MODUL 4

KONGRUENSI LINIER

Gatot Muhsetyo

Pendahuluan

Dalam modul kongruensi linier ini diuraikan tentang sifat-sifat dasar kongruensi linier dan penyelesaiannya, kongruensi linier simultan, teorema sisa China, system kongruensi linier, dan penerapan kongruensi linier.

Sebagai bahasan yang berkaitan dengan aljabar (biasa), kongruensi linier serupa dengan persamaan linier, tetapi dengan semesta pembicaraan himpunan bilangan modulo. Meskipun demikian, terdapat banyak uraian dalam kongruensi linier yang memerlukan pemahaman yang berbeda dengan persamaan linier, misalnya terkait dengan banyaknya selesaian, yaitu kongruensi linier dapat tidak mempunyai selesaian, dan mempunyai satu atau lebih selesaian. Berikutnya, berbeda dengan persamaan linier satu variabel yang tidak bisa digabung dengan persamaan linier satu variabel yang lain, dua atau lebih kongruensi linier dapat digabung dan gabungannya disebut kongruensi linier simultan. Pada akhirnya pembahasan kongruensi linier yang serupa dengan persamaan linier adalah system kongruensi linier, dengan banyak variabel sama dengan banyaknya kongruensi.

Kompetensi Umum

Kompetensi Umum dalam mempelajari modul ini adalah mahasiswa mampu memahami konsep dan sifat kongruensi linier, penyelesaian kongruensi linier, kongruensi linier simultan, dan sistem kongruensi linier.

Kompetensi Khusus

Kompetensi Khusus dalam mempelajari modul ini adalah mahasiswa mampu menjelaskan konsep kongruensi linier dan sifat-sifatnya, konsep kongruensi linier simultan dan sifat-sifatnya, konsep sistem kongruensi linier dan sifat-sifatnya, serta keterkaitan satu sama lain untuk diterapkan dalam menyelesaikan masalah-masalah tertentu.

Susunan Kegiatan Belajar

Modul 4 ini terdiri dari dua Kegiatan Belajar. Kegiatan Belajar pertama adalah Kongruensi Linier, dan Kegiatan Belajar kedua adalah Sistem Kongruensi Linier. Setiap kegiatan belajar memuat Uraian, Contoh, Tugas dan Latihan, Rambu-Rambu Jawaban Tugas dan Latihan, Rangkuman, dan Tes Formatif. Pada bagian akhir modul 2 ini ditempatkan Rambu-Rambu Jawaban Tes Formatif 1 dan Tes Formatif 2.

Petunjuk Belajar

1. Bacalah Uraian dan Contoh dengan cermat dan berulang-ulang sehingga Anda benar-benar memahami dan menguasai materi pembahasan.
2. Kerjakan Tugas dan Latihan yang tersedia secara mandiri. Jika dalam kasus atau tahapan tertentu Anda mengalami kesulitan menjawab, maka pelajarilah Rambu-Rambu Jawaban Tugas dan Latihan. Jika langkah ini belum berhasil menjawab permasalahan, maka mintalah bantuan tutor Anda, atau orang lain yang lebih tahu.
3. Kerjakan Tes Formatif secara mandiri, dan periksalah Tingkat Penguasaan Anda dengan cara mencocokkan jawaban Anda dengan Rambu-Rambu Jawaban Tes Formatif. Ulangilah pengerjaan Tes Formatif sampai Anda benar-benar merasa mampu mengerjakan semua soal dengan benar.

MODUL 4

KEGIATAN BELAJAR 1

KONGRUENSI LINIER

Uraian

Di dalam aljabar (biasa), pembahasan utama tentang persamaan adalah mencari **akar,** atau **selesaian** dari persamaan polinomial dengan koefisien bulat f(x) = 0 dengan :

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_o$

Nilai-nilai x yang memenuhi persamaan f(x) = 0 disebut akar atau selesaian persamaan f(x) = 0 . Persamaan f(x) = 0 berderajad n paling banyak mempunyai n selesaian.

Serupa dengan persamaan aljabar, pembahasan utama kongruensi adalah mencari bilangan-bilangan bulat yang memenuhi $f(x) \equiv 0 \pmod{m}$ dengan :

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_o$

Sebagai peragaan, kongruensi

$f(x) \equiv x^3 + 6x^2 - 11 \equiv 0 \pmod{5}$

dipenuhi oleh x = 3 sebab jika x diganti 3 diperoleh pernyataan yang benar :

$f(3) = 3^3 + 6.3^2 - 11 = 27 + 54 - 11 \equiv 0 \pmod{5}$

Nilai x = 3 disebut **selesaian** kongruensi $f(x) = x^3 + 6x^2 - 11 \equiv 0 \pmod{5}$.

Menyelesaikan kongruensi berarti mencari selesaian kongruensi.

Definisi 4.1

Ditentukan f(x) adalah suatu polynomial dengan koefisien-koefisien bulat, dan $\{a_o , a_1 , \dots , a_{m-1}\}$ adalah suatu system residu yang lengkap modulo m.

Banyaknya selesaian kongruensi :

$f(x) \equiv 0 \pmod{m}$

adalah banyaknya a_i , dengan $a_i = 0,1,2, \dots , m - 1$ yang memenuhi kongruensi :

$f(a_i) \equiv 0 \pmod{m}$

Kita perlu memperhatikan bahwa jika $x = x_o$ adalah suatu selesaian kongruensi $f(x) \equiv 0 \pmod{m}$, dan diketahui $x_1 \equiv x_o \pmod{m}$, maka :

$f(x_1) \equiv f(x_o) \pmod{m} \equiv 0 \pmod{m}$

Dengan demikian x_1 adalah juga suatu selesain. Jadi, jika satu unsure dari suatu klas kongruensi modulo m adalah suatu selesaian, maka semua unsur dari klas kongruensi modulo m adalah juga selesaian-selesaian. Banyaknya selesaian suatu kongruensi modulo m adalah banyaknya selesaian tidak kongruen modulo m, yaitu banyaknya m klas kongruensi modulo m yang memberikan selesaian.

Contoh 4.1

Diketahui $f(x) = 2x - 4$

Banyaknya selesaian dari $f(x) = 2x - 4 \equiv 0 \pmod 6$ ditentukan oleh banyaknya unsur tidak kongruen dari suatu sistem residu lengkap modulo 6, atau dari banyaknya klas residu modulo 6 yang memberikan satu unsur yang memenuhi kongruensi. Untuk keperluan menyelesaikan $f(x) = 2x - 4 \equiv 0 \pmod 6$, suatu langkah yang lebih mudah adalah dengan mengambil $\{0,1,2,3,4,5\}$ sebagai suatu sistem residu yang lengkap modulo 6. Karena pasangan unsur-unsur himpunan $\{0,1,2,3,4,5\}$ tidak ada yang kongruen, maka selesaian dari $f(x) = 2x - 4 \equiv 0 \pmod 6$ dapat dilakukan dengan mencari unsur-unsur $\{0,1,2,3,4,5\}$ yang memenuhi kongruensi, yaitu :

$f(0) = 2.0 - 4 = -4$, tidak kongruen 0 (mod 6)

$f(1) = 2.1 - 4 = -4$, tidak kongruen 0 (mod 6)

$f(2) = 2.2 - 4 = 0 \equiv \pmod 6$

$f(3) = 2.3 - 4 = 2$, tidak kongruen 0 (mod 6)

$f(4) = 2.4 - 4 = 4$, tidak kongruen 0 (mod 6)

$f(5) = 2.5 - 4 = 6 \equiv 0 \pmod 6$

Dengan demikian selesaian kongruensi adalah $x \equiv 2 \pmod 6$ dan $x \equiv 5 \pmod 6$, dan banyaknya selesaian adalah dua.

Definisi 4.2

Suatu kongruensi yang mempunyai bentuk :

$$ax \equiv b \pmod m$$

dengan a, b, m $\in$ Z disebut suatu **kongruensi linier satu variabel.**

Perhatikan bahwa jika $x = x_o$ adalah suatu selesaian $ax \equiv b \pmod m$, dan jika diketahui bahwa $x_1 \equiv x_o \pmod m$, maka $ax_1 \equiv ax_o \pmod m$, dengan demikian x_1 juga suatu selesaian.

Contoh 4.2

Kongruensi linier $7x \equiv 3 \pmod{12}$ mempunyai satu selesaian $x \equiv 9 \pmod{12}$ sebab $x = 9$ merupakan satu-satunya unsur dalam suatu klas residu modulo 12 yang memberikan satu unsur yang memenuhi kongruensi. Dengan demikian $x = 9$ merupakan satu unsur dari suatu sistem residu yang lengkap modulo 12 yang memenuhi kongruensi, x = 9 adalah satu unsur dari sistem residu lengkap modulo 12 yaitu {0,1,2,3,4,5,6,7,8,9,10,11}

Contoh 4.3

Kongruensi linier $6x \equiv 9 \pmod{15}$ mempunyai tiga selesaian, $x = 4 + 15r$, $x = 9 + 15r$, dan $x = 14 + 15r$ untuk sebarang bilangan bulat r.

Nilai-nilai x $\in$ {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14} tidak ada yang memenuhi kongruensi $6x \equiv 9 \pmod{15}$ selain 4, 9, dan 14.

Berikut ini adalah suatu teorema yang penting karena dapat memberikan alasan dapat atau tidak dapat suatu kongruensi linier diselesaikan, serta memberikan jawaban tentang banyaknya selesaian suatu kongruensi linier.

Teorema 4.1

Jika $(a,m) = d$ dan kongruensi $ax \equiv b \pmod{m}$ mempunyai selesaian, maka $d \mid b$

Jika $d \mid b$, maka kongruensi $ax \equiv b \pmod{m}$ mempunyai d selesaian.

Bukti :

$ax \equiv b \pmod{m}$, maka menurut definisi 3.1, $m \mid ax - b$

Diketahui $d = (a,m)$, maka menurut definisi 2.3, $d \mid a$ dan $d \mid m$. Karena $d \mid a$, maka sesuai teorema 2.1, $d \mid ax$ untuk sebarang bilangan bulat x. Selanjutnya, dari $d \mid m$ dan $m \mid ax - b$, sesuai dengan teorema 2.2, $d \mid ax - b$.

Berdasarkan teorema 2.9, $d \mid ax$ dan $d \mid ax - b$, berakibat $d \mid -b$, sehingga $d \mid b$.

Selanjutnya, $ax \equiv b \pmod{m}$ dapat dinyatakan sebagai $d(a/d)x \equiv d(b/d) \pmod{m}$, dan sesuai dengan teorema 3.6 (a), dapat ditentukan $(a/d)x \equiv (b/d) \pmod{m/d}$.

Karena $(a/d,m/d) = 1$ dan $(a/d)x \equiv (b/d) \pmod{m/d}$, maka menurut teorema 3.10, kongruensi linier $(a/d)x \equiv (b/d) \pmod{m/d}$ mempunyai suatu selesaian $x = x_o + t.\frac{m}{d}$

dengan $x_o \equiv (\frac{a}{d})^{\phi(m)-1}.(\frac{b}{d}) \pmod{m}$ dan $t \in Z$. Dengan demikian seluruh selesaian kongruensi adalah :

$$x = x_0 \text{ , } x_0 + 1(\frac{m}{d}) \text{ , } x_0 + 2(\frac{m}{d}) + \ldots + x_0 + (d-1)(\frac{m}{d})$$

Contoh 4.4

Selesaikan kongruensi-kongruensi linier :

(a) $36x \equiv 8 \pmod{102}$

(b) $3x \equiv 2 \pmod 5$

(c) $15x \equiv 6 \pmod{18}$

Jawab :

(a) $(36,102) = 6$ dan 6 tidak membagi 8, maka $36x \equiv 8 \pmod{102}$ tidak mempunyai selesaian.

(b) $(3,5) = 1$ dan $1 \mid 2$, maka $3x \equiv 2 \pmod 5$ mempunyai satu selesaian $x \equiv 4 \pmod 5$

(c) $(15,18) = 3$ dan $3 \mid 6$, maka $15x \equiv 8 \pmod{18}$ mempunyai tiga selesaian, yaitu $x \equiv 4,10,16 \pmod{18}$

Contoh 4.5

Selesaikan kongruensi linier $144x \equiv 216 \pmod{360}$

Jawab:

FPB dari 144 dan 360 dicari dengan menggunakan teorema 2.20 Algoritma Euclides

$360 = 2.144 + 72$

$144 = 2.72 + 0$

$(144,360) = 72$

$72 \mid 216$, maka $144x \equiv 216 \pmod{360}$ mempunyai 72 selesaian. Seluruh selesaian dicari sebagai berikut :

$144x \equiv 216 \pmod{360}$

$2x \equiv 3 \pmod 5$

$x \equiv 2^3.3 \pmod 5 \equiv 8.3 \pmod 5 \equiv 4 \pmod 5$

Selesaian kongruensi linier $144x \equiv 216 \pmod{360}$ adalah :

$x \equiv 4,\ 4 + 1.5,\ 4 + 2.5,\ \dots,\ 4 + (72 - 1).5 \pmod{360}$

$x \equiv 4,\ 9,\ 14,\ \dots,\ 359 \pmod{360}$

Perhatikan tiga hal dalam menyelesaikan kongruensi linier.

(1) $ax \equiv ay \pmod m$ diselesaikan melalui $x \equiv y \left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$

(2) $ax \equiv ay \pmod m$ dan $(a,m) = 1$ diselesaikan melalui $x \equiv y \pmod m$

(3) $ax \equiv b \pmod m$ dengan nilai-nilai a, b, dan m yang relative besar dilakukan dengan menyederhanakan kongruensi, yaitu mengganti kongruensi semula dengan kongru-

ensi lain yang mempunyai bilangan modulo lebih kecil. Prosedur ini bisa diulangi sampai diperoleh suatu kongruensi yang selesaiannya mudah ditentukan.

Diketahui kongruensi linier $ax \equiv b \pmod{m}$, misalkan $a < m$ (jika $a > m$, maka a dapat "dikecilkan" dengan jalan mencari residu (sisa) positif terkecil dari a modulo m).

$ax \equiv b \pmod{m}$, maka $m \mid ax - b$, sehingga $ax - b = my$ untuk suatu $y \in Z$, berarti $my + b = ax$, dan akibatnya $a \mid my + b$, atau $my \equiv -b \pmod{a}$. Karena $m > a$, maka m dapat "dikecilkan" dengan jalan mencari residu positif terkecil dari m modulo a. Sampai pada tahap ini jelas bahwa kongruensi linier semula $ax \equiv b \pmod{m}$ berubah menjadi kongruensi linier $my \equiv -b \pmod{a}$ yang lebih "sederhana" karena mempunyai modulo a yang lebih kecil dari a.

Selesaikan kongruensi linier $my \equiv -b \pmod{a}$ jika memang sudah menjadi lebih mudah untuk diselesaikan, misalkan selesaiannya adalah $y = y_o$. Dengan demikian dari $ax - b = my$, atau $x = \dfrac{my+b}{a}$, dapat ditentukan bahwa $x_0 = \dfrac{my_0+b}{a}$ merupakan suatu selesaian kongruensi linier $ax \equiv b \pmod{m}$.

Ulangi langkah serupa jika memang kongruensi linier $my \equiv -b \pmod{a}$ masih sulit untuk diselesaikan. Misalkan residu positif terkecil m modulo a adalah k, maka $my \equiv -b \pmod{a}$ dapat diubah menjadi $az \equiv b \pmod{a}$. Demikian seterus-sehingga pada tahapan tertentu dapat diperoleh suatu selesaian, dan dari selesaian yang diperoleh dapat diproses mundur sehingga diperoleh selesaian dari kongruensi $ax \equiv b \pmod{m}$.

Contoh 4.6

Selesaikan $10x \equiv 3 \pmod{23}$

Jawab :

Dari $10x \equiv 3 \pmod{23}$ dapat diperoleh kongruensi lain yang lebih "sederhana", misalnya dengan variabel y, yaitu $23y \equiv -3 \pmod{10}$, dan berikutnya dapat dicari residu positif terkecil 23 modulo 10, yaitu 3, sehingga diperoleh kongruensi $3y \equiv -3 \pmod{10}$, dan kita sudah dapat menentukan selesaian $3y \equiv -3 \pmod{10}$ yaitu $y \equiv -1 \pmod{10}$ atau $y \equiv 9 \pmod{10}$, berarti $y_o = 9$, sehingga dapat ditentukan $x_0 = \dfrac{23y_0+3}{10} = \dfrac{23.9+3}{10} = 21$

Contoh 4.7

Selesaikan 19x ≡ 2 (mod 49)

Jawab :

Dari 19x ≡ 2 (mod 49) dapat diperoleh kongruensi lain 49y ≡ – 2 (mod 19) atau 11y ≡ – 2 (mod 19). Karena kita relative masih sulit untuk menentukan selesaian 11y ≡ – 2 (mod 19) , maka langkah serupa dilakukan dengan memilih suatu variabel lain sehingga diperoleh 19z ≡ 2 (mod 11), atau 8z ≡ 2 (mod 11). Karena kita merasakan masih sulit untuk menyelesaikan, langkah serupa diulang sehingga diperoleh 11r ≡ – 2 (mod 8), atau 3r ≡ – 2 (mod 8). Ternyata kita sudah lebih mumemperoleh selesaian, yaitu $r_0 \equiv 2 \pmod 8$, selanjutnya $z_0 = (11r_0 + 2)/8 = 3$, $y_0 = (19z_0 - 2)/11 = 5$, dan $x_0 = (49y_0 + 2)/19 = 13$. Selesaian kongruensi adalah x ≡ 13 (mod 49)

Jika kita cermati contoh 4.7, langkah-langkah memperoleh selesaian dapat diperagakan sebagai berikut :

19x ≡ 2 (mod 49) → $x_0 = \dfrac{49y_0 + 2}{19} = 13$

49y ≡ -2 (mod 19)

11y ≡ -2 (mod 19) → $y_0 = \dfrac{19z_0 - 2}{11} = 5$

19z ≡ 2 (mod 11)

8z ≡ 2 (mod 11) → $z_0 = \dfrac{11r_0 + 2}{8} = 3$

11r ≡ -2 (mod 8)

3r ≡ -2 (mod 8) → $r_0 = 2$

Contoh 4.8

Selesaikan kongruensi linier 67320x ≡ 136 (mod 96577)

Jawab :

(67320,96577) dicari dengan menggunakan teorema 2.20 Algoritma Euclides :

96577 = 1.67320 + 29257

67320 = 2.29257 + 8806

29257 = 3.8806 + 2839

8806 = 3.2839 + 289

2839 = 9.289 + 238

289 = 1.238 + 51

238 = 4.51 + 34

51 = 1.34 + 17

34 = 2.17 + 0

Karena (67320,96577) = 17, dan 17 | 136, maka kongruensi dapat diselesaikan dan mempunyai 17 selesaian.

Selanjutnya, dari 67320x ≡ 136 (mod 96577), atau :

17.3960 x ≡ 17.8 (mod 17.5681)

dengan (67320,96577) = 17, kita dapat menggunakan teorema 3.6 (a) sehingga diperoleh 3960 x ≡ 8 (mod 5681), dan diselesaikan seperti uraian sebelumnya.

$3960\,x \equiv 8 \pmod{5681} \rightarrow x_0 = \dfrac{5681y_0 + 8}{3960} = 4694$

$5681\,y \equiv -8 \pmod{3960}$

$1721\,y \equiv -8 \pmod{3960} \rightarrow y_0 = \dfrac{3960z_0 - 8}{1721} = 3272$

$3960\,z \equiv 8 \pmod{1721}$

$518\,z \equiv 8 \pmod{1721} \rightarrow z_0 = \dfrac{1721r_0 + 8}{518} = 1422$

$1721\,r \equiv -8 \pmod{518}$

$167\,r \equiv -8 \pmod{518} \rightarrow r_0 = \dfrac{518s_0 - 8}{167} = 428$

$518\,s \equiv 8 \pmod{167}$

$17\,s \equiv 8 \pmod{167} \rightarrow s_0 = \dfrac{167t_0 + 8}{17} = 138$

$167\,t \equiv -8 \pmod{17}$

$14t \equiv -8 \pmod{17} \quad \rightarrow \quad t_0 = \dfrac{17m_0 - 8}{14} = 14$

$17m \equiv 8 \pmod{14}$

$3m \equiv 8 \pmod{14} \quad \rightarrow \quad m_0 = 12$

Selesaian kongruensi adalah :

$x \equiv 4694, 4694 + 1.5681, \ldots, 4694 + 16.5681 \pmod{96577}$

$x \equiv 4694, 10375, \ldots, 95560 \pmod{96577}$

Marilah sekarang kita bahas lebih lanjut gabungan dari dua atau lebih kongruensi linier dengan satu variabel, dan gabungan ini disebut **sistem kongruensi linier simultan**.

Definisi 4.3

Sistem kongruensi linier satu variabel :

$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_r \pmod{m_r}$,

disebut system kongruensi linear simultan

Untuk mencari selesaian system kongruensi linier simultan, kita memerlukan pembahasan awal tentang system yang terdiri dari dua kongruensi linier.

Teorema 4.2

Sistem kongruensi linier simultan :

$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$

dapat diselesaikan jika dan hanya jika $a_1 \equiv a_2 \pmod{(m_1, m_2)}$

Bukti :

$(\rightarrow)$ Diketahui $x \equiv a_1 \pmod{m_1}$, maka sesuai teorema 3.1, $x = a_1 + m_1 k$, $k \in Z$

Selanjutnya, dari $x = a_1 + m_1 k$ dan $x \equiv a_2 \pmod{m_2}$, dapat ditentukan bahwa $a_1 + m_1 k \equiv a_2 \pmod{m_2}$, atau $m_1 k \equiv a_2 - a_1 \pmod{m_2}$

Sesuai teorema 4.1, kongruensi linier $m_1 k \equiv a_2 - a_1 \pmod{m_2}$ dapat diselesaikan jika $(m_1, m_2) \mid a_2 - a_1$, dan sesuai definisi 3.1, $a_1 \equiv a_2 \pmod{(m_1, m_2)}$

$(\leftarrow)$ Buktikan !

Teorema 4.2 juga memberikan petunjuk, jika banyaknya kongruensi linear dalam system yang simultan lebih dari dua, maka penyelidikan dapat dilakukan untuk semua kemungkinan pasangan kongruensi. Demikian pula dapat ditentukan, jika $(m_1, m_2) = 1$, maka system kongruensi linier simultan $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ selalu dapat diselesaikan, dan hal ini dapat diperluas untuk sistem kongruensi linier simultan yang terdiri lebih dari dua kongruensi linier.

Berikutnya, beberapa cara yang dapat digunakan menyelesaikan sistem kongruensi linier simultan adalah cara **biasa**, cara **iterasi**, dan cara sisa **China**.

Cara Biasa

Cara ini disebut biasa karena kita hanya membuat barisan bilangan yang memenuhi masing-masing kongruensi, dan dilanjutkan dengan pencarian unsur persekutuan dari semua kongruensi. Penetapan selesaian didasarkan pada teorema 3.6 (b).

Contoh 4.9

Selesaikan sistem kongruensi linier simultan $x \equiv 13 \pmod{16}$ dan $x \equiv 5 \pmod{14}$

Jawab :

$13 \equiv 5$ (mod (16,14), atau $8 \equiv 0 \pmod{2}$, maka sistem kongruensi dapat diselesai-kan.

$x \equiv 13 \pmod{16} \equiv 13,29,45,61,77,93,109, \ldots \pmod{16}$

$x \equiv 5 \pmod{14} \equiv 5,19,33,47,61,75,89,103, \ldots \pmod{14}$

Unsur persekutuan dari kedua kongruensi linier adalah 61, sehingga :

$x \equiv 61 \pmod{16}$ dan $x \equiv 61 \pmod{14}$

dan sesuai dengan teorema 3.6 (b), $x \equiv 61 \pmod{[16,14]} \equiv 61 \pmod{112}$

Contoh 4.10

Sistem kongruensi linier simultan $x \equiv 15 \pmod{51}$ dan $x \equiv 7 \pmod{42}$ tidak mempunyai selesaian sebab 15 tidak kongruen 7 modulo $(51,42) = 3$.

Meskipun sederhana dan mudah, cara biasa menjadi semakin sulit dan tidak efisien jika banyaknya kongruensi linier bertambah banyak, yaitu barisan atau daftar bilangan yang dibuat menjadi panjang.

Cara Iterasi

Makna iterasi memuat adanya langkah atau proses berulang. Ini berarti bahwa langkah berikutnya dikerjakan serupa setelah langkah sebelumnya dilakukan. Sebagai ilustrasi, jika ada tiga kongruensi linier yang simultan, maka dua kongruensi diselesaikan lebih dahulu, sehingga diperoleh selesaian, dilanjutkan dengan penyelesaian kongruensi ketiga dengan selesaian dua kongruensi yang telah dikerjakan.

Contoh 4.11

Selesaikan sistem kongruensi linier simultan $2x \equiv 3 \pmod 5$, $3x \equiv 4 \pmod 7$, dan $5x \equiv 8 \pmod{12}$

Jawab :

Ketiga kongruensi belum memenuhi syarat "baku", sehingga masing-masing perlu disesuaikan, diperoleh $x \equiv 4 \pmod 5$, $x \equiv 3 \pmod 7$, dan $x \equiv 4 \pmod{12}$.

$x = 4 + 5t$ sebab $x \equiv 4 \pmod 5$.

Dari substitusi $x = 4 + 5t$ kepada $x \equiv 3 \pmod 7$ diperoleh $4 + 5t \equiv 3 \pmod 7$, atau $5t \equiv -1 \pmod 7 \equiv 6 \pmod 7$, sehingga $t \equiv 4 \pmod 7$, atau $t = 4 + 7s$.

Dari substitusi $t = 4 + 7s$ kepada $x = 4 + 5t$ diperoleh $x = 4 + 5(4 + 7s) = 24 + 35s$.

Dengan demikian $x \equiv 24 \pmod{35}$.

Berikutnya kita akan menyelesaikan $x \equiv 24 \pmod{35}$ dan $x \equiv 4 \pmod{12}$.

$x \equiv 24 \pmod{35}$, berarti $x = 24 + 35s$.

Substitusi $x = 24 + 35s$ kepada $x \equiv 4 \pmod{12}$ diperoleh $24 + 35s \equiv 4 \pmod{12}$, $11s \equiv 4 \pmod{12}$, atau $s \equiv 8 \pmod{12}$, sehingga $s = 8 + 12r$.

Dari substitusi $s = 8 + 12r$ kepada $x = 24 + 35s$ diperoleh $x = 24 + 35(8 + 12r)$ $= 304 + 420s$. Dengan demikian $x \equiv 304 \pmod{420}$

Sebelum kita membicarakan cara China, marilah kita lihat suatu teorema yang diperlukan untuk membuktikan teorema sisa China.

Teorema 4.3

Jika $p_1 \mid q$, $p_2 \mid q$, dan $(p_1,p_2) = 1$, maka $p_1p_2 \mid q$

Bukti :

$(p_1,p_2) = 1$, maka sesuai teorema 2.12, $xp_1 + yp_2 = 1$ untuk suatu $x,y \in Z$, sehingga $xp_1q + yp_2q = q$.

$p_1 \mid q$ dan $p_2 \mid q$, maka sesuai teorema 2.8, $p_1p_2 \mid p_2q$ dan $p_1p_2 \mid p_1q$.

Selanjutnya, dari $p_1p_2 \mid p_2q$ dan $p_1p_2 \mid p_1q$, sesuai teorema 2.1, $p_1p_2 \mid yp_2q$ dan $p_1p_2 \mid xp_1q$, dan berdasarkan teorema 2.4, $pr \mid xpq + yqr$, atau $pr \mid q$.

Teorema 4.4

Jika $p_1 \mid q$, $p_2 \mid q$, … , $p_r \mid q$, dan $(p_1,p_2, \dots ,p_r) = 1$, maka $p_1p_2 \dots p_r \mid q$

Buktikan !

Cara China

Masalah kongruensi linier muncul pada awal abad satu, dan dapat ditemukan di dalam aritmetika matematisi China yang bernama Sun-Tsu (Rosen, 1993:136). Cara China untuk menyelesaikan system kongruensi linier didasarkan pada suatu teorema yang disebut **Teorema Sisa China**, dimana pasangan dari setiap dua modulo dari kongruensi adalah relatif prima.

Teorema 4.5. Teorema Sisa China

Ditentukan bahwa $m_1,m_2, \dots , m_r$ adalah bilangan-bilangan bulat positif yang setiap pasang adalah relative prima, dan $a_1,a_2, \dots , a_r$ adalah sebarang r bilangan bulat.

Sistem kongruensi linier simultan :

$$x \equiv a_1 \pmod{m_1} , x \equiv a_2 \pmod{m_2} , \dots , x \equiv a_r \pmod{m_r}$$

mempunyai suatu selesaian yang tunggal modulo $M = m_1.m_2 \dots m_r$

Bukti :

$M = m_1.m_2 \dots m_r$, dan ambil $M_i = M/m_i$, maka $m_i \mid M$ sehingga $(M_i ,m_i) = 1$ dengan $1 \le i \le r$.

Sesuai dengan teorema 4.1, karena $(M_i ,m_i) = 1$, maka tentu ada satu $b_i \in Z$ sedemikian hingga $M_ib_i \equiv 1 \pmod{m_i}$, dan $M_ib_i \equiv 0 \pmod{m_j}$ jika $i \neq j$.

Ambil $x = M_1b_1a_2 + M_2b_2a_2 + \dots + M_rb_ra_r$, maka x adalah suatu selesaian simultan dari r kongruensi linier. Untuk menunjukkan hal ini, kita harus membuktikan bahwa $x \equiv a_i \pmod{m_i}$ untuk $i = 1,2, \dots , r$.

$$\begin{aligned} x &= M_1b_1a_2 + M_2b_2a_2 + \dots + M_rb_ra_r \\ &\equiv (M_1b_1a_1 + M_2b_2a_2 + \dots + M_ib_ia_i + \dots + M_rb_ra_r) \pmod{m_i} \\ &\equiv (0.a_1 + 0.a_2 + \dots + 1.a_i + \dots + 0.a_r) \pmod{m_i} \end{aligned}$$

$$x \equiv a_i \pmod{m_i} , i = 1,2, \dots ,r$$

Untuk menunjukkan ketunggalan selesaian, dimisalkan ada dua selesaian yaitu x_0 dan x_1 , maka $x_0 \equiv x_1 \equiv a_i \pmod{m_i}$, yaitu $x_0 \equiv x_1 \pmod{m_i}$, atau $m_i \mid x_0 - x_1$.

Dengan demikian $m_1 \mid x_0 - x_1$, $m_2 \mid x_0 - x_1$, … , $m_r \mid x_0 - x_1$, dan sesuai dengan teorema 4.4, $m_1m_2 \dots m_r \mid x_0 - x_1$, atau $M \mid x_0 - x_1$, berarti $x_0 \equiv x_1 \pmod{M}$.

Jadi selesaian simultan dari r kongruensi linier adalah tunggal dengan modulo m.

Contoh 4.12

Selesaikan system kongruensi linier simultan $x \equiv 5 \pmod{8}$, $x \equiv 3 \pmod{7}$, dan $x \equiv 4 \pmod{9}$

Jawab :

$a_1 = 5$, $a_2 = 3$, $a_3 = 4$, $m_1 = 8$, $m_2 = 7$, dan $m_3 = 9$

$(m_1,m_2) = (m_1,m_3) = (m_2,m_3) = 1$

$M = m_1m_2m_3 = 8.7.9 = 504$

$(M/m_1)b_1 \equiv 1 \pmod{m_1}$, maka $7.9b_1 \equiv 1 \pmod{8}$, sehingga $b_1 = 7$

$(M/m_2)b_2 \equiv 1 \pmod{m_2}$, maka $8.9b_2 \equiv 1 \pmod{7}$, sehingga $b_2 = 4$

$(M/m_3)b_3 \equiv 1 \pmod{m_3}$, maka $8.7b_3 \equiv 1 \pmod{9}$, sehingga $b_3 = 5$

Jadi $x = 7.9.7.5 + 8.9.4.3 + 8.7.5.4 = 4189$

$x \equiv 157 \pmod{504}$

Contoh 4.13

Selesaikan system kongruensi linier simultan $3x \equiv 2 \pmod{5}$, $4x \equiv 3 \pmod{7}$, $8x \equiv 5 \pmod{9}$, dan $4x \equiv 7 \pmod{11}$

Jawab :

Masing-masing kongruensi linier perlu diubah menjadi kongruensi lain dengan koefisien x adalah 1 :

$3x \equiv 2 \pmod{5}$, maka $x \equiv 4 \pmod{5}$

$4x \equiv 3 \pmod{7}$, maka $x \equiv 6 \pmod{7}$

$8x \equiv 5 \pmod{9}$, maka $x \equiv 4 \pmod{9}$

$4x \equiv 7 \pmod{9}$, maka $x \equiv 10 \pmod{11}$

$a_1 = 4$, $a_2 = 6$, $a_3 = 4$, $a_4 = 10$, $m_1 = 5$, $m_2 = 7$, $m_3 = 9$, $m_4 = 11$

$(m_1,m_2) = (m_1,m_3) = (m_1,m_4) = (m_2,m_3) = (m_2,m_4) = (m_3,m_4) = 1$

$M = m_1m_2m_3m_4 = 5.7.9.11 = 3465$

$(M/m_1)b_1 \equiv 1 \pmod{m_1}$, maka $7.9.11b_1 \equiv 1 \pmod{5}$, sehingga $b_1 = 2$

$(M/m_2)b_2 \equiv 1 \pmod{m_2}$, maka $5.9.11b_2 \equiv 1 \pmod{7}$, sehingga $b_2 = 3$

$(M/m_3)b_3 \equiv 1 \pmod{m_3}$, maka $5.7.11b_3 \equiv 1 \pmod{9}$, sehingga $b_3 = 4$

$(M/m_4)b_4 \equiv 1 \pmod{m_4}$, maka $5.7.9b_4 \equiv 1 \pmod{9}$, sehingga $b_4 = 8$

Jadi $x = 7.9.11.2.4 + 5.9.11.3.6 + 5.7.11.4.4 + 5.7.9.8.10 = 4581$

$x \equiv 769 \pmod{3465}$

Tugas dan Latihan

Tugas

Setelah banyak mempelajari tentang bahan paparan pada kegiatan belajar 1 ini, maka cobalah jelaskan atau uraikan bagaiman cara menyelesaikan suatu sistem kongruensi linier simultan yang dapat diselesaikan tetapi tidak semua pasangan modulo adalah relatif prima.

Berikutnya, dari suatu kongruensi linier $ax \equiv b \pmod{m}$ y, pilih suatu nilai m lebih dari 10000, nilai a lebih dari 1000, dan nilai b lebih dari 10, sedemikian hingga $(a,m) > 1$ dan $(a,m) \mid b$. Selesaikan kongruensi linier ini.

Latihan

1. Selesaikan kongruensi linier $19x \equiv 1 \pmod{140}$ menggunakan teorema sisa China
2. Selesaikan kongruensi linier $29393x \equiv 4743 \pmod{2805}$
3. Selesaikan system kongruensi linier simultan $2x \equiv 8 \pmod{20}$ dan $3x \equiv 2 \pmod{7}$
4. Selesaikan system kongruensi linier simultan $x \equiv 1 \pmod{2}$, $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{7}$, dan $x \equiv 2 \pmod{11}$
5. Seorang gadis membawa sekeranjang telur. Jika telur-telur itu dihitung dua-dua, maka akan tertinggal satu telur. Jika telur-telur itu dihitung tiga-tiga, maka akan tertinggal dua telur. Jika dilanjutkan dengan menghitung lima-lima dan tujuh-tujuh, maka secara berturut-turut akan tertinggal empat telur dan enam telur. Tidak ada telur yang tertinggal jika dihitung sebelas-sebelas. Berapa banyaknya telur minimal di dalam keranjang ?

Rambu-Rambu Jawaban Tugas Dan Latihan

Rambu-Rambu Jawaban Tugas

Bagian dari kongruensi-kongruensi linier yang memenuhi syarat $(m_i,m_j) = 1$ untuk $i \neq j$ diselesaikan dengan teorema sisa China, dan bagian dari kongruensi-kongruensi yang lain diselesaikan dengan iterasi, kemudian gabungannya diselesaikan dengan memlih cara yang memungkinkan untuk digunakan.

Pilih suatu kongruensi $3375x \equiv 30 \pmod{21480}$. Gunakan Algoritma Euclides untuk mencari $(3375,21480)$ sehingga diperoleh 15. Karena 15 membagi 30, maka kongruensi linier mempunyai selesaian. Selesaikan dengan cara bertahap sehingga diperoleh :

$x \equiv 1362, 2794, \ldots, 21410 \pmod{21480}$

Rambu-Rambu Jawaban Latihan

1. $140 = 4.5.7$ dan $(4,5) = (4,7) = (5,7) = 1$, sehingga kongruensi $19x \equiv 30 \pmod{140}$ dapat dipecah menjadi sistem kongruensi linier simultan $19x \equiv 30 \pmod 4$, $19x \equiv 30 \pmod 5$, dan $19x \equiv 30 \pmod 7$

   Masing-masing kongruensi linier secara berturut-turut diubah menjadi $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, dan $x \equiv 3 \pmod 7$.

   $35b_1 \equiv 1 \pmod 4$, maka $b_1 = 3$

   $28b_2 \equiv 1 \pmod 5$, maka $b_2 = 2$

   $20b_3 \equiv 1 \pmod 7$, maka $b_3 = 6$

   $x = 35.3.3 + 28.2.4 + 20.6.3 = 899 \equiv 59 \pmod{140}$

2. $29393x \equiv 4743 \pmod{2805}$ diubah menjadi $1343x \equiv 1938 \pmod{2805}$

   $2805 = 2.1343 + 119$

   $1343 = 11.119 + 34$

   $119 = 3.34 + 17$

   $34 = 2.17 + 0$

   $(1343,2845) = 17$ dan $17 \mid 1938$, berarti terdapat 17 selesaian

   $1343x \equiv 1938 \pmod{2805}$

   $79x \equiv 114 \pmod{165} \quad \rightarrow x_0 = \dfrac{165.74+114}{79} = 156$

   $165y \equiv -114 \pmod{79}$

   $7y \equiv 44 \pmod{79} \quad \rightarrow y_0 = \dfrac{79.6+44}{7} = 74$

   $79z \equiv -44 \pmod 7$

   $2z \equiv 5 \pmod 7 \quad \rightarrow z_0 = 6$

   Jadi $x \equiv 156, 321, \ldots, 2796 \pmod{2805}$

3. $2x \equiv 8$ (mod 20 , maka $x \equiv 4 \pmod{20}$ dan $x \equiv 14 \pmod{20}$

   $3x \equiv 2 \pmod 7$, maka $x \equiv 3 \pmod 7$

   Dari kongruensi linier simultan $x \equiv 4 \pmod{20}$ dan $x \equiv 3 \pmod 7$,dengan cara biasa atau cara iterasi dapat diperoleh $x \equiv 24 \pmod{140}$

   Dari kongruensi linier simultan $x \equiv 14 \pmod{20}$ dan $x \equiv 3 \pmod 7$,dengan cara biasa atau cara iterasi dapat diperoleh $x \equiv 94 \pmod{140}$

4. Dari $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 4$, dan $x \equiv 1 \pmod 6$, dapat ditentukan bahwa $x \equiv 1$ (mod [2,3,4,5]), atau $x \equiv 1 \pmod{60}$.

   Selanjutnya, dari $x \equiv 2 \pmod 7$, dan $x \equiv 2 \pmod{11}$ dapat ditentukan bahwa $x \equiv 2 \pmod{77}$

   Dengan demikian $77b_1 \equiv 1 \pmod{60}$ dan $60b_2 \equiv 1 \pmod{77}$, sehingga diperoleh $b_1 = 53$ dan $b_2 = 9$

   Jadi $x = 77.53.1 + 60.9.2 = 5161 \equiv 541 \pmod{4620}$

5. Misalkan banyaknya telur sekeranjang adalah x, maka : $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 2 \pmod 7$, dan $x \equiv 0 \pmod{11}$

   Dari $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$, dan $x \equiv 2 \pmod 7$ dapat ditentukan bahwa $x \equiv 2 \pmod{105}$

   Dengan demikian dapat ditentukan suatu system kongruensi linier simultan

   $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod{105}$ dan $x \equiv 0 \pmod{11}$

   kemudian dapat dicari :

   $105.11b_1 \equiv 1 \pmod 2$, atau $b_1 = 1$

   $2.11b_2 \equiv 1 \pmod{105}$, atau $b_2 = 43$

   $105.2b_3 \equiv 1 \pmod{11}$, atau $b_3 = 1$

   Jadi $x = 105.11.1.1 + 2.11.43.2 + 105.2.1.0 = 3047 \equiv 737 \pmod{2310}$

   Banyaknya telur minimal dalam keranjang adalah 737.

   Jika tidak dibatasi oleh minimal, maka jawaban yang diperoleh banyak, yaitu :

   $737,\ 737 + 2310,\ 737 + 2.2310,\ \ldots,\ 737 + k.2310$ dengan $k \in Z^+$

Rangkuman

Berdasarkan seluruh paparan pada Kegiatan Belajar 1 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, dan penerapan dalam penyelesaian masalah terkait, terutama tentang konsep kongruensi linier , cara menyelesaikan kongruensi linier, konsep system kongruensi linier simultan, dan cara menyelesaikan system kongruensi linier simultan.

1. **Definisi 4.1** tentang banyaknya selesaian kongruensi
2. **Definisi 4.2** tentang kongruensi linier simultan satu variabel
3. Tiga hal yang perlu diperhatikan dalam menyelesaikan kongruensi linier
   (a) $ax \equiv ay \pmod m$ jika $(a,m)\ \ 1$
   (b) $ax \equiv ay \pmod m$ jika $(a,m) = 1$
   (c) $ax \equiv b \pmod m$ untuk nilai-nilai a, b, dan m yang relatif besar

4. **Definisi 4.3** tentang sistem kongruensi linier simultan
5. **Teorema 4.2**

   Sistem kongruensi linier simultan :

   $x \equiv a_1 (\text{mod } m_1),\ x \equiv a_2 (\text{mod } m_2)$

   dapat diselesaikan jika dan hanya jika $a_1 \equiv a_2$ (mod (m_1,m_2))

6 Cara-cara menyelesaikan sistem kongruensi linier simultan : cara biasa, cara iterasi, dan cara China

7. **Teorema 4.3**

   Jika $p_1 \mid q$, $p_2 \mid q$, dan $(p_1,p_2) = 1$, maka $p_1p_2 \mid q$

8. **Teorema 4.4**

   Jika $p_1 \mid q$, $p_2 \mid q$, … , $p_r \mid q$, dan $(p_1,p_2, \ldots ,p_r) = 1$, maka $p_1p_2 \ldots p_r \mid q$

9. **Teorema 4.5. Teorema Sisa China**

   Ditentukan bahwa $m_1,m_2, \ldots , m_r$ adalah bilangan-bilangan bulat positif yang setiap pasang adalah relative prima, dan $a_1,a_2, \ldots , a_r$ adalah sebarang r bilangan bulat.

   Sistem kongruensi linier simultan :

   $x \equiv a_1 \ (\text{mod } m_1)\ ,\ x \equiv a_2 \ (\text{mod } m_2)\ , \ldots ,\ x \equiv a_r \ (\text{mod } m_r)$

   mempunyai suatu selesaian yang tunggal modulo $M = m_1.m_2 \ldots \ m_r$

Tes Formatif 1

1. Skor 20

   Selesikan kongruensi linier $23x \equiv 17$ (mod 180) dengan dua cara:

   (a) cara penyelesaian kongruensi linier

   (b) cara penyelesaian sistem kongruensi linier simultan

2. Skor 20

   Sekelompok 13 orang perompak akan membagikan sekantung butir berlian.

   Dalam usaha pembagian pertama, ternyata tersisa 5 butir berlian, dan karena dirasa tidak bisa adil, terjadi perkelaihan dan 4 perompak terbunuh.

   Dalam usaha pembagian kedua, ternyata tersisa 6 butir berlian, dank arena dirasa masih belum adil, terjadi perkelaihan dan 2 perompak terbunuh.

   Dalam usaha pembagian ketiga, ternyata tersisa 3 butir berlian, dan perkelaihan kembali terjadi dengan 2 orang terbunuh.

   Dalam usaha pembagian keempat, ternyata tidak ada butir berlian yang tersisa, semua perompak yang masih hidup menerima bagian yang banyaknya sama.

   Berapa banyaknya butir berlian minimal dalam kantung ?

3. Skor 20

   Selesaikan sistem kongruensi linier simultan $5x \equiv 1 \pmod 6$, $3x \equiv 10 \pmod{11}$, $2x \equiv 7 \pmod{13}$, $3x \equiv 4 \pmod 5$, $4x \equiv 3 \pmod 7$

4. Skor 10

   Selesaikan sistem kongruensi linier simultan $9x \equiv 4 \pmod{14}$, $5x \equiv 17 \pmod{21}$ dan $7x \equiv 10 \pmod{30}$

5. Skor 20

   Carilah suatu bilangan kelipatan 13 yang bersisa 2 jika dibagi 3,5,7, dan 8, serta bersisa 10 jika dibagi 17.

6. Skor 10

   Selesaikan $26733x \equiv 133 \pmod{54340}$

Cocokkanlah jawaban Anda dengan Rambu-Rambu atau Kunci Jawaban Tes Formatif 1 yang terdpat di bagian akhir modul ini. Kemudian perkirakan skor jawaban Anda yang menurut Anda benar, dan gunakan kriteria berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\textbf{Tingkat Penguasaan} = \frac{\textbf{Skor Jawaban Yang Benar}}{\textbf{100}} \times \textbf{100 \%}$$

Tingkat Penguasaan Anda dikelompokkan menjadi :

Baik sekali	:	90 % - 100 %
Baik	:	80 % - 89 %
Cukup	:	70 % - 79 %
Kurang	:	< 70 %

Apabila Anda mencapai tingkat penguasaan 80 % atau lebih, maka Anda dapat meneruskan ke Kegiatan Belajar 2, Bagus !

Jika tingkat penguasaan Anda kurang dari 80 %, maka seharusnya Anda mengulangi materi Kegiatan Belajar 1, terutama pada bagian-bagian yang belum Anda pahami dan kuasai dengan baik. Selamat Belajar !

MODUL 4

KEGIATAN BELAJAR 2

SISTEM KONGRUENSI LINIER

Uraian

Pada pembahasan tentang aljabar (biasa), salah satu topik adalah sistem persamaan linier. Dua persamaan linier dua variabel, tiga persamaan linier tiga variabel, atau n persamaan linier n variabel membentuk sistem persamaan linier.

Penyelesaian sistem persamaan linier dapat dilakukan dengan cara eliminasi, cara substitusi, cara matriks, atau cara determinan. Masing-masing cara mempunyai langkah-langkah dan aturanp-aturan tertentu dalam memperoleh selesaian.

Serupa dengan pembahasan di aljabar, salah satu topik di teori bilangan adalah sistem kongruensi linier. Sistem kongruensi linier n variabel adalah gabungan dari n kongruensi linier bermodulo sama yang masing-masing-masing memuat paling banyak n variabel.

Penyelesaian system kongruensi linier dapat dilakukan dengan substitusi, eliminasi, atau dengan menggunakan matriks dan determinan.

Marilah kita mulai pembahasan tentang sistem kongruensi linier ini dengan sebuah peragaan, yaitu kita akan mencari semua bilangan bulat x dan y sehingga :

$2x + 3y \equiv 7 \pmod{11}$

$3x + 5y \equiv 6 \pmod{11}$

Jika kita menggunakan cara **substitusi**, maka $2x + 3y \equiv 7 \pmod{11}$ diubah menjadi kongruensi $2x \equiv 7 - 3y \pmod{11}$ atau $3y \equiv 2x \pmod{11}$, kemudian disubstitusikan ke kongruensi $3x + 5y \equiv 6 \pmod{11}$. Misalkan kita memilih $2x \equiv 7 - 3y \pmod{11}$, maka kita kalikan kedua ruas kongruensi dengan 6, sehingga diperoleh :

$12x \equiv 42 - 18y \pmod{11}$, atau $x \equiv 9 - 7y \pmod{11}$.

Substitusi $x \equiv 9 - 7y \pmod{11}$ ke dalam $3x + 5y \equiv 6 \pmod{11}$ diperoleh :

$3(9 - 7y) + 5y \equiv 6 \pmod{11}$, atau $-16\, y \equiv -21 \pmod{11}$, atau $6y \equiv 1 \pmod{11}$,

atau $y \equiv 2 \pmod{11}$

Dengan demikian $x \equiv 9 - 7.2 \pmod{11} \equiv -5 \pmod{11} \equiv 6 \pmod{11}$

Jadi sistem kongruensi linier mempunyai selesaian $x \equiv 6 \pmod{11}$ dan $y \equiv 2 \pmod{11}$

Selesaian x dan y yang diperoleh dapat diperiksa kebenarannya dengan mensubstitusi kannya ke dalam masing-masing kongruensi linier.

Jika kita menggunakan cara eliminasi, maka kita perlu menetapkan lebih dahulu yang dieliminasi, yaitu x atau y. Misalkan kita tetapkan y dieliminasi, maka kongruensi pertama dikalikan 5 dan kongruensi kedua dikalikan 3, sehingga diperoleh :

$10x + 15y \equiv 35 \pmod{11}$

$9x + 15y \equiv 18 \pmod{11}$

Jika kongruensi pertama dikurangi kongruensi kedua, maka diperoleh :

$x \equiv 18 \pmod{11}$, atau $x \equiv 6 \pmod{11}$

Dengan jalan yang sama, jika x yang dieliminasi, maka kongruensi pertama dikalikan 3 dan kongruensi kedua dikalikan 2, sehingga diperoleh :

$6x + 9y \equiv 21 \pmod{11}$

$6x + 10y \equiv 12 \pmod{11}$

Jika kongruensi kedua dikurangi kongruensi pertama, maka diperoleh :

$y \equiv -9 \pmod{11}$, maka $y \equiv 2 \pmod{11}$

Dengan cara substitusi ini kita dapat menyelesaikan sebarang system kongruensi linier dua variabel.

Teorema 4.6

Ditentukan $a,b,c,d,e,f,m \in Z$, $m > 0$, dan $\Delta = ad - bc$ sehingga $(\Delta, m) = 1$

Sistem kongruensi linier :

$ax + by \equiv e \pmod{m}$

$cx + dy \equiv f \pmod{m}$

mempunyai suatu selesaian tunggal yaitu :

$x \equiv \bar{\Delta}(de - bf) \pmod{m}$

$y \equiv \bar{\Delta}(af - ce) \pmod{m}$

dimana $\bar{\Delta}$ adalah inverse dari Δ modulo m .

Bukti :

Jika y akan dieliminasi, maka kongruensi pertama dikalikan d dan kongruensi kedua dikalikan b , sehingga diperoleh :

$adx + bdy \equiv de \pmod{m}$

$bcx + bdy \equiv bf \pmod{m}$

Jika kongruensi pertama dikurangi kongruensi kedua, maka diperoleh :

$(ad - bc)x \equiv (de - bf) \pmod{m}$ atau $\Delta x \equiv (de - bf) \pmod{m}$ sehingga

$\bar{\Delta}\,\Delta x \equiv \bar{\Delta}$ (de – bf) (mod m)

Karena $\bar{\Delta}\,\Delta \equiv 1$ (mod m), maka diperoleh $x \equiv \bar{\Delta}$ (de – bf) (mod m)

Selanjutnya, jika x akan dieliminasi, maka kongruensi pertama dikalikan c dan kongruensi kedua dikalikan a , sehingga diperoleh :

$acx + bcy \equiv ce \pmod{m}$

$acx + ady \equiv af \pmod{m}$

Jika kongruensi kedua dikurangi kongruensi pertama, maka diperoleh :

$(ad – bc)y \equiv (af – ce) \pmod{m}$ atau $\Delta y \equiv (af – ce) \pmod{m}$ sehingga

$\bar{\Delta}\,\Delta y \equiv \bar{\Delta}$ (af – ce) (mod m)

Karena $\bar{\Delta}\,\Delta \equiv 1$ (mod m), maka diperoleh $y \equiv \bar{\Delta}$ (af – ce) (mod m)

Contoh 4.14

Selesaikan system kongruensi linier :

$4x – 7y \equiv 6 \pmod{17}$

$5x + 2y \equiv 9 \pmod{17}$

Jawab :

$\Delta = 4.2 – (-7)(5) = 43 \equiv 9 \pmod{17}$ dan $\bar{\Delta} = 2$, sebab $\bar{\Delta}\,\Delta = 18 \equiv 1 \pmod{17}$

Dengan demikian $x \equiv \bar{\Delta}(de – bf) \pmod{m} \equiv 2\,(2.6 + 7.9) \pmod{17} \equiv 14 \pmod{17}$

dan $y \equiv \bar{\Delta}(af – ce) \pmod{m} \equiv 2\,(4.9 – 5.6) \pmod{17} \equiv 12 \pmod{17}$

Pemeriksaan : jika x = 14 dan y = 12 disubstitusikan pada masing-masing kongruensi diperoleh $4x – 7y = 56 – 84 = –28 \equiv 6 \pmod{17}$ dan $5x + 2y = 5.14 + 2.12 = 70 + 24 = 94 \equiv 9 \pmod{17}$

Untuk menyelesaikan sistem kongruensi linier 3 variabel atau lebih dengan cara eliminasi memerlukan langkah-langkah yang lebih panjang karena tahapan memperoleh x melalui eliminasi variabel-variabel yang lain.

Cara menyelesaikan sistem kongruensi linier n variabel yang relative mudah adalah dengan menggunakan aljabar linier, yaitu persamaan matriks.

Definisi 4.3

Ditentukan A dan B adalah matriks-matriks berukuran p x q dengan unsur-unsur bulat, a_{ij} merupakan unsur A pada baris ke i kolom ke j , dan b_{ij} merupakan unsur B pada baris ke i kolom ke j.

A disebut kongruen dengan B modulo m jika $a_{ij} \equiv b_{ij}$ (mod m) untuk semua pasangan (i,j) dengan $1 \leq i \leq n$ dan $1 \leq j \leq n$, ditulis $A \equiv B$ (mod m)

Contoh 4.15

(a) $\begin{bmatrix} 34 & 46 \\ 23 & 29 \end{bmatrix} \equiv \begin{bmatrix} 8 & 7 \\ 10 & 3 \end{bmatrix}$ (mod 13)

(b) $\begin{bmatrix} -20 & 5 & 39 \\ 15 & 7 & 58 \\ -62 & 12 & 41 \end{bmatrix} \equiv \begin{bmatrix} 1 & 5 & 4 \\ 1 & 0 & 2 \\ 1 & 5 & 6 \end{bmatrix}$ (mod 7)

Teorema 4.7

Jika A dan B adalah matriks-matriks berukuran p x q , $A \equiv B$ (mod m) , dan C adalah suatu matriks berukuran q x r , D adalah suatu matriks berukuran r x p , semuanya dengan unsur-unsur bulat, maka $AC \equiv BC$ (mod m) dan $DA \equiv DB$ (mod m)

Bukti :

Misalkan unsur-unsur A adalah a_{ij} , unsur-unsur B adalah b_{ij} dengan $1 \leq i \leq p$ dan $1 \leq j \leq q$, dan unsur-unsur C adalah c_{ij} dengan $1 \leq j \leq q$ dan $1 \leq j \leq r$.

Unsur AC dan BC pada baris ke i kolom ke j berturut-turut adalah :

$$\sum_{k=1}^{q} a_{ik}c_{kj} \text{ dan } \sum_{k=1}^{q} b_{ik}c_{kj} \,,\ 1 \leq i \leq p \text{ dan } 1 \leq j \leq r$$

Diketahui bahwa $A \equiv B$ (mod m) , maka sesuai definisi 4.3 , $a_{ik} \equiv b_{ik}$ (mod m) untuk semua i dan k, yaitu :

$$\sum_{k=1}^{q} a_{ik}c_{kj} = \sum_{k=1}^{q} b_{ik}c_{kj} \,,\ 1 \leq i \leq p \text{ dan } 1 \leq j \leq r$$

Akibatnya, $AC \equiv BC$ (mod m).

Dengan jalan yang sama, buktikan $DA \equiv DB$ (mod m).

Contoh 4.16

Diketahui : A dan B keduanya berukuran 3 x 2 , A = $\begin{bmatrix} 9 & 12 \\ 13 & 10 \\ 20 & 7 \end{bmatrix}$ dan B = $\begin{bmatrix} 1 & 4 \\ 5 & 2 \\ 4 & 7 \end{bmatrix}$

C berukuran 2 x 4, D berukuran 2 x 3 , C = $\begin{bmatrix} 2 & 4 & 6 & 1 \\ 5 & 3 & 2 & 7 \end{bmatrix}$ dan D = $\begin{bmatrix} 7 & 1 & 4 \\ 4 & 1 & 0 \end{bmatrix}$

$$AC = \begin{bmatrix} 9 & 12 \\ 13 & 10 \\ 20 & 7 \end{bmatrix} \begin{bmatrix} 2 & 4 & 6 & 1 \\ 5 & 3 & 2 & 7 \end{bmatrix} = \begin{bmatrix} 78 & 72 & 78 & 93 \\ 76 & 82 & 98 & 83 \\ 75 & 101 & 134 & 69 \end{bmatrix} \equiv \begin{bmatrix} 6 & 0 & 6 & 5 \\ 4 & 2 & 2 & 3 \\ 3 & 5 & 6 & 5 \end{bmatrix} \pmod 8$$

$$BC = \begin{bmatrix} 1 & 4 \\ 5 & 2 \\ 4 & 7 \end{bmatrix} \begin{bmatrix} 2 & 4 & 6 & 1 \\ 5 & 3 & 2 & 7 \end{bmatrix} = \begin{bmatrix} 22 & 16 & 14 & 29 \\ 20 & 26 & 34 & 19 \\ 43 & 37 & 38 & 53 \end{bmatrix} \equiv \begin{bmatrix} 6 & 0 & 6 & 5 \\ 4 & 2 & 2 & 3 \\ 3 & 5 & 6 & 5 \end{bmatrix} \pmod 8$$

$$DA = \begin{bmatrix} 7 & 1 & 4 \\ 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} 9 & 12 \\ 13 & 10 \\ 20 & 7 \end{bmatrix} = \begin{bmatrix} 28 & 58 \\ 9 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix} \pmod 8$$

$$DB = \begin{bmatrix} 7 & 1 & 4 \\ 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 5 & 2 \\ 4 & 7 \end{bmatrix} = \begin{bmatrix} 28 & 58 \\ 9 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \pmod 8$$

Perhatikan bahwa AC ≡ BC (mod 8) dan DA ≡ DB (mod 8)

Marilah sekarang kita lihat cara memperoleh selesaian sistem kongruensi linier dengan menggunakan persamaan matriks, suatu cara yang serupa dengan cara memperoleh selesaian sistem persamaan linier di dalam aljabar (linier).

Secara umum, suatu sistem kongruensi linier dapat dinyatakan sebagai :

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1 \pmod m \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2 \pmod m \\ \quad . \qquad . \qquad \ldots \qquad . \qquad . \\ \quad . \qquad . \qquad \ldots \qquad . \qquad . \\ \quad . \qquad . \qquad \ldots \qquad . \qquad . \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \equiv b_n \pmod m \end{array}$$

Dalam bentuk persamaan matriks, sistem kongruensi linier ini dapat ditulis dengan :

AX ≡ B (mod m)

dimana :

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdot & \cdot & \cdot & a_{1n} \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ a_{n1} & a_{n2} & \cdot & \cdot & \cdot & a_{nn} \end{bmatrix} \quad \mathbf{,} \quad \mathbf{X} = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} \quad \mathbf{, \ dan} \quad \mathbf{B} = \begin{bmatrix} b \\ b_2 \\ \cdot \\ \cdot \\ \cdot \\ b_n \end{bmatrix}$$

Contoh 4.17

Suatu sistem kongruensi linier :

$2x + 3y + 4z \equiv 2 \pmod{11}$

$3x + y + 2z \equiv 7 \pmod{11}$

$4x + 2y + z \equiv 3 \pmod{11}$

dapat dinyatakan sebagai :

$$\begin{bmatrix} 2 & 3 & 4 \\ 3 & 1 & 2 \\ 4 & 2 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 7 \\ 3 \end{bmatrix} \pmod{11}$$

Selesaian sistem kongruensi linier :

A X ≡ B (mod m)

diperoleh dari :

$\mathbf{A^{-1}}$ A X ≡ $\mathbf{A^{-1}}$ B (mod m) , $\mathbf{A^{-1}}$ adalah inverse A modulo m

I X ≡ $\mathbf{A^{-1}}$ B (mod m) , I adalah matriks identitas

X ≡ $\mathbf{A^{-1}}$B (mod m)

dengan $\mathbf{A^{-1}}$ didefinisikan sebagai berikut :

Definisi 4.4

Jika A dan A^{-1} adalah matriks-matriks dengan unsur-unsur bilangan bulat, dan berukuran n x n , serta $A^{-1}A \equiv A\,A^{-1} \equiv 1 \pmod{m}$, dengan :

$$I = \begin{bmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 1 & . & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \end{bmatrix}$$ adalah matriks identitas berderajad n ,

maka A^{-1} disebut inverse matriks A modulo m .

Teorema 4.8

Diketahui suatu matriks :

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

dengan unsur-unsur bilangan bulat, Δ = det A = ad – bc , dan (Δ,m) = 1.

Maka inversi matriks A modulo m adalah :

$$A^{-1} = \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

dengan Δ^{-1} adalah inversi Δ modulo m

Bukti :

Untuk membuktikan A^{-1} adalah inversi A modulo m, kita harus membuktikan bahwa $AA^{-1} \equiv A^{-1}A \pmod{m}$

$$AA^{-1} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \equiv \Delta^{-1} \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix}$$

$$\equiv \Delta^{-1} \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \Delta^{-1}\Delta & 0 \\ 0 & \Delta^{-1}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv 1 \pmod{m}$$

Dengan jalan yang sama, buktikan bahwa $A^{-1}A \equiv I \pmod{m}$

Contoh 4.18

Diketahui $A = \begin{bmatrix} 5 & 3 \\ 7 & 8 \end{bmatrix}$, dengan demikian Δ = 5.8 – 7.3 = 19

Inversi dari $\Delta = 19$ modulo 11 adalah $\Delta^{-1} = 7$ sebab $\Delta\,\Delta^{-1} = 19.7 = 133 \equiv 1 \pmod{11}$

Jadi inversi A adalah $A^{-1} = 7\begin{bmatrix} 8 & -3 \\ -7 & 5 \end{bmatrix} = \begin{bmatrix} 56 & -21 \\ -49 & 35 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 6 & 2 \end{bmatrix}$ (mod 11)

Selanjutnya, seperti uraian yang telah kita pelajari dalam aljabar linier, terutama pada topic matriks dan determinan, kita mengenal dan memahami tentang matriks adjoit dan dan rumusan mencari inversi matriks dengan menggunakan matriks adjoit dan determinan. Secara rinci Anda dipersilahkan membaca ulang materi-materi itu, termasuk di antaranya minor dan kofaktor.

Definisi 4.5

Ditentukan A adalah suatu matriks berukuran n x n

Adjoit dari matriks A, ditulis **adj A**, adalah suatu matriks berukuran n x n yang unsur-unsurnya adalah α_{ji} dimana α_{ij} sama dengan $(-1)^{i+j}$ dikalikan determinan suatu matriks yang diperoleh dengan menghapus semua unsur A pada baris ke i dan kolom ke j

Teorema 4.9

Jika A adalah suatu matriks berukuran n x n dan A bukan matriks nol , maka

A (adj A) = Δ I

Buktikan (lihat di buku-buku aljabar linier)

Teorema 4.10

Jika A adalah suatu matriks berukuran n x n dan semua unsur-unsurnya adalah bilangan bulat, serta m adalah bilangan bulat positif sehingga $(\Delta, m) = 1$, maka inversi dari A adalah :

$A^{-1} = \Delta^{-1}$ (adj A)

Bukti :

Karena $(\Delta, m) = 1$, maka $\Delta \neq 0$, dan sesuai teorema 4.9 , A (adj A) = Δ I

Selanjutnya, dari $(\Delta, m) = 1$ dapat ditentukan bahwa Δ mempunyai inverse Δ^{-1} modulo m, sehingga :

$A(\Delta^{-1})(\text{adj } A) \equiv A(\text{adj } A)\,\Delta^{-1} = (\Delta I)\,\Delta^{-1} \equiv \Delta\,\Delta^{-1} I \equiv I \pmod{m}$, dan

$\Delta^{-1}(\text{adj } A)\,A \equiv \Delta^{-1}(\text{adj } A \,.\, A) \equiv \Delta^{-1}\,\Delta\, I \equiv I \pmod{m}$

Jadi Δ^{-1} (adj A) adalah inversi A, atau $A^{-1} = \Delta^{-1}$ (adj A)

Contoh 4.19

Diketahui A = $\begin{bmatrix} 2 & 2 & -2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}$, maka $\Delta = 4$, dan $\Delta^{-1} \equiv 3$ (mod 11)

$$A^{-1} = \Delta^{-1}(\text{adj } A) = 3\begin{bmatrix} -1 & -14 & 10 \\ 2 & 12 & -8 \\ -1 & -2 & 2 \end{bmatrix} = \begin{bmatrix} -3 & -42 & 30 \\ 6 & 36 & -24 \\ -3 & -6 & 6 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 8 & 2 & 8 \\ 6 & 3 & 9 \\ 8 & 5 & 6 \end{bmatrix} \text{ (mod 11)}$$

Pemeriksaan :

$$AA^{-1} = \begin{bmatrix} 2 & 2 & -2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}\begin{bmatrix} 8 & 2 & 8 \\ 6 & 3 & 9 \\ 8 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 12 & 0 & 22 \\ 44 & 23 & 44 \\ 66 & 33 & 67 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ (mod 11)}$$

Sekarang kita dapat menggunakan inverse A modulo m untuk menyelesaikan suatu kongruensi linier :

$A X \equiv B$ (mod m)

dimana $(\Delta, m) = 1$.

Berdasarkan teorema 4.10, karena $(\Delta, m) = 1$, maka A mempunyai invers, misalnya A^{-1} sehingga jika kedua ruas $A X \equiv B$ (mod m) dikalikan A^{-1} diperoleh :

$A^{-1}(A X) = A^{-1} B$ (mod m)

$(A^{-1} A) X = A^{-1} B$ (mod m)

$I X = A^{-1} B$ (mod m)

$X = A^{-1} B$ (mod m)

Dengan demikian selesaian kongruensi linier simultan adalah $X = A^{-1} B$ (mod m)

Contoh 4.20

Selesaikan system kongruensi linier :

$x + 2y + z \equiv 4$ (mod 7), $x - y + z \equiv 5$ (mod 7), $2x + 3y + z \equiv 1$ (mod 7)

Jawab : $\begin{bmatrix} 1 & 2 & 1 \\ 1 & -1 & 1 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix}$

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 1 & -1 & 1 \\ 2 & 3 & 1 \end{bmatrix}, \; X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \text{ dan } B = \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix}$$

$\Delta = 3$, dan $(\Delta,7) = (3,7) = 1$, maka $\Delta^{-1} \equiv 5 \pmod 7$

$$A^{-1} = \Delta^{-1} (\text{adj } A) = 5 \begin{bmatrix} -4 & 1 & 3 \\ 1 & -1 & 0 \\ 5 & 1 & -3 \end{bmatrix} = \begin{bmatrix} -20 & 5 & 15 \\ 5 & -5 & 0 \\ 25 & 5 & -15 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 5 & 1 \\ 5 & 2 & 0 \\ 4 & 5 & 6 \end{bmatrix}$$

$$X = A^{-1} B = \begin{bmatrix} 1 & 5 & 1 \\ 5 & 2 & 0 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 30 \\ 30 \\ 47 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 2 \\ 5 \end{bmatrix}$$

Tugas Dan Latihan

Tugas

Bacalah suatu buku tentang teori bilangan, misalnya Elementary Number Theory and Its Applications yang ditulis oleh Kenneth H. Rosen, dan diterbitkan oleh Addison-Wesley Publishing Company, carilah topik tentang Metode Monte Carlo.

Jelaskan topik itu terkait dengan masalah teori bilangan yang mana, bagaimana langkah-langkahnya, dan berilah paling sedikit satu contoh.

Latihan

1. Selesaikan sistem kongruensi linier:

   (a) $x + 2y \equiv 1 \pmod 5$
   $\quad 2x + y \equiv 1 \pmod 5$

   (b) $x + 3y \equiv 1 \pmod 5$
   $\quad 3x + 4y \equiv 1 \pmod 5$

2. Carilah inversi matriks A modulo 7 jika :

   $$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

3. Selesaikan sistem kongruensi linier :

$x + y \equiv 1 \pmod 7$

$x + z \equiv 2 \pmod 7$

$y + z \equiv 3 \pmod 7$

4. Selesaikan sistem kongruensi linier :

$2x + 5y + 6z \equiv 3 \pmod 7$

$2y + z \equiv 4 \pmod 7$

$x + 2y + 3z \equiv 3 \pmod 7$

5. Carilah matriks T jika :

$$T \equiv \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 4 & 0 \\ 2 & 1 \end{bmatrix} \pmod 5$$

dan semua unsur T adalah bilangan-bilangan bulat tidak negative kurang dari 5

Rambu-Rambu Jawaban Tugas dan Latihan

Rambu-Rambu Jawaban Tugas

Metode Monte Carlo adalah suatu metode pemfaktoran yang didasarkan pada kongruensi dan dikembangkan oleh J.M. Pollard pada tahun 1974 (Rosen, 1993:156).

Ditentukan n adalah bilangan komposit yang relative cukup besar dan p adalah faktor prima n yang terkecil. Keinginan kita adalah memilih bilangan-bilangan bulat :

$x_0 , x_1 , \dots , x_s$

sedemikian hingga mempunyai residu-residu non-negatif terkecil modulo n yang berbeda, tetapi tidak untuk kejadian yang sama modulo p.

Misalkan kita sudah temukan x_i dan x_j , $0 \le i < j \le s$ sehingga $x_i \equiv x_j \pmod p$ tetapi x_i tidak kongruen dengan x_j modulo n , maka $p \mid x_i - x_j$ tetapi n tidak membagi $x_i - x_j$ sehingga $(x_i - x_j , n)$ adalah faktor non-trivial dari n, dan dapat dicari dengan mudah menggunakan algoritma Euclides.

Untuk mencari bilangan-bilangan bulat x_i dan x_j digunakan langkah-langkah :

(a) mulailah dengan suatu nilai awal (bibit) x_0 yang dipilih secara random

(b) ambil suatu polynomial f(x) dengan koefien-koefisien bulat dan berderajad lebih dari 1.

(c) Hitunglah suku-suku x_k , k = 1,2,3, … dengan menggunakan definisi rekursif :

$$x_{k+1} \equiv f(x_k) \pmod n , 0 \le x_{k+1} , n$$

(d) Polinomial f(x) seharusnya mempunyai sifat bahwa barisan $x_0 , x_1 , \dots , x_s$ mempunyai tingkah laku seperti barisan random yang diinginkan.

Sebagai peragaan, ambil n = 8051.

(a) ambil suatu nilai awal $x_0 = 2$

(b) ambil suatu polynomial $f(x) = x^2 + 1$

(c) Hitung x_k secara ekursif

$x_0 = 2$

$x_1 = f(x_0) = f(2) = 2^2 + 1 = 5$

$x_2 = f(x_1) = f(5) = 5^2 + 1 = 26$

$x_3 = f(x_2) = f(26) = 26^2 + 1 = 677$

$x_4 = f(x_3) = f(677) = 677^2 + 1 \equiv 7474 \pmod{8051}$

$x_5 = f(x_4) = f(7474) = 7474^2 + 1 \equiv 2839 \pmod{8051}$

$x_6 = f(x_5) = f(2839) = 2839^2 + 1 \equiv 871 \pmod{8051}$

dan seterusnya.

Berikutnya, berdasarkan definisi rekursif x_k , jika d adalah suatu bilangan bulat positif, dan $x_i \equiv x_j \pmod{d}$, maka :

$x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1} \pmod{d}$

Hal ini berarti barisan x_k besifat periodik dengan periode $(j – i)$, $x_q \equiv x_r \pmod{j – i}$ dengan $q \geq i$ dan $r \geq j$, dan akibatnya, jika s adalah bilangan bulat positif kelipatan $j – i$, maka $x_s \equiv x_{2s} \pmod{d}$.

Untuk memperoleh suatu faktor dari n , kita cari fpb dari $x_{2k} – x_k$ dan n , k = 1,2,3,… yaitu setelah kita memperoleh k yang mana $1 < x_{2k} – x_k < n$.

Secara praktis, apabila metode rho Pollard digunakan, polynomial yang sering dipilih adalah $f(x) = x^2 + 1$, dan nilai awal yang dipilih adalah $x_0 = 2$.

Contoh :

Dengan menggunakan metode rho Pollard (atau metode Monte Carlo), dengan $x_0 = 2$ dan polynomial pembangkit $f(x) = x^2 + 1$ untuk memperoleh factor non-trivial dari suatu bilangan komposit n = 8051.

Jawab :

Dari hasil hitungan x_0 , x_1 , x_2 , x_3 , x_4 , x_5 , dan x_6 di atas, dan berdasarkan hitungan algoritma Euclides, dapat ditentukan bahwa :

$(x_2 – x_1,8051) = (21,8051) = 1$

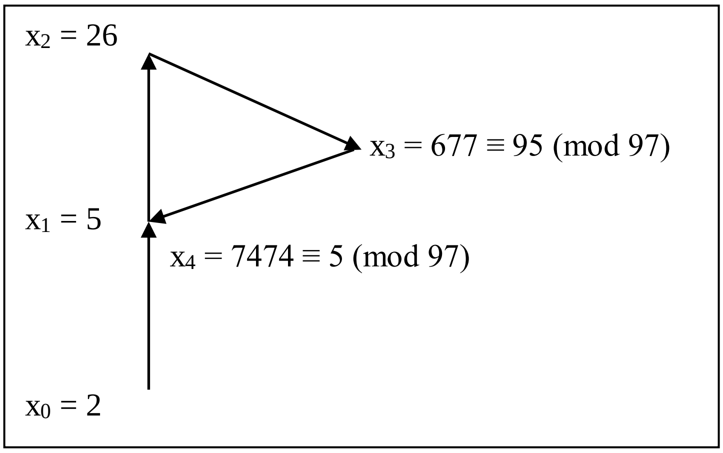
$(x_4 – x_2,8051) = (7448,8051) = 1$

$(x_6 – x_3,8051) = (194,8051) = 97$

Jadi 97 adalah suatu faktor dari 8051.

Tingkah laku dari periodik dari barisan x_i dengan $x_0 = 2$ dan $x_{i+1} = x_i^2 + 1 \pmod{97}$

dan $i \geq 1$, dapat terlihat seperti model berikut :



Rambu-Rambu Jawaban Latihan

1. (a) Ada tiga pilihan cara menyelesaikan : substitusi, eliminasi, atau matriks.

Misalkan digunakan cara substitusi.

$x + 2y \equiv 1 \pmod 5$, atau $x \equiv 1 - 2y \pmod 5$, substitusikan ke $2x + y \equiv 1 \pmod 5$ diperoleh $2(1 - 2y) + y \equiv 1 \pmod 5$, atau $-3y \equiv -1 \pmod 5$, $2y \equiv 4 \pmod 5$, sehingga $y \equiv 2 \pmod 5$.

$x \equiv 1 - 2.2 \pmod 5 \equiv -3 \pmod 5$, sehingga $x \equiv 2 \pmod 5$

(b) Misalkan digunakan cara eliminasi

x akan dieliminasi, maka kongruensi pertama dikalikan dengan 3, dan kongruensi kedua tetap :

$$3x + 9y \equiv 3 \pmod 5$$
$$3x + 4y \equiv 2 \pmod 5$$

Jika kongruensi pertama dikurangi kongruensi kedua diperoleh :

$$5y \equiv 1 \pmod 5$$

Kongruensi tidak mempunyai selesaian sebab $(5,5) = 5$ tidak membagi 1

2. $\Delta = -2 \equiv 5 \pmod 7$, maka $\Delta^{-1} \equiv 3 \pmod 7$

$$A^{-1} = \Delta^{-1}(\text{adj } A) = 3\begin{bmatrix} -1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} -3 & -3 & 3 \\ -3 & 3 & -3 \\ 3 & -3 & -3 \end{bmatrix} \equiv \begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \end{bmatrix}$$

3. Gunakan persamaan matriks untuk menyelesaikan

$$\begin{bmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}1\\ 2\\ 3\end{bmatrix} \text{(mod 7)}\ \ \text{atau}\ \ A\,X \equiv B \text{ (mod 7)}$$

$$X \equiv A^{-1}B \text{ (mod 7)} \equiv \begin{bmatrix}4 & 4 & 3\\ 4 & 3 & 4\\ 3 & 4 & 4\end{bmatrix}\begin{bmatrix}1\\ 2\\ 3\end{bmatrix} \text{(mod 7)} \equiv \begin{bmatrix}21\\ 22\\ 23\end{bmatrix} \text{(mod 7)} \equiv \begin{bmatrix}0\\ 1\\ 2\end{bmatrix}$$

4. $$\begin{bmatrix}2 & 5 & 6\\ 2 & 0 & 1\\ 1 & 2 & 3\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}3\\ 4\\ 1\end{bmatrix} \text{(mod 7) atau } A\,X \equiv B \text{ (mod 7)}$$

$$X \equiv A^{-1}B \text{ (mod 7)} \equiv \begin{bmatrix}6 & 2 & 6\\ 1 & 0 & 5\\ 2 & 4 & 2\end{bmatrix}\begin{bmatrix}3\\ 4\\ 1\end{bmatrix} \text{(mod 7)} \equiv \begin{bmatrix}32\\ 8\\ 24\end{bmatrix} \equiv \begin{bmatrix}4\\ 1\\ 3\end{bmatrix}$$

5. $$T \equiv \begin{bmatrix}2 & 1\\ 4 & 3\end{bmatrix}\begin{bmatrix}4 & 0\\ 2 & 1\end{bmatrix} \text{ (mod 5)} \equiv \begin{bmatrix}10 & 1\\ 22 & 3\end{bmatrix} \text{(mod 5)} \equiv \begin{bmatrix}0 & 1\\ 2 & 3\end{bmatrix} \text{(mod 5)}$$

Rangkuman

Berdasarkan seluruh paparan pada Kegiatan Belajar 2 ini, maka garis besar bahan yang dibahas meliputi Definisi, Teorema, dan penerapan dalam penyelesaian masalah terkait, terutama tentang konsep sistem kongruensi linier , cara menyelesaikan system kongruensi linier yang terdiri dari substitusi, eliminasi, dan matriks, dan metode rho Pollard atau metode Monte Carlo untuk mencari factor prima suatu bilangan komposit dengan menggunakan kongruensi.

1. **Definisi 4.3** tentang dua matriks A dan B yang kongruen modulo m
2. **Definisi 4.4** tentang inversi suatu matriks A modulo m.
3. **Definisi 4.5** tentang adjoint suatu matriks A modulo m
4. **Teorema 4.6** tentang ketunggalan selesaian sistem kongruensi linier :

$$ax + by \equiv e \text{ (mod m)}$$
$$cx + dy \equiv f \text{ (mod m)}$$

jika $(\Delta, m) = 1$ dengan $\Delta = ad - bc$

5. Teorema 4.7

Jika A dan B adalah matriks-matriks berukuran p x q , A ≡ B (mod m) , dan C adalah suatu matriks berukuran q x r , D adalah suatu matriks berukuran r x p , semuanya dengan unsur-unsur bulat, maka AC ≡ BC (mod m) dan DA ≡ DB (mod m)

6. Teorema 4.8

Inversi matriks A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ adalah $A^{-1} = \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

7. Teorema 4.9

Jika A adalah suatu matriks berukuran n x n dan A bukan matriks nol , maka

$$A\,(\text{adj } A) = \Delta I$$

8. Teorema 4.10

Jika A adalah suatu matriks berukuran n x n dan semua unsur-unsurnya adalah bilangan bulat, serta m adalah bilangan bulat positif sehingga (Δ ,m) = 1, maka inversi dari A adalah :

$$A^{-1} = \Delta^{-1}\,(\text{adj } A)$$

Tes Formatif 2

1. Skor 10

Selesaikan system kongruensi linier :

(a) 4x + y ≡ 2 (mod 5)

2x + 3y ≡ 1 (mod 5)

(b) 2x + 3y ≡ 5 (mod 5)

x + 5y ≡ 6 (mod 5)

2. Skor 20

Carilah inversi dari A modulo 7 jika :

A = $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{bmatrix}$

3. Skor 20

Selesaikan sistem kongruensi linier :

x + y + z ≡ 1 (mod 7)

x + y + w ≡ 1 (mod 7)

x + z + w ≡ 1 (mod 7)

y + z + w ≡ 1 (mod 7)

4. Skor 10

   Carilah banyaknya selesaian tidak kongruen dari sistem kongruensi linier :

   $$\begin{aligned} 2x + 3y + z &\equiv 3 \pmod 5 \\ x + 2y + 3z &\equiv 1 \pmod 5 \\ 2x + z &\equiv 1 \pmod 5 \end{aligned}$$

5. Skor 15

   Carilah pemfaktoran prima dari 1927 menggunakan metode rho Pollard dengan $x_0 = 2$ dan $f(x) = x^2 + 1$

6. Skor 15

   Carilah pemfaktoran prima dari 1387 menggunakan metode rho Pollard dengan $x_0 = 3$ dan $f(x) = x^2 + 1$

Cocokkanlah jawaban Anda dengan Rambu-Rambu atau Kunci Jawaban Tes Formatif 2 yang terdpat di bagian akhir modul ini. Kemudian perkirakan skor jawaban Anda yang menurut Anda benar, dan gunakan kriteria berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\textbf{Tingkat Penguasaan} = \frac{\textbf{Skor Jawaban Yang Benar}}{\textbf{100}} \times \textbf{100 \%}$$

Tingkat Penguasaan Anda dikelompokkan menjadi :

Baik sekali	:	90 % - 100 %
Baik	:	80 % - 89 %
Cukup	:	70 % - 79 %
Kurang	:	< 70 %

Apabila Anda mencapai tingkat penguasaan 80 % atau lebih, maka Anda dapat meneruskan ke Modul 5. Bagus !

Jika tingkat penguasaan Anda kurang dari 80 %, maka seharusnya Anda mengulangi materi Kegiatan Belajar 2, terutama pada bagian-bagian yang belum Anda pahami dan kuasai dengan baik. Selamat Belajar !

Rambu-Rambu Jawaban Tes Formatif

Rambu-Rambu Jawaban Tes Formatif 1

1. (a) $23x \equiv 17 \pmod{180}$

$(23,180) = 1 \mid 17$, maka kongruensi linier mempunyai satu selesaian.

$23x \equiv 17 \pmod{180} \quad \rightarrow \quad x_0 = \dfrac{180.10+17}{23} = 79$

$180y \equiv -17 \pmod{23}$

$19y \equiv -17 \pmod{23} \quad \rightarrow \quad y_0 = \dfrac{23.9-17}{19} = 10$

$23z \equiv 17 \pmod{19}$

$4z \equiv 17 \pmod{19} \quad \rightarrow \quad z_0 = \dfrac{19.1+17}{4} = 9$

$19r \equiv -17 \pmod{4}$

$3r \equiv 3 \pmod{4} \quad \rightarrow \quad r_0 = 1$

Penyelesaian : $x \equiv 79 \pmod{180}$

(b) $180 = 4.5.9$, maka kongruensi linier dapat dinyatakan dalam sistem kongruensi linier simultan :

$23x \equiv 17 \pmod{4}$, atau $x \equiv 3 \pmod{4}$

$23x \equiv 17 \pmod{5}$, atau $x \equiv 4 \pmod{5}$

$23x \equiv 17 \pmod{9}$, atau $x \equiv 7 \pmod{9}$

Dengan demikian dapat dicari b_1 , b_2 , dan b_3 :

$5.9b_1 \equiv 1 \pmod{4}$, maka $b_1 = 1$

$4.9b_2 \equiv 1 \pmod{5}$, maka $b_2 = 1$

$4.5b_3 \equiv 1 \pmod{9}$, maka $b_3 = 5$

$x = 5.9.1.3 + 4.9.1.4 + 4.5.5.7 = 979$

Jadi : $x \equiv 79 \pmod{180}$

2. Permasalahan banyaknya butir berlian dalam kantung dapat dinyatakan dalam suatu bentuk sistem kongruensi linier simultan. Misalkan banyaknya butir berlian dalam kantung adalah x, maka keadaan pertama dapat dinyatakan dengan $x \equiv 5 \pmod{13}$. Setelah terjadi 4 orang terbunuh, maka keadaan kedua dapat dinyatakan dengan $x \equiv 6 \pmod{9}$. Demikian seterusnya sehingga diperoleh lagi dua kongruensi linier

yaitu $x \equiv 3 \pmod 7$ dan $x \equiv 0 \pmod 5$.

$9.7.5b_1 \equiv 1 \pmod{13}$, $b_1 = 9$

$13.7.5b_2 \equiv 1 \pmod 9$, $b_2 = 2$

$13.9.5b_3 \equiv 1 \pmod 7$, $b_3 = 2$

$13.9.7b_4 \equiv 1 \pmod 5$, $b_4 = 4$

$x = 9.7.5.9.5 + 13.7.5.2.6 + 13.9.5.2.3 + 13.9.7.4.0 = 23145 \equiv 2670 \pmod{4095}$

Banyaknya butir berlian minimal dalam kantung adalah 2670

3. Sistem kongruensi linier simultan dapat dinyatakan dengan $x \equiv 5 \pmod 6$, $x \equiv 7 \pmod{11}$, $x \equiv 10 \pmod{13}$, $x \equiv 3 \pmod 5$, dan $x \equiv 6 \pmod 7$, sehingga :

$11.13.5.7b_1 \equiv 1 \pmod 6$, $b_1 = 1$

$6.13.15.7b_2 \equiv 1 \pmod{11}$, $b_2 = 6$

$6.11.5.7b_3 \equiv 1 \pmod{13}$, $b_3 = 3$

$6.11.13.7b_4 \equiv 1 \pmod 5$, $b_4 = 1$

$6.11.13.5b_5 \equiv 1 \pmod 7$, $b_5 = 6$

$x = 11.13.5.7.5.1 + 6.13.15.7.7.6 + 6.11.5.7.10.3 + 6.11.13.7.3.1 + 6.11.13.5.6.6$

$= 25025 + 114660 + 69300 + 18018 + 154440 = 381443 \equiv 21083 \pmod{30030}$

4. Dengan cara biasa dapat dibuat barisan-bilangan yang memenuhi masing-masing kongruensi , kemudian dicari suku atau unsur yang sama.

$9x \equiv 4 \pmod{14}$, maka $x \equiv 2,16,44,58,72,86,100, \ldots,310, \ldots \pmod{14}$

$5x \equiv 17 \pmod{21}$, maka $x \equiv 16,37,58,79,100, \ldots ,310, \ldots \pmod{21}$

$7x \equiv 10 \pmod{20}$, maka $x \equiv 10,30,50,70, \ldots,310, \ldots \pmod{20}$

$x \equiv 310 \pmod{14}$, $x \equiv 310 \pmod{21}$, dan $x \equiv 310 \pmod{30}$, maka :

$x \equiv 310 \pmod{[14,21,30]} \equiv 310 \pmod{420}$

Coba kerjakan dengan cara iterasi, untuk memeriksa apakah hasilnya sama.

5. Misalkan bilangan itu adalah x , maka :

$x \equiv 0 \pmod{13}$, $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 2 \pmod 8$, dan $x \equiv 10 \pmod{17}$

Dari $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 2 \pmod 7$, dan $x \equiv 2 \pmod 8$ dapat ditentukan bahwa $x \equiv 2 \pmod{[3,5,7,8]}$, atau $x \equiv 2 \pmod{840}$.

Dengan demikian terdapat sistem kongruensi linier simultan $x \equiv 0 \pmod{13}$, $x \equiv 2 \pmod{840}$, dan $x \equiv 10 \pmod{17}$

$840.17b_1 \equiv 1 \pmod{13}$, $b_1 = 11$

$13.17b_2 \equiv 1 \pmod{840}$, $b_2 = 821$

$13.840b_3 \equiv 1 \pmod{17}$, $b_3 = 3$

$x = 840.17.0.11 + 13.17.2.821 + 13.840.10.3 = 690482 \equiv 133562 \pmod{185640}$

6. Langkah pertama adalah mencari (26733,54340) dengan menggunakan Algoritma Euclides : 54340 = 2.26733 + 874

   26733 = 30.874 + 513

   874 = 1.513 + 361

   513 = 1.361 + 152

   361 = 2.152 + 57

   152 = 2.57 + 38

   57 = 1.38 + 19

   38 = 2.19 + 0

   (26733,54340) = 19 | 133 , maka kongruensi linier mempunyai 19 selesaian.

$$26733x \equiv 133 \pmod{54340}$$

$$1407x \equiv 7 \pmod{2860} \quad \rightarrow \quad x_0 = \frac{2860.581+7}{1407} = 1181$$

$$2860y \equiv -7 \pmod{1407}$$

$$46y \equiv -7 \pmod{1407} \quad \rightarrow \quad y_0 = \frac{1407.19-7}{46} = 581$$

$$1407z \equiv 7 \pmod{46}$$

$$27z \equiv 7 \pmod{46} \quad \rightarrow \quad z_0 = \frac{46.11+7}{27} = 19$$

$$46r \equiv -7 \pmod{27}$$

$$19r \equiv -7 \pmod{27} \quad \rightarrow \quad r_0 = \frac{27.8-7}{19} = 11$$

$$27s \equiv 7 \pmod{19}$$

$$8\ s \equiv 7 \pmod{19} \quad \rightarrow \quad s_0 = \frac{19.3+7}{8} = 8$$

$$19\ t \equiv -7 \pmod{8}$$

$$3\ t \equiv -7 \pmod{8} \quad \rightarrow \quad t_0 = \frac{8.2-7}{3} = 3$$

$$8k \equiv 7 \pmod{3}$$
$$2k \equiv 1 \pmod{3} \quad \rightarrow \quad k_0 = 2$$

Penyelesaian : x ≡ 1181,4041,6901, … , 52661 (mod 54340)

Rambu-Rambu Jawaban Tes Formatif 2

1. (a) 4x + y ≡ 2 (mod 5) , maka y ≡ 2 – 4x (mod 5)

   2x + 3y ≡ 1 (mod 5) , maka 2x + 3(2 – 4x) ≡ 1 (mod 5), –10x ≡ – 5 (mod 5)

   atau 10x ≡ 5 (mod 5), dengan demikian x ≡ 0,1,2,3,4 (mod 5), sehingga

   y ≡ 2,3,4,0,1 (mod 5)

   (b) 2x + 3y ≡ 5 (mod 5)

   x + 5y ≡ 6 (mod 5)

2. Semua selesaian adalah : (0,4), (1,1), (2,5), (3,2), (4,6), (5,3), dan (6,0)

3. $$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \pmod{7}$$

$$\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} \equiv \begin{bmatrix} 5 & 5 & 5 & 4 \\ 5 & 5 & 4 & 5 \\ 5 & 4 & 5 & 5 \\ 4 & 5 & 5 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \pmod{7} \equiv \begin{bmatrix} 5 \\ 5 \\ 5 \\ 5 \end{bmatrix} \pmod{7}$$

4. Jika kongruensi pertama dikurangi kongruensi ketiga, maka diperoleh :

   3y ≡ 2 (mod 5) , atau y ≡ 4 (mod 5)

   Selanjutnya, jika x = 0,1,2,3,4 , maka diperoleh z = 1,4,2,0,3

   Jadi terdapat lima selesaian tidak kongruen (0,4,1), (1,4,4) , (2,4,2) , (3,4,0) , (4,4,3)

5. $x_0 = 2$

   $x_1 = f(x_0) = f(2) = 2^2 + 1 = 5$

   $x_2 = f(x_1) = f(5) = 5^2 + 1 = 26$

   $x_3 = f(x_2) = f(26) = 26^2 + 1 = 677$

   $x_4 = f(x_3) = f(677) = 677^2 + 1 \equiv 1631 \pmod{1927}$

   $x_5 = f(x_4) = f(1631) = 1631^2 + 1 \equiv 902 \pmod{1927}$

   $x_6 = f(x_5) = f(902) = 902^2 + 1 \equiv 411 \pmod{1927}$

   $x_7 = f(x_6) = f(411) = 411^2 + 1 = 1273 \pmod{1927}$

   Ternyata, $(x_7 - x_0 , 1927) = (1273 - 2 , 1927) = (1271 , 1927) = 41$

   Jadi 1927 = 41.47

6. $x_0 = 3$

$x_1 = f(x_0) = f(3) = 3^2 + 1 = 10$

$x_2 = f(x_1) = f(10) = 10^2 + 1 = 101$

$x_3 = f(x_2) = f(101) = 101^2 + 1 = 493 \pmod{1387}$

$x_4 = f(x_3) = f(493) = 493^2 + 1 \equiv 325 \pmod{1387}$

$x_5 = f(x_4) = f(325) = 325^2 + 1 \equiv 214 \pmod{1387}$

$x_6 = f(x_5) = f(214) = 214^2 + 1 \equiv 26 \pmod{1387}$

$x_7 = f(x_6) = f(26) = 26^2 + 1 = 677 \pmod{1387}$

$x_8 = f(x_7) = f(677) = 677^2 + 1 = 620 \pmod{1387}$

$x_9 = f(x_8) = f(620) = 620^2 + 1 \equiv 202 \pmod{1387}$

$x_{10} = f(x_9) = f(202) = 202^2 + 1 \equiv 582 \pmod{1387}$

$x_{11} = f(x_{10}) = f(582) = 582^2 + 1 \equiv 297 \pmod{1387}$

$x_{12} = f(x_{11}) = f(297) = 297^2 + 1 = 829 \pmod{1387}$

Ternyata, $(x_{12} - x_6 , 1387) = (829 - 26 , 1387) = (803 , 1387) = 73$

Jadi $1387 = 73.19$

Daftar Kepustakaan

Niven, I., Zuckerman, H.S., dan Montgomery, H.L. (1991). **An Introduction to The Theory of Numbers.** New York : John Wiley & Sons.

Redmond, D. (1996). **Number Theory.** New York : Marcel Dekker.

Rosen, K.H. (1993). **Elementary Number Theory And Its Applications.** Massachusetts : Addison-Wesley.