	Tidak	Bukan solusi dari sistem

Demikian contoh dari penggunaan algoritma *intelligent inspection type*-I untuk menyelesaikan sistem kongruensi linear, selanjutnya adalah teknik lain untuk meyelesaikan sistem kongruensi linear yaitu algoritma *intelligent inspection type*-II.

3.3. Algoritma Intelligent Inspection Tipe-II

Misalkan $\begin{cases} z \equiv p_1 \pmod{q_1} \\ z \equiv p_2 \pmod{q_2} \\ \vdots \\ z \equiv p_r \pmod{q_r} \end{cases}$ adalah sistem kongruensi linear, dimana $p_1, p_2, \dots, p_r$ bilangan bulat dan $q_1, q_2, \dots, q_r$ adalah bilangan bulat positif dengan $q_1 < q_2 < \cdots < q_r$.

Langkah 1 : Tentukan solusi awal dari $z \equiv p_r \pmod{q_r}$ yaitu p_r

Langkah 2 : Uji apakah p_r merupakan solusi dari setidaknya satu dari kongruensi linear lain yang tersisa (dari $n-1$ kongruensi) dalam sistem atau tidak.

Langkah 3 : Jika p_r adalah solusi $z \equiv p_{r-1} (mod\ q_{r-1})$. Hitung $KPK(q_{r-1}, q_r)$ dan solusi positif berturut – turut dari $p_r + k \cdot KPK(q_{r-1}, q_r)$ modulo $KPK(q_{r-1}, q_r)$ dimana $t = 0,1, \dots$ dengan syarat $p_r + k \cdot KPK(q_{r-1}, q_r)$ kurang dari $KPK(m_{n-2}, m_{n-1}, m_n)$. Selanjutnya, aplikasikan langkah 2 pada kongruensi linear dengan modulus m_{n-2}.

Langkah 4 : Dengan cara yang sama, diperoleh solusi umum z_0 dari sistem yang diberikan. Lebih jauh lagi, solusi apapun z dari sistem tersebut diberikan oleh $z \equiv p_r + k.KPK(q_2, \dots, q_r) \pmod{Q}$.

Catatan : jika solusinya tidak ada, maka dapat disimpulkan bahwa sistem tersebut tidak memiliki solusi.

Contoh 14. Diberikan sistem kongruensi linear sebagai berikut

$$\begin{cases} z \equiv 5 \pmod 7 \\ z \equiv 3 \pmod 8 \\ z \equiv 7 \pmod 9 \end{cases}$$

Mulai dengan $z \equiv 5\ (mod\ 7)$. Pilih $z_0 = 5$ sebagai solusi awal. Dengan menggunakan algoritma *intelligent inspection tipe*-II, solusi selanjutnya menggunakan kongruensi kedua, solusinya akan memiliki bentuk $z = 5 + 7k, k = 0,1,2, \dots$ dengan $z < \text{KPK}(7,8) = 56$. Pilih $k = 2$ sehingga solusinya adalah $19 = 5 + 7(2)$ dimana memenuhi $19 \equiv 3 \pmod 8$. Selanjutnya cari solusi selanjutnya dengan cara yang serupa dimana solusinya berbentuk $19 + k \cdot \text{KPK}(7,8) = 19 + 56k$ dengan $k = 0,1,2, \dots$ dengan $z < \text{KPK}(7,8,9) = 504$. Pilih $k = 3$ maka $187 = 19 + 56(3)$ karena memenuhi kongruensi ketiga. Solusi akhir dari sistem kongruensi di atas adalah $187 + 504k$ atau $z \equiv 187 \pmod{504}$.

Contoh 6. Solusi dari sistem kongruensi linear berikut dengan menggunakan *Chinese Remainder Theorem*, Algoritma *Intelligent Inspection* tipe-I dan Algoritma *Intelligent Inspection* tipe-II

$$\begin{cases} z \equiv 102^{2025} \pmod 5 \\ z \equiv 5! \pmod 7 \\ 2z \equiv 2024 \pmod 9 \end{cases}$$

Penggunaan *Fermat Little's Theorem* digunakan untuk menyederhanakan kasus kongruensi pertama yaitu $z \equiv 102^{2025} \pmod 5$. Bentuk $z \equiv 102^{2025} \pmod 5$ dapat disederhanakan menjadi $z \equiv (102^4)^{506} \cdot 102 \pmod 5 \equiv (2^4)^{506} \cdot 102 \pmod 5 \equiv 1^{506} \cdot 102 \pmod 5 \equiv 2 \pmod 5$. Bentuk $z \equiv 5! \pmod 7$ pada kongruensi kedua equivalen dengan $6z \equiv 6! \pmod 7$. Berdasarkan *Wilson Theorem*, diperoleh bahwa $(7-1)! \pmod 7 \equiv -1 \pmod 7$. Maka $6z \equiv -1 \pmod 7$. Dengan sifat kanselasi, diperoleh bahwa $z \equiv 6^{-1}(-1) \pmod 7 \equiv 6 \cdot 6 \pmod 7 \equiv 1 \pmod 7$. Kasus kongruensi ketiga, penyederhanaan dilakukan dengan menyederhanakan $2024 \pmod 9 \equiv 8 \pmod 9$. Sehingga kongruensinya menjadi $2z \equiv 8 \pmod 9$. Dengan menggunakan sifat kanselasi maka diperoleh $z \equiv 2^{-1} \pmod 9 \cdot 8 \pmod 9 \equiv 5 \cdot 8 \pmod 9 \equiv 4 \pmod 9$. Sehingga sistem kongruensi linearnya dapat disederhanakan menjadi,

$$\begin{cases} z \equiv 2 \pmod 5 \\ z \equiv 1 \pmod 7 \\ z \equiv 4 \pmod 9 \end{cases}$$

Sistem kongruensi linear di atas dapat diselesaikan dengan berbagai cara. Berdasarkan *Chinese Remainder Theorem*, pilih $q = 5 \cdot 7 \cdot 9 = 315$ dan

$$Q_1 = \frac{q}{5} = 63 \qquad Q_2 = \frac{q}{7} = 45 \qquad Q_3 = \frac{q}{9} = 35$$

Maka kongruensi linearnya menjadi

$$63z \equiv 1 \pmod 5 \quad 45z \equiv 1 \pmod 7 \quad 35z \equiv 1 \pmod 9$$

Nilai z yang memenuhi adalah $z_1 = 2, z_2 = 5$, dan $z_3 = 8$. Sehingga diperoleh solusi dari sistem kongruensi linear di atas adalah

$$z = 2 \cdot 63 \cdot 2 + 1 \cdot 45 \cdot 5 + 4 \cdot 35 \cdot 8 = 1597$$

Tabel 2. Solusi sistem kongruensi linear dengan algoritma intelligent inspection tipe-I

k	$z = 2 + 5k$	Apakah z solusi dari $z \equiv 1 \pmod 7$?	Apakah z solusi dari $z \equiv 4 \pmod 9$?	Catatan
0	2	Tidak	Tidak	Bukan solusi dari sistem
1	7	Tidak	Tidak	Bukan solusi dari sistem
2	12	Tidak	Tidak	Bukan solusi dari sistem
3	15	Tidak	Tidak	Bukan solusi dari sistem
4	22	Ya	Ya	Solusi dari sistem
5	27	Tidak	Tidak	Bukan solusi dari sistem
⋮	⋮	⋮	⋮	⋮
62	312	Tidak	Tidak	Bukan solusi dari sistem

Jadi, diperoleh solusi yaitu $z = 1597 \equiv 22 \pmod{315}$.

Cara alternatif lainnya, sistem kongruensi linear di atas dapat diselesaikan dengan algoritma *intelligent inspection tipe*-I. Nilai $\text{KPK}(5,7,9) = 315$. Pilih $z_0 = 2$ sebagai solusi awal dari $z \equiv 2 \pmod 5$. Dengan substitusi ke dalam sistem, $z_0 = 2$ bukan solusi dari kongrensi tersebut. Semua solusi z berdasarkan teorema pembagian memiliki bentuk $z = 2 + 5k$ dimana $k = 0,1,2 \ldots$ dan $z < 315$.

Berdasarkan Tabel 2. Dapat disimpulkan bahwa $z = 22$ salah satu solusi dari sistem. Lebih jauh lagi $z \equiv 22 \pmod{315}$ merupakan solusi dari sistem kongruensi linear di atas.

Sistem kongruensi linear di atas juga dapat diselesaikan dengan menggunakan Algoritma *Intelligent Inspection* tipe-II. Mulai dengan $z \equiv 2$ sebagai solusi awal. Solusinya akan memiliki bentuk $z = 2 + 5k, k = 0,1,2, \ldots$ dengan $z < \text{KPK}(5,7) = 35$. Dengan menggunakan kongruensi kedua pilih $k = 4$ maka $z = 2 + 5(4) = 22$. Selanjutnya cari solusi selanjutnya dengan kongruensi ketiga dimana solusinya akan berbentuk $22 + k \cdot \text{KPK}(5,7) = 22 + 35\text{k}$ dengan $k = 0,1,2, \ldots$ dengan $z < \text{KPK}(5,7,9) = 315$. Pilih $k = 0$ maka $22 = 22 + 35(0)$ memenuhi kongruensi ketiga. Solusi akhir dari sistem kongruensi di atas adalah $22 + 315k$ atau $z \equiv 22 \pmod{315}$.

4. Kesimpulan

Kongruensi merupakan alat penting dalam menyelesaikan berbagai persoalan dalam teori bilangan. Pada makalah ini, dibahas mulai dari berbagai sifat dasar hingga teorema-teorema khusus yang berkaitan dengan kongruensi. Dengan berbagai konsep mengenai kongruensi, dibangunnya konsep sistem kongruensi linear. Proses pencarian solusi untuk sistem kongruensi linear pun dapat diperoleh melalui berbagai metode yaitu *Chinese Remainder Theorem*, Algoritma *Intelligent Inspection* tipe-I dan Algoritma *Intelligent Inspection* tipe-II sehingga memberikan fleksibilitas dalam pendekatan dan penerapannya.

Daftar Pustaka

1. Rahma, A. N., Rahmawati, R., & Wahyuni, W. 2020. Metode Eliminasi Gauss untuk Penyelesaian Sistem Kongruensi Linier. *Jurnal Sains Matematika dan Statistika*, *6*(1), 30. https://doi.org/10.24014/jsms.v6i1.9250.
2. Cuarto, P. 2017. Algebraic Method for Solving System of Linear Congruences. *Recoletos Multidisciplinary Research Journal*, *3*(1), 93–99. https://doi.org/10.32871/rmrj1503.01.07.
3. Bibak, K., Kapron, B. M., Srinivasan, V., Tauraso, R., & Tóth, L. 2017. Restricted linear congruences. *Journal of Number Theory*, *171*, 128–144. https://doi.org/10.1016/j.jnt.2016.07.018.
4. Namboothiri, K. V. 2018. On the number of solutions of a restricted linear congruence. *Journal of Number Theory*, *188*, 324–334. https://doi.org/10.1016/j.jnt.2018.01.013.
5. Wardani, R. D. 2019. The Application of Number Theory to Determine Congruence in Traffic Lights. *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, *13*(1), 047–052. https://doi.org/10.30598/barekengvol13iss1pp047-052ar697.
6. Orhani, S., & Çeko, B. 2023. Some applications of linear congruence from number theory, *3*(2). https://doi.org/10.5281/zenodo.8141702.
7. Ramli, Fitriana, L., Hidayat, D., & Priyowidodo, S. 2019. Application of linear congruent method in try out examination based on web application. *Journal of Physics: Conference Series*, *1361*(1), 012073. https://doi.org/10.1088/1742-6596/1361/1/012073.

8. Tadesse, S., & Molla, M. 2019. An Algorithm to Solve A System of Linear Congruences with Applications. *Mathematical Theory and Modeling*. https://doi.org/10.7176/mtm/9-10-05.
9. Shi, Z., Fang, Y., & Song, H. 2024. Intelligent Inspection Method and System of Plastic Gear Surface Defects Based on Adaptive Sample Weighting Deep Learning Model. *Sensors*, *24*(14), 4660. https://doi.org/10.3390/s24144660.
10. Elliott, J., & Schost, É. 2024. Some Applications of Chinese Remainder Theorem Codes with Error-Correction under Creative Commons License Attribution 4.0 International (CC BY 4.0). Retrieved from http://ceur-ws.org
11. Alhassan, E. A., Tian, K., Abban, O. J., Ohiami, I. E., Michael Adjabui, M., Armah, G., & Agyemang, S. 2021. On Some Algebraic Properties of the Chinese Remainder Theorem with Applications to Real Life. *Journal of Applied Mathematics and Computation*, *5*(3), 219–224. https://doi.org/10.26855/jamc.2021.09.008.
12. Dairi, M. S., Setiani Asih, M., & author, corespondent. 2022. *Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan Implementation Of RSA Cryptographic Algorithms in Library Information System Applications*. *Januari* (Vol. 2023). Retrieved from https://jurnal.unity-academy.sch.id/index.php/jirsi/index
13. Muchlis, B. S., Budiman, M. A., & Rachmawati, D. 2017. Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. *Jurnal & Penelitian Teknik Informatika*, *2*(2).
14. Beno, I. S., Direvisi, D. :, & Dipublikasi, : 2023. *Analisis Teorema Sisa Cina dalan Dekripsi Data Text Terenkripsi RSA Abstrak Sejarah Artikel* (Vol. 1). Retrieved from https://ejurnal.fmipa.uncen.ac.id/index.php/KJTIP40
15. Obaid, T. S. 2020. Study A Public Key in RSA Algorithm. *European Journal of Engineering and Technology Research*, *5*(4), 395–398. https://doi.org/10.24018/ejeng.2020.5.4.1843.
16. Harahap, A. A., & Hasibuan, N. A. 2020. Implementation of LCM (Linear Congruent Method) Method in Region Song Game. *The IJICS (International Journal of Informatics and Computer Science)*, *4*(2), 57. https://doi.org/10.30865/ijics.v4i2.2118.
17. Ilmu Matematika Dan Terapan, J., & Desember, |. 2017. *Penerapan Teori Kongruensi Dalam Permainan Nim* (Vol. 11).
18. Purnamasari, D. R. 2016. *Implementasi Linear Congruent Method (LCM) Pada Game Hangaroo Berbasis Android*. *Jurnal Riset Komputer (JURIKOM)*. Retrieved from http://hangaroo.id.downloadastro.com,
19. Amrullah, & Al-khowarizmi. 2022. Implementation Of Linear Congruent Method in Online Exam Applications For SMK Students. Retrieved from http://infor.seaninstitute.org/index.php/infokum/index
20. Jasri, M., & Toyib, J. 2023. *Android-Based Muhammadiyah Organization Introduction Application Using the Linear Congruent Generator Method*. *Jurnal Media Computer Science* (Vol. 2). Article History.
21. Burton, D. M. . 2011. *Elementary number theory*. McGraw-Hill.
22. Kurniadi, E., Carnia, E., & Gusriani, N. 2021. *Pengantar Teori Grup Hingga*. Tahta Media Group.