# BAB III

# KONGRUENSI POLINOMIAL BERDERAJAD SATU

## 3.1 PENGANTAR

**Definisi 3.1**

Jika terdapat bilangan bulat m yang tidak kosong, membagi suatu selang a-b, maka a adalah kongruen terhadap b modulo m dan ditulis $a \equiv b \pmod{m}$. Jika a-b tidak dapat dibagi dengan m, maka dikatakan a tidak kongruen terhadap b modulo m dan ditulis $a \not\equiv b \pmod{m}$, a-b dapat dibagi oleh m, jika dapat dibagi oleh -m.

**Teorema 3.1**

Ambil a,b,c,d,x,y sebagai bilangan bulat maka:

(1) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, dan $a-b \equiv 0 \pmod{m}$ adalah merupakan pernyataan yang equivalent.

(2) jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$ maka $a \equiv c \pmod{m}$.

(3) jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ maka:

$ax+cy \equiv bx+dy \pmod{m}$.

(4) jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ maka $ac \equiv bd \pmod{m}$

(5) jika $a \equiv b \pmod{m}$ dan $d \mid m$, $d>0$, maka $a \equiv b \pmod{d}$.

(6) jika $a \equiv b \pmod{m}$ maka $ac \equiv bc \pmod{mc}$ untuk $c>0$.

**Bukti :**

(1) $a \equiv b \pmod m \Rightarrow a-b=km$ dengan $k=0,\pm1,\pm2,\ldots$

$\Rightarrow m \mid a-b \Rightarrow m \mid -(a-b) \Rightarrow m \mid b-a$ maka $b \equiv a \pmod m$.

$b \equiv a \pmod m \Rightarrow b-a \equiv a-a \pmod m \Rightarrow b-a \equiv 0 \pmod m$ karena

$m \mid a-b \Rightarrow m \mid b-a$ maka $a-b \equiv 0 \pmod m$

$a-b \equiv 0 \pmod m \Rightarrow a-b+b \equiv 0+b \pmod m \Rightarrow a \equiv b \pmod m$

(2) $a \equiv b \pmod m \Rightarrow m \mid a-b$

$b \equiv c \pmod m \Rightarrow m \mid b-c$

sehingga $m \mid (a-b)+(b-c) \Rightarrow m \mid a-c$ maka $a \equiv c \pmod m$

(3) $a \equiv b \pmod m \Rightarrow m \mid a-b \Rightarrow m \mid x(a-b)$

$c \equiv d \pmod m \Rightarrow m \mid c-d \Rightarrow m \mid y(c-d)$

maka $m \mid x(a-b)+y(c-d) \Rightarrow m \mid (ax+cy)-(bx+dy)$ yang artinya

$ax+cy \equiv bx+dy \pmod m$

(4) $a \equiv b \pmod m \Rightarrow m \mid a-b$

$c \equiv d \pmod m \Rightarrow m \mid c-d$ maka :

$m \mid (a-b)(c-d)$ dengan $(a-b)(c-d)=(ac-bd)(b(d-c)+d(b-a))$

sehingga $m \mid (ac-bd)$ jadi $ac \equiv bd \pmod m$

(5) $a \equiv b \pmod m \Rightarrow m \mid a-b$ dengan $m=kd$, $d>0$ maka :

$kd \mid a-b \Rightarrow d \mid a-b \Rightarrow a \equiv b \pmod m$ untuk $d>0$.

(6) $a \equiv b \pmod m \Rightarrow m \mid a-b \Rightarrow mc \mid (a-b)c$ untuk $c>0$ jadi :

$ac \equiv bc \pmod{mc}$

**Teorema 3.2**

Ambil f yang dinyatakan sebagai polinomial dengan koefisien bilangan bulat. Jika $a \equiv b \pmod m$ maka berlaku : $f(a) \equiv f(b) \pmod m$.

**Bukti :**

Diandaikan $f(x)=c_0x^n+c_1x^{n-1}+\ldots+c_n$ dengan $c_i$ adalah bilangan bulat. Dari $a \equiv b \pmod m$ dengan menerapkan teorema 3.1 bagian 4 secara berulang-ulang sehingga didapatkan: $a^2 \equiv b^2 \pmod m$, $a^3 \equiv b^3 \pmod m$,...,$a^n \equiv b^n \pmod m$ dan kemudian $c_j a^{n-j} \equiv c_j b^{n-j} \pmod m$ dan akhirnya didapatkan $c_0a^n+c_1a^{n-1}+\ldots+c_n \equiv c_0b^n+c_1b^{n-1}+\ldots+c_n \pmod m$ didapat dari teorema 3.1 bagian 3. Sehingga terukti bahwa jika: $a \equiv b \pmod m$ maka $f(a) \equiv f(b) \pmod m$.

**Teorema 3.3**

(1) $ax \equiv ay \pmod m$ jika dan hanya jika $x \equiv y \left(\mod \frac{m}{(a,m)}\right)$.

(2) jika $ax \equiv ay \pmod m$ dan $(a,m)=1$ maka $x \equiv y \pmod m$.

(3) $x \equiv y \pmod{m_i}$ untuk $i=1,2,\ldots,r$ jika dan hanya jika $x \equiv y \pmod{[m_1,m_2,\ldots,m_r]}$.

**Bukti :**

(1) jika $ax \equiv ay \pmod m$ maka $ax-ay=mz$ untuk beberapa bilangan bulat $z$, sedemikian hingga diperoleh $\frac{a}{(a,m)}(y-x)=\frac{m}{(a,m)}z$ dan kemudian $\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(y-x)$ Tetapi $\left(\frac{a}{(a,m)},\frac{m}{(a,m)}\right)=1$ dan oleh karena itu maka $\left\{\frac{m}{(a,m)}\right\} \mid (y-x)$ dan pernyataan ini menyatakan bahwa $x \equiv y \left(\mod \left(\frac{m}{(a,m)}\right)\right)$. Akibatnya jika $x \equiv y \left(\mod \left(\frac{m}{(a,m)}\right)\right)$ digandakan dengan a diperoleh $ax \equiv ay \left(\mod \left(\frac{am}{(a,m)}\right)\right)$ dengan menggunakan teorema 3.1 bagian 6.

Tetapi (a,m) adalah pembagi dari a dan dapat ditulis $ax \equiv ay \pmod m$ dari teorema 3.1 bagian 5.

Untuk contoh :

$15x \equiv 15y \pmod{10}$ adalah equivalent dengan $x \equiv y \pmod 2$.

(2) ini adalah merupakan kasus khusus pada bagian 1.

(3) jika $x \equiv y \pmod{m_i}$ untuk $i=1,2,\ldots,r$ maka $m_i \mid (y-x)$ untuk $i=1,2,\ldots,r$ $y-x$ adalah pergandaan biasa dari $m_1, m_2, \ldots, m_r$ dan karena itu $[m_1, m_2, \ldots, m_r] \mid (y-x)$ ini menyatakan bahwa $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

Jika $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$ maka $x \equiv y \pmod{m_i}$ dari teorema 3.1 bagian 5 dengan $m_i \mid [m_1, m_2, \ldots, m_r]$.

Dalam hubungannya dengan bilangan bulat modulo m pada dasarnya dilakukan operasi biasa dari arithmatika tetapi tanpa memperdulikan pergandaan dari m. Dalam pengertian ini tidak dibedakan antara a dan a+mx, dengan x adalah bilangan bulat. Diberikan bilangan bulat a, ambil q dan r sebagai hasil ganda dan sisa pembagian dengan m, jadi $a=qm+r$. Sekarang $a \equiv r \pmod m$ dan dari r yang memenuhi pertidaksamaan $0 \leq r \leq m$, diperoleh bahwa setiap bilangan bulat kongruen modulo m adalah salah satu dari harga-harga $0,1,2,\ldots,m-1$.

Definisi 3.2

Jika $x \equiv y \pmod m$ maka y disebut residu dari x modulo m. Himpunan $x_1, x_2, \ldots, x_m$ disebut sistem residu lengkap modulo m jika untuk setiap bilangan bulat y terdapat satu dan hanya satu $x_j$ sedemikian hingga $y \equiv x_j \pmod m$.

Jelas terdapat tak berhingga sistem residu lengkap modulo m himpunan 1,2,3,...,m-1,m adalah salah satu contoh. Himpunan dari m bilangan bulat adalah berbentuk sistem residu lengkap modulo m jika tidak terdapat dua bilangan bulat dalam himpunan kongruen modulo m.

**Teorema 3.4**

Jika $x \equiv y \pmod m$ maka $(x,m)=(y,m)$.

**Bukti :**

Dari bentuk $x \equiv y \pmod m$ diperoleh persamaan bahwa $y-x=mz$ untuk beberapa bilangan bulat z. Dari $(x,m) \mid x$ dan $(x,m) \mid m$ didapatkan bahwa $(x,y) \mid y$ dan karena itu maka $(x,m) \mid (y,m)$. Kemudian dari persamaan $y-x=mz$ dan dari bentuk $x \equiv y \pmod m$ diketahui bahwa $(y,m) \mid y$ dan $(y,m) \mid m$ sehingga didapatkan bahwa $(x,y) \mid x$ dan karena itu maka $(y,m) \mid (x,m)$ dan karena $(x,m) \mid (y,m)$ dan $(y,m) \mid (x,m)$ maka kemudian diperoleh $(x,m)=(y,m)$ dengan keduanya berharga positif.

**Definisi 3.3**

Reduksi sistem residu modulo m adalah himpunan dari bilangan-bilangan bulat $r_i$ sedemikian hingga $(r_i,m)=1$, $r_i \not\equiv r_j \pmod m$ jika $i \neq j$, sedemikian hingga setiap x prime ke m adalah kongruen modulo m dengan beberapa anggota dari himpunan $r_i$.

**Definisi 3.4**

Bilangan $\phi(m)$ adalah banyaknya bilangan bulat positif yang lebih kecil atau sama dengan m yang merupakan relatif prime terhadap m.

**Teorema 3.5**

Ambil (a,m)=1 misal $r_1, r_2, \ldots, r_n$ adalah komplit atau bagian dari sistem residu lengkap modulo m. Maka $ar_1, ar_2, \ldots, ar_n$ berturut-turut adalah merupakan komplit atau bagian dari sistem residu lengkap modulo m.

**Bukti :**

Diandaikan bahwa (a,m)=c dengan $c \neq 1$ berarti a dan m tidak saling relatif prime. Apabila $r_1, r_2, \ldots, r_n$ adalah sistem residu lengkap modulo m, kemudian dilakukan operasi pergandaan antara bilangan a dengan sistem residu lengkap modulo m. Karena a dan m tidak saling relatif prime, maka akan terdapat hasil pergandaan $ar_i$ dengan i=1,2,3,...,n yang berada dalam klas yang sama. sehingga ada $r_1, r_2, \ldots, r_n$ yang tidak mempunyai kawan dengan salah satu dari $ar_1, ar_2, \ldots, ar_n$ karena ada lebih dari satu $ar_i$ yang berkorespondensi pada $r_i$ yang sama. Sehingga agar $r_1, r_2, \ldots, r_n$ tepat berkorespondensi satu-satu dengan $ar_1, ar_2, \ldots, ar_n$ maka (a,m)=1 atau a dan m saling relatif prime.

**Teorema 3.6 (Teorema Euler)**

Jika (a,m)=1 maka $a^{\phi(m)} \equiv 1 \pmod{m}$

**Bukti :**

Ambil $r_1, r_2, \ldots, r_{\phi(m)}$ sebagai reduksi sistem residu modulo m. Kemudian dari Teorema 3.5 $ar_1, ar_2, \ldots, ar_{\phi(m)}$ adalah juga reduksi sistem residu modulo m. Dari sini dihubungkan dengan tiap-tiap $r_i$ terdapat satu dan hanya satu $ar_j$ sedemikian hingga $r_i \equiv ar_j \pmod m$. Selanjutnya untuk $r_i$ yang berbeda akan dihubungkan dengan $ar_j$ yang berbeda juga. Ini berarti bahwa bilangan-bilangan $ar_1, ar_2, \ldots, ar_{\phi(m)}$ hanya merupakan residu modulo m dari $r_1, r_2, \ldots, r_{\phi(m)}$ tetapi tidak harus dalam orde yang sama. Dengan operasi pergandaan dan dengan menggunakan Teorema 3.1 bagian 4 didapatkan $\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod m$, dan selanjutnya

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod m.$$

Karena $(r_j, m)=1$ maka digunakan Teorema 3.3 bagian 2, dengan menghapus $r_j$ didapatkan bahwa $a^{\phi(m)} \equiv 1 \pmod m$.

**Teorema 3.7** (Teorema Fermat)

Ambil p yang merupakan prime. Jika $p \nmid a$ maka : $a^{p-1} \equiv 1 \pmod p$. Untuk setiap bilangan bulat a, $a^p \equiv a \pmod p$

**Akibat** (Bukti dari Teorema 3.7)

Jika $p \nmid a$ maka $(a,p)=1$ dan $a^{\phi(p)} \equiv 1 \pmod p$. Untuk mendapatkan $\phi(p)$, digunakan definisi 3.4. Semua bilangan-bilangan bulat $1, 2, 3, \ldots, p-1, p$ dengan

pengecualian pada p adalah relatif prime dari p. Jadi diperoleh $\phi(p)=p-1$. Dari Teorema 3.6 didapatkan persamaan $a^{\phi(p)} \equiv 1 \pmod{p}$ dan $\phi(p)=p-1$, maka $a^{p-1} \equiv 1 \pmod{p}$.

**Teorema 3.8**

Jika $(a,m)=1$ maka $ax \equiv b \pmod{m}$ mempunyai solusi $x=x_1$. Setiap solusi diberikan dengan persamaan $x=x_1+jm$ dengan $j=0,\pm1,\pm2,\ldots$

**Bukti :**

Diketahui bahwa $(a,m)=1$ atau saling relatif prime. Dimisalkan solusinya ada 2, yaitu $x_1$ dan $x_2$. Karena $x_1$ dan $x_2$ solusi maka didapatkan bahwa :

$ax_1 \equiv b \pmod{m}$ dan

$ax_2 \equiv b \pmod{m}$

Dari persamaan diatas menyatakan bahwa $ax_1$ dan $ax_2$ berada dalam klas yang sama yaitu b. Serta dengann menggunakan Teorema 3.5, berarti $(a,m) \neq 1$ atau a dan m tidak saling relatif prime. Kontradiksi dengan yang diketahui berarti yang benar hanya ada solusi tunggal. Misal solusi tersebut adalah $x=x_1$ dari $(a,m)=1$ dan $1 \leq m$ didapatkan bahwa $\phi(m) \geq 1$. Maka didapatkan bentuk $x_1=a^{\phi(m)-1}b$. Jika x adalah solusi maka $ax-ax_1 \equiv b-b \equiv 0 \pmod{m}$ dan selanjutnya $a(x-x_1) \equiv 0 \pmod{m}$. Dengan menggunakan teorema 3.3 bagian 2 didapatkan $x-x_1 \equiv 0 \pmod{m}$, yang menyatakan bahwa $x=x_1+jm$ dengan j adalah bilangan bulat.

Teorema 3.9 (Teorema Wilson)

Jika p adalah prime, maka $(p-1)! \equiv -1 \pmod{p}$

**Bukti :**

Diberikan bilangnn bulat j yang memenuhi $1 \leq j \leq p-1$, maka $(j,p)=1$ dan didapatkan dari teorema 3.8 bahwa terdapat bilangan bulat i sedemikian hingga $ji \equiv 1 \pmod{p}$ dan $0 \leq i \leq p-1$ i=0 adalah tidak mungkin, maka didapatkan $1 \leq i \leq p-1$. Dengan tiap-tiap j ini akan dihubungkan dengan bilangan bulat i. Dari $ij \equiv ji \equiv 1 \pmod{p}$ didapat bahwa j adalah bilangan bulat sekawan dengan i. Bilangan bulat 1 adalah sekawan dengan dirinya sendiri. Dengan mengabaikan harga-harga tersebut, diperoleh $2 \leq j \leq p-2$. Sehingga didapatkan $(j-1,p)=(j+1,p)=1$ dan karenanya $j^2-1=(j+1)(j-1) \not\equiv 0 \pmod{p}$. Tiap-tiap j ini akan disekawankan dengan $i \neq j$, $2 \leq i \leq p-2$ dan sekawan dari i adalah j sendiri. Jadi bilangan-bilangan bulat $2,3,\ldots,p-2$ dapat berpasang-pasangan dan $ji \equiv 1 \pmod{p}$. Pergandaan dari semuanya menghasilkan $2.3.\ldots.(p-2) \equiv 1 \pmod{p}$ dan teorema Wilson menyatakan $1.\ldots.(p-1) \equiv -1 \pmod{p}$.

Teorema 3.10

Ambil p prime. Maka $p^2 \equiv -1 \pmod{p}$ mempunyai solusi jika dan hanya jika $p=2$ atau $p \equiv 1 \pmod{4}$.

**Bukti :**

Jika p=2 didapatkan solusi x=1. Untuk beberapa prime yang lain pada harga p dapat dituliskan sebagai teorema Wilson yang berbentuk

$$\left(1.2\ldots j\ldots.\frac{p-1}{2}\right)\left(\frac{p+1}{2}\ldots(p-j)\ldots(p-1)\right) \equiv -1 \pmod{p}$$

hasil pada bagian kiri dibagi dalam 2 bagian, masing-masing dengan bilangan yang sama dari faktor-faktornya. Pasangan-pasangan j dalam bagian pertama dengan p-j pada bagian kedua dapat ditulis dalam kongruensi yang berbentuk

$$\prod_{j=1}^{\frac{(p-1)}{2}} j(p-j) \equiv -1 \pmod{p}$$

tetapi $j(p-j) \equiv -j^2 \pmod{p}$ jika $p \equiv 1 \pmod{4}$, akan didapat persamaan

$$\prod_{j=1}^{\frac{(p-1)}{2}} j(p-j) \equiv \prod_{j=1}^{\frac{(p-1)}{2}} -j^2 \equiv (-1)^{\frac{(p-1)}{2}} \left( \prod_{j=1}^{\frac{(p-1)}{2}} j \right)^2$$

$$\equiv \left( \prod_{j=1}^{\frac{(p-1)}{2}} j \right)^2 \pmod{p}$$

dan ini berarti mempunyai solusi $\prod_{j=1}^{\frac{(p-1)}{2}} j$, dari $x^2 \equiv -1 \pmod{p}$

Jika $p \neq 2$ dan $p \neq 1 \pmod{4}$ maka $p \equiv 3 \pmod{4}$. Dalam kasus ini, jika untuk beberapa bilangan bulat x, $x^2 \equiv -1 \pmod{p}$, maka diperoleh $x^{p-1} \equiv (x^2)^{\frac{(p-1)}{2}} \equiv (-1)^{\frac{(p-1)}{2}} \equiv -1 \pmod{p}$ dengan $\frac{(p-1)}{2} \equiv 1 \pmod{2}$. tetapi jelas $p \nmid x$, didapat $x^{p-1} \equiv 1 \pmod{p}$

dari Teorema 3.6. Kontradiksi ini menunjukkan bahwa $x^2 \equiv -1 \pmod{p}$ tidak mempunyai solusi dalam kasus ini.

## 3.2 SOLUSI DARI KONGRUENSI

Solusi masalah kongruensi adalah analog dengan solusi pada persamaan aljabar. Dalam bab ini akan didefinisikan $f(x)$ sebagai polinomial dengan koefisien bilangan bulat dan ditulis dalam bentuk $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$. Jika u adalah bilangan bulat sedemikian hingga $f(u)\equiv 0 \pmod{m}$ maka dikatakan u adalah solusi dari $f(x)\equiv 0 \pmod{m}$, bilangan bulat atau bukan bilangan bulat adalah merupakan solusi dari kongruensi pada modulus m maupun pada polinomial $f(x)$. Jika bilangan bulat u adalah solusi dari $f(x)\equiv 0 \pmod{m}$, dan jika $v\equiv u \pmod{m}$, teorema 3.2 menunjukkan bahwa v adalah juga merupakan solusi. Karena disebutkan bahwa $x\equiv u \pmod{m}$ adalah solusi dari $f(x)\equiv 0 \pmod{m}$, yang berarti bahwa setiap bilangan bulat kongruen ke u modulo m memenuhi $f(x)\equiv 0 \pmod{m}$.

## 3.3 ALGORITHMA UNTUK KONGRUENSI LINEAR DAN TEOREMA CHINESE REMAINDER

Diberikan bilangan bulat a,b dan $m>1$, dikatakan bahwa $ax\equiv b \pmod{m}$ adalah kongruensi dari derajad satu atau kongruensi linear. Pokok pembicaraan adalah apakah kongruensi mempunyai banyak solusi untuk x dan jika demikian bagaimana harganya dapat diperoleh. Yang pertama dibahas adalah pertanyaan tentang keberadaan suatu solusi

dari kongruensi. Dan jika diberikan algorithma untuk menentukan solusi dalam kasus numerik.

Dalam teorema 3.8 diketahui bahwa jika (a,m)=1, maka $ax\equiv b \pmod m$ dapat diselesaikan dengan tepat satu solusi, dikatakan $x\equiv x_1 \pmod m$. Selanjutnya diandaikan bahwa $g|b$. Maka kongruensi $ax\equiv b \pmod m$ dapat diselesaikan jika dan hanya jika terdapat bilangan bulat x sedemikian hingga $m|(ax+b)$. Dengan g adalah pembagi dari m,a dan b ini adalah equivalen dengan pertanyaan apakah terdapat bilangan bulat x sedemikian hingga $m|g$ adalah pembagi pada $(ax+b)|g$.

**Teorema 3.11**

Kongruensi $ax\equiv b \pmod m$ mempunyai tepat satu solusi jika (a,m)=1. Lebih umum, jika g dinotasikan sebagai faktor persekutuan terbesar (a,m). Kongruensi ini dapat diselesaikan jika dan hanya jika $g|b$. Jika $g|b$ maka kongruensi ini mempunyai tepat g solusi $x\equiv x_o+t(m/g) \pmod m$ untuk $t=0,1,2,\ldots,g-1$ dengan $x_o$ adalah merupakan solusi dari $(a/g)x\equiv(b/g) \pmod{m/g}$.

**Bukti :**

Karena $m\geq 1$, maka terlihat bahwa $\phi(m)\geq 1$, dengan $\phi$ adalah fungsi yang didefinisikan oleh Euler sebagai $\phi(m)=(0<z<m, (z,m)=1)$. Dari teorema Fermat diperoleh, jika $\phi(m)=1$ maka $a^{\phi(m)}\equiv 1 \pmod m$. Dari hasil ini dapat dikonstruksikan $x_o=a^{\phi(m)-1}b$, yang merupakan penyelesaian

dari $ax \equiv b \pmod m$ dan bentuk yang demikian adalah tunggal. Andaikan g bukan merupakan pembagi dari b ( dinotasikan $g \nmid b$ ), maka $g \nmid (ax-b)$ sehingga berlaku pula $m \nmid (ax-b)$, akibatnya $ax \equiv b \pmod m$ tidak mempunyai penyelesaian.

Jika $g \mid b$ maka $ax \equiv b \pmod m$ mempunyai penyelesaian jika ditemukan $x_o$ sedemikian hingga $m \mid (ax_o - b)$. Karena $g \mid m$, $g \mid b$ dan $g \mid a$, maka dapat pula dikatakan $ax \equiv b \pmod m$ mempunyai penyelesaian jika $(m/g) \mid ((ax_o - b)/g)$.

Karena $((a/g),(m/g))=1$, maka $((ax-b)/g) \equiv 0 \pmod{m/g}$ juga mempunyai penyelesaian tunggal yaitu $x_o$ yang tentu juga merupakan penyelesaian dari $ax \equiv b \pmod m$.

Untuk mencari penyelesaian lengkap dari $ax \equiv b \pmod m$ dapat dikonstruksikan sebagai berikut:

$$x_1 = x_o + (m/g)$$

$$x_2 = x_o + (2m/g)$$

.....

.....

.....

$$x_g = x_o + (g-1)(m/g)$$

Bila harga-harga a,b dan m relatif besar, pemilihan harga awal dengan cara coba-coba dari penyelesaian pada $ax \equiv b \pmod m$ cukup sulit. Sehingga bentuk asli perlu direduksi menjadi bentuk yang lebih sederhana, sehingga memudahkan pemilihan harga dari penyelesaian awal.

Algorithma untuk menyederhanakan dan mencari penyelesaian dari $ax \equiv b \pmod m$ adalah sebagai berikut:

*(1) Bentuk* $ax \equiv b \pmod m$ *direduksi menjadi* $my \equiv -b \pmod a$

*tujuannya adalah membentuk kongruensi baru dengan harga modulus yang lebih kecil.*

(2) *Dengan menggunakan sifat-sifat kongruensi dilakukan proses penyederhanaan bentuk dan dicoba untuk mencari penyelesaian awal secara coba-coba. Bila pencarian penyelesaian awal sulit dilakukan karena harga-harga a,b dan m masih cukup besar, maka kembali ke langkah awal, sampai diperoleh bentuk kongruensi yang mudah dicari penyelesaian awalnya.*

(3) *Jika* $y_o$ *merupakan penyelesaian* $my \equiv -b \pmod a$ *maka* $my_o+b$ *merupakan kelipatan dari* a, *dikatakan* $my_o+b=ax_o$ *dan* $x_o=(my_o+b)/a$ *merupakan penyelesaian dari :*

$ax \equiv b \pmod m$.

**Contoh 1 :**

Akan dicari penyelesaian dari $6x \equiv 9 \pmod{21}$.

Bentuk $6x \equiv 9 \pmod{21}$ dapat disederhanakan dengan membagi bentuk tersebut dengan 3 sehingga menjadi $2x \equiv 3 \pmod 7$ yang berarti a=2 b=3, dan m=7. Terlihat bahwa $(a,m)=(2,7)=1$ sehingga mempunyai penyelesaian tunggal, dan dengan coba-coba diperoleh $x_o=5$. Penyelesaian lengkap dari $6x \equiv 9 \pmod{21}$ ada 3 penyelesaian karena $(a,m)=(6,21)$ ada 3. Adapun penyelesaian lengkapnya adalah sebagai berikut :

$x_o=5$

$x_1=5+(21/3)$ $\quad x_1=12$

$x_2=5+2(21/3)$ $\quad x_2=19$

**Contoh 2 :**

Mencari bentuk penyelesaian dari $863x \equiv 880 \pmod{2151}$. Bentuk $863x \equiv 880 \pmod{2151}$ direduksi menjadi bentuk baru dengan harga modulus yang lebih kecil $2151y \equiv -880 \pmod{863}$, selanjutnya disederhanakan menjadi $425y \equiv -880 \pmod{863}$, hal ini memungkinkan karena $2151 = 1726 + 425$. Bentuk terakhir disederhanakan lagi menjadi $425y \equiv -17 \pmod{863}$ dan direduksi menjadi $863z \equiv 17 \pmod{425}$, disederhanakan menjadi $13z \equiv 17 \pmod{425}$, direduksi menjadi $425w \equiv -17 \pmod{13}$ disederhanakan menjadi $9w \equiv -4 \pmod{13}$ atau $9w \equiv 9 \pmod{13}$, sehingga $w \equiv 1 \pmod{13}$, sehingga $w = 1$ merupakan penyelesaian awal secara iterasi langkah demi langkah dikembalikan ke kongruensi yang direduksi sehingga

$$z_o = \frac{425.1 + 17}{13} = 34$$

$$y_o = \frac{863.34 - 17}{425} = 69$$

$$x_o = \frac{2151.69 + 880}{863} = 173$$

$x_o = 173$ merupakan peyelesaian tunggal karena $(865, 2151) = 1$. Langkah-langkah iterasi senantiasa menggunakan bentuk-bentuk yang direduksi secara langsung pada tahap reduksi berikutnya atau dengan kata lain menggunakan bentuk paling sederhana pada tiap tingkat reduksi. Sebagai contoh, pada tahap mencari $z_o$ digunakan bentuk dari $13z \equiv 17 \pmod{425}$ bukan bentuk $863z \equiv 17 \pmod{425}$.

Contoh 3 :

Mencari penyelesaian dari $6x\equiv4 \pmod 9$

Terlihat bahwa a=6, b=4 dan m=9. Karena $(6,9)=3$ dan bukan merupakan pembagi dari 4, maka bentuk $6x\equiv4 \pmod 9$ tidak mempunyai penyelesaian.

Teorema 3.12 (Teorema Chinnese Remainder)

Ambil $m_1, m_2, \ldots, m_r$ yang menyatakan r buah bilangan bulat yang saling relatif prime. Maka kongruensi dari $x\equiv a_i \pmod m$, $i=1,2,\ldots,r$ mempunyai penyelesaian umum. Terdapat 2 solusi kongruen modulo $m_1, m_2, \ldots, m_r$.

Dengan lain perkataan :

Jika moduli $m_1, m_2, \ldots, m_r$ bukan pasangan yang relatif prime, maka tidak mungkin ada solusi yang kongruen.

Bukti :

Dinyatakan $m=m_1 . m_2 \ldots . m_r$ maka terlihat bahwa $m \mid m_j$ adalah bilangan bulat dan bahwa $(m/m_j, m)=1$. Sedemikian hinngga dari teorema 3.8, terdapat bilangan bulat $b_j$ sedemikian hingga $(m/m_j)b_j\equiv1\pmod{m_j}$. Sehingga jelas bahwa $(m/m_j)b_j\equiv0 \pmod{m_i}$ jika $i\neq j$. Sekarang jika didefinisikan $x_o$ sebagai :

$$x_o=\sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \qquad (3.1)$$

maka akan diperoleh

$$x_o \equiv \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}$$

Sedemikian hingga $x_o$ adalah solusi umum dari kongruensi asal. Jika $x_o$ dan $x_1$ keduanya adalah solusi umum $x \equiv a_i \pmod{m}$, $i=1,2,\ldots,r$, maka didapatkan $x_o \equiv x_1 \pmod{m_i}$ untuk $i=1,2,3,\ldots,r$ dan karena itu $x_o \equiv x_1 \pmod{m}$ diperoleh dari teorema 3.3 bagian 3.

**Contoh 4 :**

Mencari penyelesaian kongruensi $19x \equiv 1 \pmod{140}$ ini sama dengan mencari solusi simultan dari :

$19x \equiv 1 \pmod{4}$ $19x \equiv 1 \pmod{5}$ $19x \equiv 1 \pmod{7}$

solusi-solusi dari kongruensi ini adalah :

$x \equiv 3 \pmod{4}$ $x \equiv 4 \pmod{5}$ $x \equiv 3 \pmod{7}$

sekarang digunakan teorema diatas dengan :

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

dengan bilangan-bilangan bulat $b_1, b_2, b_3$ didapat dengan menggunakan kongruensi $(m/m_j)b_j \equiv 1 \pmod{m_j}$, maka :

$35b_1 \equiv 1 \pmod{4}$ $28b_2 \equiv 1 \pmod{5}$ $20b_3 \equiv 1 \pmod{7}$

yang kemudian didapatkan $b_1=-1$ $b_2=2$ $b_3=-1$

dengan menggunakan persamaan (3.1) maka didapatkan bahwa :

$$x_o = \frac{140}{5}(-1)(3) + \frac{140}{4}(2)(4) + \frac{140}{7}(-1)(3) = 136$$

sehingga diperoleh kongruensi $x \equiv 136 \pmod{140}$

harga-harga dari $b_1, b_2, b_3$ bukan merupakan satu-satunya

jawab. Kemungkinan jawab yang lain adalah $b_1=3$ $b_2=2$ $b_3=-1$ dan darisini dengan menggunakan persamaan (3.1) akan diperoleh hasil :

$$x_o=\frac{140}{5}(3)(3)+\frac{140}{4}(2)(4)+\frac{140}{7}(-1)(3)=472$$

tetapi $x\equiv 472 \pmod{140}$ hanya merupakan alternatif jawab yang lain.

Contoh 5 :

Mencari bilangan bulat terkecil yang diberikan dengan sisa 1,2,3,4 dan 5 yang dibagi dengan 3,5,7,9 dan 11 secara berulang-ulang.

Dalam hubungan dengan ini pemecahan masalahnya adalah :

$x\equiv 2 \pmod 5$ $x\equiv 3 \pmod 7$ $x\equiv 4 \pmod 9$ $x\equiv 5 \pmod{11}$

yang merupakan bentuk yang simultan.

Dengan $x\equiv 1 \pmod 3$ diabaikan karena telah dinyatakan dengan $x\equiv 4 \pmod 9$. Dari persamaan diatas didapat :

$m_1=5$ $m_2=7$ $m_3=9$ $m_4=11$ dan $a_1=2$ $a_2=3$ $a_3=4$ $a_4=5$

selanjutnya diperlihatkan bahwa $b_1,b_2,b_3,b_4$ yang memenuhi adalah $693b_1\equiv 1 \pmod 5$ $495b_2\equiv 1 \pmod 7$ $385b_3\equiv 1 \pmod 9$ $315b_4\equiv 1 \pmod{11}$ yanng kemudian didapatkan bahwa :

$b_1=-3$ $b_2=3$ $b_3=4$ $b_4=-3$ dengan dua darinya dipilih negatif untuk mendapatkan $x_o$ dalam bentuk yang sederhana.

Dengan menggunakan persamaan (3.1) diperoleh :

$x_o=(693)(-3)(2)+(495)(3)(3)+(385)(4)(4)+(315)(-3)(5)=1732$

ini adalah bilangan bulat terkecil yang memenuhi keadaan yang diberikan. Semua solusi yang lain dari kongruensi ini

pdiperoleh dengan cara menambah atau mengurangi 3465 secara berulang-ulang terhadap 1732.