Kongruen Lanjar dan Berbagai Aplikasi dari Kongruen Lanjar

Mario Tressa Juzar (13512016)[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13512016@std.stei.itb.ac.id

***Abstract*—Makalah ini akan membahas tentang salah satu obyek studi di bidang teori bilangan, yaitu kongruen lanjar. Disini akan dibahas mulai dari apa itu definisi kongruen lanjar, sifat kekongruenan lanjar, serta berbagai aplikasi dari kongruen lanjar.**

***Index Terms*—teori bilangan, kongruen lanjar, aplikasi kongruen lanjar.**

I. PENDAHULUAN

Banyak keilmuan yang sudah ada dan berkembang di dunia ini. Salah satunya yaitu bidang keilmuan matematika. Di matematika sendiri terdapat cabang ilmu yaitu Matematika Diskrit. Matematika Diskrit yaitu cabang keilmuan di bidang matematika yang membahas obyek-obyek diskrit. Salah satu bagian dari Matematika Diskrit yang ingin penulis bahas adalah kongruen lanjar. Kongruen lanjar merupakan bagian dari obyek studi di bidang teori bilangan di Matematika Diskrit.

Kongruen lanjar mulai berkembang dan mulai banyak diaplikasikan dalam kehidupan sehari-hari. Kongruen lanjar sendiri memiliki banyak aplikasi dalam penyelesaian berbagai masalah, seperti *Chinese Remainder Theorem*, uji bilangan prima, untuk mencek digit ISBN, dan berbagai hal lainnya yang memungkinkan penggunaan dari sifat kongruen lanjar itu sendiri.

Dewasa ini, dengan perkembangan zaman yang cukup pesat, kita butuh keamanan dalam pengiriman informasi. Cara untuk menjaga keamanan dari informasi tersebut adalah dengan meng-enkripsi data dari informasi tersebut dan setelah sampai ke orang yang dituju baru di-dekripsi sehingga bisa dipahami kembali. Dari sini muncullah cabang keilmuan yaitu Kriptografi yang secara dasarnya menggunakn sifat dari kongruen lanjar sehingga data bisa di-enkripsi secara aman dengan menggunakan 'kunci' tertentu.

Dari sini terlihat betapa pentingnya kongruen lanjar dewasa ini, salah satunya adalah contoh kasus di atas. Menyadari pentingnya kongruen lanjar, banyak para ilmuwan meneliti kongruen lanjar untuk mengembangkan algoritma tertentu.

II. TEORI DASAR

A. Keterbagian

Teori Bilangan merupakan salah satu bidang dari matematika diskrit yang mencakup bahasan tentang bilangan bulat serta teorema yang mendasarinya. Salah satu teorema dasar dalam teori bilangan adalah teori keterbagian atau yang lebih dikenal dengan Teorema Euclidian.

Teorema Euclidian :

"Misalkan x dan y bilangan bulat, dengan y > 0. Jika x dibagi y maka akan terdapat bilangan unik q(*quotient*) dan r(*remainder*), sedemikian sehingga

$$x = q.y + r$$

dengan $0 \leq r < y$"

Dari teorema diatas, bisa dikatakan bahwa jika sebuah bilangan x dibagi y maka pasti akan ada bilangan q dan r yang memenuhi persamaan dari teorema diatas.

Selanjutnya, terdapat kasus khusus dimana r = 0. Hal ini dijelaskan dalam definisi membagi dibawah ini.

Definisi membagi:

"Misalkan x dan y bilangan bulat, dengan $a \neq 0$. y dikatakan membagi x jika terdapat bilangan bulat q sedemikian sehingga x = q.y"

Membagi ini dilambangkan dengan "|", misal x habis membagi y maka dituliskan dengan "x|y".

Dalam kaitannya dengan teorema Euclidian, didefinisikan x = q.y + r, jika habis membagi maka nilai r=0.

Jika x = q.y + r dengan $r \neq 0$ maka dikatakan y tidak habis membagi x, dan dilambangkan dengan "x ł y".

Selanjutnya, konsep keterbagian ini digunakan dalam mencari faktor pembagi bersama terbesar.

Pembagi bersama terbesar(*great common divisor – gcd*) dari bilangan bulat x dan y adalah d sedemikian sehingga d habis membagi x dan d habis y. Dinyatakan dalam bentuk gcd(x,y) = d.

Selanjutnya, terdapat teorema :

"Misalkan x dan y bilangan bulat, dengan y > 0, sedemikian sehingga

$$x = q.y + r, \quad 0 \leq r < y$$

maka gcd(x,y) = gcd(y,r)"

Misalkan x dan y adalah bilangan bulat tak negatif dengan $x \geq y$. Misalkan $r_0 = x$ dan $r_1 = y$.

Lakukan secara berturut-turut pembagian untuk memperoleh

$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 \leq r_1,$
$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 \leq r_2,$
$\vdots$
$r_{n-2} = r_{n-1}\, q_{n-1} + r_n \quad 0 \leq r_n \leq r_{n-1},$
$r_{n-1} = r_n q_n + 0$

$\gcd(x,y) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.

r_n merupakan pembagi bersama terbesar dari bilangan bulat x dan y.

Berikutnya, kita kenal istilah *divisor*(pembagi) dan faktor. Dua istilah ini memiliki makna dan esensi yang sama, yaitu misalkan x dan y bilangan bulat, x dikatakan divisor/faktor dari y jika x|y.

B. Modulo

Modulo adalah sebuah operasi bilangan yang menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lainnya.

Teori dasar modulo:

"Misalkan x adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi modulo x mod m (dibaca 'x modulo m') memberikan sisa jika x dibagi dengan m. Dengan mengikuti teorema euclidian maka:

x mod m = r, sedemikian sehingga
x = q.m + r, dengan $0 \leq r < m$

Bilangan m disebut modulus atau modulo, dan r merupakan hasil dari aritmetika modulo dimana r terletak dalam selang {0,1,2,...,m-1}".

Dari teori dasar modulo diatas sudah sangat menjelaskan apa itu modulo. Modulo ini berlaku untuk seluruh x bilangan bulat yang artinya juga berlaku untuk bilangan bulat negatif.

Untuk bilangan bulat negatif maka operasi modulonya akan mengikuti :

-x mod m = r, sedemikian sehingga
-x = q.m + r, dengan $0 \leq r < m$, dan $q < 0$

Disini nilai sisa(*remainder*) haruslah lebih besar atau sama dengan 0 dan kurang dari m, dan akan menyebabkan nilai q nya menjadi lebih kecil dari 0.

Beberapa kesalahan yang terjadi adalah dengan membuat nilai r itu kurang dari 0, sedangkan dalam konsep keterbagian nilai dari r harus lebih besar atau sama dengan 0.

Contoh kasus: -17 mod 7

Dengan mengikuti teori dasar modulo diatas maka

-17 mod 7 = 4, nilai 4 didapat dari -17 = -3(7) + 4.

Sedangkan kesalahan yang sering terjadi adalah seperti ini -17 = -2(7) + (-3), yang menyebabkan nilai sisa r nya kecil dari 0. Jawaban -17 mod 7 adalah 4, bukan -3.

Selanjutnya, terdapat kasus khusus dimana hasil modulo itu adalah 0. Jika hasil x mod m adalah 0, maka bisa dikatakan x merupakan bilangan kelipatan m.

C. Kongruen Lanjar

Setelah membahas definisi dan teorema-teorema mengenai sifat keterbagian pada bilangan dan modulo, sekarang kita akan membahas apa itu kongruen lanjar. Sebelum itu, terlebih dahulu akan dibahas mengenai kongruen. Berikut merupakan definisi formal mengenai kongruen.

Definisi kongruen:

"Misalkan x dan y adalah bilangan bulat dan m adalah bilangan bulat > 0. Bilangan x dan y dikatakan kongruen dalam modulo m jika dan hanya jika keduanya memberikan hasil sisa bagi yang sama ketika dibagi dengan m."

Kongruen secara simbolik dilambangkan dengan "≡". Jadi untuk definisi diatas secara simbolik ditulis menjadi:

$x \equiv y \pmod m$

Selanjutnya, sesuai dengan teorema sebelumnya, $x = q_1.m + r$, dan $y = q_2.m + r$, dengan melakukan operasi pengurangan

$x - y = (q_1.m + r) - (q_2.m + r)$
$x - y = q_1.m - q_2.m$

Dengan memanfaatkan sifat distributif perkalian

$x - y = (q_1 - q_2)m$

Dari sini bisa katakan bahwa x – y habis dibagi dengan m. Atau secara simbolis ditulis $m|(x-y)$.

Selanjutnya, kongruen juga dapat didefinisikan :

"Misalkan x dan y adalah bilangan bulat dan m adalah bilangan bulat > 0. Bilangan x dan y dikatakan kongruen dalam modulo m jika dan hanya jika x – y habis dibagi oleh m."

Secara matematis ditulis

$x \equiv y \pmod m \quad \leftrightarrow \quad m|(x-y)$

Kekongruenan dapat dituliskan dalam bentuk persamaan lanjar. Kekongruenan $x \equiv y \pmod m$ dapat dituliskan menjadi

$x = y + k.m$

dimana k merupakan bilangan bulat.

Berdasarkan definisi aritmetika modulo sebelumnya, maka x mod m = y dapat dituliskan sebagai

$x \equiv y \pmod m$.

Selanjutnya, akan dibahas sifat-sifat yang berlaku pada kongruen. Berikut ini merupakan sifat-sifat dasar pada kekongruenan :

i. Jika diketahui $x \equiv y \pmod m$ dan p merupakan sembarang bilanga positif
   Maka berlaku operasi:
   a. $x + p = (x + p) \pmod m$
   b. $xp = yp \pmod m$
   c. $x^p = x^p \pmod m$
   Berikut merupakan pembuktian darimana asal ketiga operasi tersebut:
   Karena $x \equiv y \pmod m$, maka bisa dituliskan menjadi $x = y + k.m$.
   Lalu dilakukan operasi penjumlahan
   $x + p = y + k.m + p$
   $(x + p) = (y + p) + k.m$
   $(x + p) = (y + p) \pmod m$ ..(a)

Untuk yang selanjutnya dilakukan operasi perkalian

$x.p = p.(y + k.m)$

$x.p = y.p + p.k.m$

$x.p = y.p \pmod m$ ..(b)

Untuk yang selanjutnya dilakukan operasi perpangkatan

$x^p = (y + k.m)^p$

$x^p = y^p + 2.y.k.m + (k.m)^p$

$x^p = y^p + m(2yk + k^p.m^{p-1})$

$x^p = y^p \pmod m$ ..(c)

ii. Jika diketahui $x \equiv y \pmod m$ dan $a \equiv b \pmod m$

Maka berlaku operasi:

a. $x + a = (y + b) \pmod m$

b. $xa = yb \pmod m$

Berikut merupakan pembuktian darimana asal kedua operasi tersebut:

Karena $x \equiv y \pmod m$, maka bisa ditulis menjadi $x = y + k.m$, dan $a \equiv b \pmod m$ bisa ditulis juga menjadi $a = b + l.m$.

Lakukan operasi penjumlahan

$(x + a) = (y + k.m) + (b + l.m)$

$(x + a) = (y + b) + (k.m + l.m)$

$(x + a) = (y + b) + m(k + l)$

$(x + a) = (y + b) \pmod m$ ..(a)

Dengan melakukan operasi perkalian

$x.a = (y + k.m)(b + l.m)$

$x.a = y.b + y.l.m + b.k.m + k.l.m^2$

$x.a = y.b + m(y.l + b.k + k.l.m)$

$x.a = y.b \pmod m$ ..(b)

Setelah membahas mengenai kongruen dan sifat-sifatnya, selanjutnya kita akan membahas mengenai kongruen lanjar. Apa itu sebenarnya kongruen lanjar? Berikut penjelasannya.

Definisi kongruen lanjar:

"Misalkan x dan y adalah bilangan bulat, m adalah bilangan bulat >0 dan z merupakan peubah bilangan bulat, maka x dan y dikatakan kongruen lanjar dengan peubah z dalam modulo m jika dan hanya jika untuk semua z yang menyebabkan hasil sisa bagi x.z dan y bernilai sama jika dibagi dengan m."

Secara matematis ditulis dengan

$x.z = y \pmod m$

z merupakan peubah bilangan bulat.

Ini membuat kongruen seperti hampir mirip dengan persamaan lanjar seperti persamaan garis $y = mx + c$, tapi ini lanjar dalam hal kongruen. Kongruen lanjar sendiri mempunya solusi z.

Karena z merupakan peubah, maka kita butuh solusi untuk z. Cara mencari solusi untuk z dengan

$x.z = y \pmod m$

$x.z = y + k.m$

$z = (y + k.m)/x$

Untuk menemukan solusi z, maka kita bisa mencoba dengan mengganti nilai k dengan sembarang bilangan bulat, bisa positif atau negatif, dimana k tersebut harus menghasilkan nilai z yang merupakan bilangan bulat.

III. APLIKASI KONGRUEN LANJAR

Kongruen lanjar tidak hanya sekedar konsep, namun juga ada penerapan konkret dari kongruen dalam penyelesaian sebuah permasalahan. Berikut ini akan dijelaskan mengenai aplikasi dari kongruen lanjar di berbagai bidang.

A. Chinese Remainder Theorem

Pada abad pertama, seorang matematikawan asal China yang bernama Sun Tse mengajukan pertanyaan berikut ini:

"Tentukan sebuah bilangan bulat yang jika dibagi dengan 5 menyisakan 3, apabila dibagi dengan 7 menyisakan 5, dan apabila dibagi dengan 11 menyisakan 7."

Ini merupakan awal dari dikenalnya "*Chinese Remainder Theorem." Chinese Remainder Theorem* ini bisa menjawab persoalan tadi dengan penyelesaian menggunakan kongruen lanjar.

Definisi *Chinese Remainder Theorem:*

"Misalkan $m_1,m_2,...,m_n$ adalah bilangan bulat positif sedemikian sehingga nilai pembagi bersama terbesarnya $\gcd(m_i,m_j) = 1$ untuk $i \neq j$. Maka sistem kongruen lanjar

$x \equiv a_k \pmod{m_k}$

mempunyai sebuah solusi unik dalam modulo $m = m_1.m_2...m_n$.

Secara garis besar, algoritma dari *Chinese Remainder Theorem* adalah sebagai berikut:

1) Ubah kongruen lanjar $x \equiv y \pmod m$ kedalam hubungan $x = y + k.m$.
2) Subtitusi bentuk hubungan kongruen lanjar tersebut ke dalam kongruen lanjar yang selanjutnya. Dalam mengganti bentuk hubungan kongruen lanjar harus dalam bentuk yang valid. Jika tidak valid harus dirubah kedalam bentuk yang valid terlebih dahulu.
3) Subtitusi hasil yang didapat dalam hubugan kongruen lanjar yang pertama tadi.
4) Ulangi langkah (2) dan (3) hingga didapatkan hasil terakhir.
5) Hasilnya yang memenuhi sistem kongruen lanjar.

Selanjutnya, kita coba cari solusi untuk pertanyaan Sun Tse tersebut.

"Sebuah bilangan bulat jika dibagi dengan 5 menyisakan 3"

Dalam bentuk kongruen lanjar

$x \equiv 3 \pmod 5$

$x = 3 + 5k_1$ ..(i)

"apabila dibagi dengan 7 menyisakan 5"

$x \equiv 5 \pmod 7$ ..(ii)

"apabila dibagi dengan 11 menyisakan 7"

$x \equiv 7 \pmod{11}$ ..(iii)

Selanjutnya, subtitusikan (i) ke (ii)

$3 + 5k_1 = 5 \pmod 7$

$5k_1 = 2 \pmod 7$

$k_1 = 6 \pmod 7$

$k_1 = 6 + 7k_2$ ..(iv)

Selanjutnya, subtitusikan (iv) ke (i)

$x = 3 + 5k_1$

$x = 3 + 5(6 + 7k_2)$

$x = 33 + 35k_2$ ...(v)

Selanjutnya, subtitusikan (v) ke (iii)

$33 + 35k_2 = 7 \pmod{11}$

$35k_2 = 4 \pmod{11}$

$k_2 = 9 \pmod{11}$

$k_2 = 9 + 11k_3$ ...(vi)

selanjutnya, subtitusikan (vi) ke (v)

$x = 33 + 35k_2$

$x = 33 + 35(9 + 11k_3)$

$x = 348 + 385k_3$

karena, semua kongruen lanjar sudah disubtitusi dan dipatkan solusi $x = 348 + 385k_3$ atau dalam bentuk kongruen lanjar menjadi

$x \equiv 348 \pmod{385}$

dengan mengambil nilai x terkecil, maka x = 348, dan semua solusinya adalah x yang merupakan nilai yang kongruen dengan 348 (mod 385).

B. Public-Key Cryptography (Algoritma RSA)

Kriptografi adalah ilmu yang mempeljari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data.

Pada prinsipnya, kriptografi memiliki 4 komponen utama yaitu :

1) Plaintext, yaitu pesan yang dapat dibaca.
2) Ciphertext, yaitu pesan yang telah di enkripsi yang tidak bisa dibaca dengan cara biasa.
3) Key, yaitu kunci untuk melakukan teknik kriptografi.
4) Algoritma, yaitu metode untuk melakukan enkripsi dan dekripsi.

Disini, kita akan lebih membahas tentang public-key. Algoritma yang dipakai adalah algoritma RSA. Algoritma RSA ditemukan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1977.

Algoritma RSA termasuk dalam *Public-Key Cryptogrhapy* karena terdapat dua kunci yang dibutuhkan untuk mengenkripsi dan mendekripsi data, yaitu kunci publik dan kunci privat. Kunci publik ini disebarluaskan dan digunakan untuk mengenkripsi data. Sedangkan, kunci privat merupakan kunci untuk mendekripsi data yang telah dienkripsi dengan kunci publik.

Dalam mengenkripsi dan dekripsi data dan informasi digunakanlah sistem kongruen lanjar ini.

Untuk mengenkripsi dan dekripsi dibutuhkan sebuah kunci, berikut adalah langkah-langkah menentukan kunci publik dan kunci privat pada algoritma RSA[1]:

1) Ambil dua bilangan prima yang sangat besar, p dan q
2) Hitung bilangan RSA, n = pq.
3) Hitung totien n, $\varphi(n) = (p-1)(q-1)$
4) Pilih suatu bilangan e dimana $1 < e < \varphi(n)$ dan e relatif prima terhadap $\varphi(n)$. Bilangan ini akan menjadi kunci publik bersama n.
5) Tentukan kunci privat d dari kekongruean lanjar $ed \equiv 1 \pmod m$

Selanjutnya, misalkan data yang akan dienkripsi adalah bilangan bulat x. Maka rumus yang digunakan untuk enkripsi dan dekripsi adalah:

- Enkripsi

  $c = x^e \pmod m$
- Dekripsi

  $p = c^d \pmod m$

Algoritma RSA ini memanfaatkan kongruen lanjar dalam penentuan kuncinya. Dengan kongruen lanjar bisa membuat kunci yang lebih baik, terutama dengan pembutan dan penentuan kunci yang sangat baik. Dalam menentukan nilai p dan q dicari bilangan prima yang sangat besar agar kuncinya jauh lebih aman. Dalam hal ini, setelah kunci publik didapatkan maka, kita harus mencari kunci privat dengan menggunakan kongruen lanjar.

C. Uji Bilangan Prima dengan Teorema Fermat

Sebelum kita menguji sebuah bilangan prima, terlebih dahulu kita harus tahu apa itu bilangan prima.

Definisi bilangan prima:

"Sebuah bilangan bulat p > 1 disebut bilangan prima, jika bilangan tersebut hanya memiliki pembagi positif 1 dan p. Bilangan bulat p yang lebih dari 1 yang bukan bilangan prima disebut bilangan komposit"[4].

Bilangan prima adalah bilangan yang unik, karena hanya memiliki dua faktor, yaitu 1 dan dirinya sendiri. Salah satu keunikan lainnya adalah, Teorema Dasar Aritmatika dalam buku *Elements* yang dikarang oleh Euclid, yang menyebutkan:

"Semua bilangan bulat n > 1 dapat ditulis sebagai hasil kali dari bilangan-bilangan prima. Penulisan ini unik, dengan mengabaikan urutan penulisan bilangan-bilangan prima tersebut"[4].

Setelah mengetahui apa itu bilangan prima sekarang kita akan mencoba menguji bilangan prima. Disini kita akan menggunakan teorema Fermat. Teorema Fermat ini merupakan dasar dari berbagai macam algoritma untuk menguji bilangan prima. Teorema Fermat ini cukup sederhana tapi sangat mangkus untuk menentukan apakah sebuah bilangan bisa dikatakan bilangan prima atau bukan. Meskipun teorema ini tidak 100% bisa menentukan keprimaan dari sebuah bilangan.

Teorema Fermat:

"Misalkan p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu memenuhi gcd(a,p) = 1, maka

$A^{p-1} \equiv 1 \pmod p$"

Berikut merupakan pembuktian untuk teorema fermat:

Perhatikan (p-1) buah bilangan kelipatan a berikut ini

a, 2a, 3a, ..., (p-1)a

tidak ada diantara semua bilangan ini yang kongruen

modulo p satu sama lain. Jika ada

$ra \equiv sa \pmod p$ $\quad 1 < r < s < p-1$

Maka, a dapat dicoret menghasilkan $r \equiv s \pmod p$, padahal $1 < r < s < p-1$, suatu hal yang tidak mungkin. Oleh karena itu himpunan bilangan tadi akan kongruen dalam modulo p dengan himpunan bilangan 1,2,..,p-1 dengan urutan tertentu.

Dengan mengalikan semua bilangan tersebut didapat:

$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$

$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$

Karena p ł (p-1)! Maka (p-1)! Dapat dicoret menghasilkan

$a^{p-1} \equiv 1 \pmod p$

Terbukti![4]

Lalu, bagaimana cara menentukan keprimaan sebuah bilangan denga teorema fermat?

Misalkan bilangan yang akan diuji adalah x. Pertama ambil sembarang bilangan bulat antara 1 sampai x-1, misalkan bilangan tersebut adalah f. Kemudian hitung $f^{x-1} \pmod x$. Jika hasilnya bukan 1, maka dipastikan bilangan x tersebut bukan bilangan prima. Jika hasilnya sama dengan 1 maka kemungkinan besar bilangan x adalah bilangan prima. Langkah ini dapat diulangi dengan mengganti nilai f dengan nilai yang lain.

Uji bilangan prima dengan teorema fermat diatas bisa dikatakan cukup mangkus dalam menentukan suatu bilangan merupakan bilangan prima atau bukan, meskipun tidak 100% benar. Bahkan tetap ada bilangan komposit yang tetap lolos uji keprimaan dengan teorema fermat ini.

Namun, bilangan komposit yang lolos itu hanya sedikit, dan bilangan komposit yang lolos uji keprimaan itu dikenal dengan istilah *pseudoprime*.

Dalam pengujian bilangan prima menggunakan teorema fermat, sangat memanfaatkan kongruen lanjar, karena teoremanya sendiri dalam bentuk kongruen lanjar.

D. Check Digit ISBN

ISBN atau *International Standard Book Number* (arti harfiah Bahasa Indonesia : Angka Standar Buku Internasional), adalah angka untuk pengidentifikasian unik untuk buku-buku yang digunakan secara komersial. Sistem ISBN diciptakan di Inggris pada tahun 1966.

ISBN diperuntukkan bagi penerbitan buku. Nomor ISBN tidak bisa digunakan secara sembarangan.

ISBN terdiri dari 10 digit nomor dengan urutan penulisan sebagai berikut

kode negara – kode penerbit – kode buku – nomor identifikasi.

Namun, mulai Januari 2007 penulisan ISBN mengalami perubahan mengikuti pola EAN, yaitu dengan menggunakan 13 digit. ISBN dengan digit yang lebih banyak ini memungkinkan penerbitan buku dengan peluang lebih banyak.

Ada sedikit perbedaan perhitungan kevalidan dari perubahan sistem ini. Namun, dalam menentukan kevalidan suatu ISBN tetap menggunakan prinsip yang sama yaitu kongruen lanjar.

- Uji ISBN 10 digit

Berikut merupakan contoh ISBN dengan standar lama berupa 10 digit.

Untuk menguji kevalidan nomor ISBN tersebut terdapat sebuah karakter uji di urutan paling akhir dari nomor ISBN tersebut.

Karakter uji adalah satu karakter terakhir dari ISBN yang digunakan untuk memvalidasi ISBN. Karakter uji dipilih sedemikian rupa sehingga memenuhi aritmatika modulo.

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$$

Suatu ISBN dikatakan valid jika :

$$(\sum_{i=1}^{9} ix_i) \bmod 11 = \text{karakter uji}$$

- Uji ISBN 13 digit

Berikut merupakan contoh ISBN dengan standar baru yaitu berupa 13 digit.

Cara perhitungan karakter uji pada ISBN 13 digit berbeda dengan dengan ISBN 10 digit. Faktor pengali untuk 12 karakter pertama ISBN tergantung pada urutan karakternya. Karakter pada urutan ganjil dikalikan dengan 1 sedangkan karakter dengan urutan genap dikalikan dengan 3.

Karakter uji dipilih sedemikian rupa sehingga memenuhi ketentuan kevalidan sebagai berikut :

$$10 - (\sum_{i=1}^{12} n.x_i) \bmod 10 = \text{karakter uji}$$

dengan x_i merupakan karakter ke i,

n = 1 untuk i ganjil

n = 3 untuk i genap

Contoh:

Kita akan menguji kevalidan nomor ISBN pada gambar diatas.

$$\sum_{i=1}^{12} n.x_i = 1.9 + 3.7 + 1.8 + 3.8 + 1.4 + 3.6 + 1.1 + 3.3 + 1.0 + 3.0 + 1.5 + 3.3 = 108$$

$$10 - (108) \bmod 10 = 10 - 8 = 2$$

Disini didapatkan karakter uji yang sesuai dengan karakter uji di ISBN tersebut, sehingga bisa dikatakan nomor ISBN tersebut valid.

Kongruen lanjar sangat membantu dalam menentukan nomor ISBN sebuah buku dan juga dalam perhitungan nomor karakter uji pada ISBN. Jika ingin membuat sebuah nomor ISBN dengan sesuai ketentuan, maka harus dicari karakter uji yang sesuai. Mencari karakter uji yang sesuai ini dengan memanfaatkan kongruen lanjar.

IV. KESIMPULAN

Dalam teori bilangan, terdapat pokok bahasan yang menarik yaitu kongruen lanjar. Kongruen lanjar memanfaatkan sifat keterbagian dan aritmatika modulo. Kongruen lanjar dimanfaatkan dalam penyelesain masalah yang berkaitan dengan hal diskrit. Kongruen lanjar memiliki berbagai macam penerapan di berbagai bidang

REFERENSI

[1] Munir, Rinaldi.*Matematika Diskrit*. Bandung. Informatika.2004.

[2] Cohen, Henri. *Number Theory, Volume I :Tools and Diophantine Equations*.Bordeaux.Institut de Mathématiques de Bordeaux.2007.

[3] Andreescu, Titu, et. al. *104 Number Theory Problem.* Dallas. University of Texas.2006.

[4] Burton, David M., *Elementary Number Theory Sixth Edition.* New York. McGraw-Hill.2007.

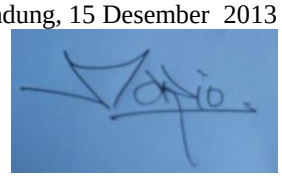
[5] http://hjaya.wordpress.com/2010/09/24/konsep-modulus-dan-kekongruenan-bilangan/. Diakses pada 14/12/2013 21.15 WIB.

[6] Rosen, Kenneth H., *Discrete Mathematics and Its Applications Sixth Edition*.New York.McGraw-Hill.2007.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 15 Desember 2013



Mario Tressa Juzar (13512016)