

Penerapan Teori Bilangan pada Permainan Tebak Umur ala *Hyakugo Gen*

Hana Fathiyah - 13520047¹

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

¹13520047@std.stei.itb.ac.id

Abstract—Matematika diskrit (*discrete mathematics*) merupakan cabang matematika yang mengkaji objek-objek diskrit. Teori bilangan merupakan salah satu bidang dalam matematika diskrit. Salah satu pembahasan dalam teori bilangan itu sendiri adalah *Chinese Remainder Theorem* atau yang biasa disingkat CRT. *Chinese Remainder Theorem* merupakan salah satu bidang yang membahas pencarian suatu bilangan berdasarkan fakta-fakta sisa hasil pembagian suatu bilangan bulat yang didasari dengan sifat keterbagian dan kongruensi. Salah satu implementasi dari *Chinese Remainder Theorem* adalah permainan tebak umur yang biasa dilakukan masyarakat Jepang atau dikenal juga dengan *Hyakugo Gen*.

Keywords—Matematika Diskrit, Teori Bilangan, *Chinese Remainder Theorem*, Bilangan Bulat, Keterbagian, Kongruensi, Tebak Umur, *Hyakugo Gen*

I. PENDAHULUAN

Matematika diskrit membahas tentang objek-objek yang bersifat diskrit. Sejumlah elemen yang bersifat berbeda dan tidak berhubungan disebut diskrit. Matematika diskrit dapat disebut sangat berkembang akhir-akhir ini karena pada dasarnya sistem komputer itu sendiri bekerja secara diskrit. Matematika diskrit juga memberi dasar perhitungan matematis dalam segala aspek di bidang informatika.

Salah satu bidang di dalam matematika diskrit adalah teori bilangan bulat. Bilangan bulat merupakan bilangan yang tidak memiliki angka pecahan desimal. Bilangan bulat memiliki sifat pembagian yang memunculkan konsep-konsep baru seperti halnya bilangan prima dan juga aritmetika modulo. Teorema yang terkenal dan penting dalam kasus pembagian bilangan bulat ini adalah teorema Euclidean. Teorema ini sudah dikenal sejak beberapa abad yang lalu. Penemunya adalah seorang matematikawan Yunani, yaitu Euclid.

Teorema Euclidean membahas tentang keterbagian yang terdiri atas pembagi (*divisor*), yang dibagi (*dividend*), hasil bagi (*quotient*), dan sisa (*remainder*). Penerapan dari teori tersebut adalah aritmetika modulo. Operator yang digunakan pada aritmetika modulo ini adalah operator mod atau yang biasa kita kenal dengan operator sisa pembagian. Di dalam aritmetika modulo itu sendiri terdapat suatu sifat yang dinamakan kongruensi. Sifat kongruen ini menyatakan sifat dua buah bilangan bulat yang memiliki sisa yang sama ketika dibagi dengan sebuah bilangan positif yang sama.

Dari sifat kongruen tersebut, terdapat juga balikan dari modulo yang kita kenal dengan inversi modulo (modulo *inverse*). Cara untuk menemukan inversi modulo dari suatu bilangan adalah dengan membuat kombinasi linier dengan angka 1. Penerapan lebih luas dari sifat kongruen ini adalah kekongruenan linier yang dapat membantu kita dalam menyelesaikan suatu persoalan dengan konsep *Chinese Remainder Theorem*.

Chinese Remainder Theorem ini ditemukan oleh seorang matematikawan China. Teorema ini digunakan untuk menemukan solusi dalam sistem kekongruenan linier. Sistem operasi yang digunakan tentunya adalah dengan memanfaatkan sifat keterbagian, sifat kekongruenan, dan juga sifat balikan sebuah modulo.

Permainan tebak umur ala *Hyakugo Gen* merupakan permainan di kalangan masyarakat Jepang. Permainan ini menerapkan ilmu matematika khususnya teori bilangan. Pada dasarnya, permainan ini memanfaatkan salah satu bahasan dari materi teori bilangan, yaitu *Chinese Remainder Theorem*.

II. LANDASAN TEORI

A. Keterbagian

Sifat dasar dari teori bilangan adalah keterbagian. Sifat pembagian (*division*) menandakan suatu bilangan habis membagi bilangan lainnya. Dalam hal ini dimisalkan dua buah bilangan a dan b merupakan bilangan bulat dengan syarat bilangan $a \neq 0$. Dapat dinyatakan bahwa bilangan a habis membagi bilangan b (a divides b) jika terdapat suatu bilangan bulat c sedemikian, sehingga $b = ac$.

Notasi untuk sifat keterbagian ditandai dengan simbol " $|$ ". Dimisalkan sebuah bilangan c merupakan bilangan bulat dan a merupakan sebuah bilangan bulat tidak nol. Dalam kasus bilangan a habis membagi bilangan b , ditandai dengan notasi sebagai berikut.

Notasi: $a | b$ jika $b = ac$, $c \in \mathbf{Z}$, $a \neq 0$

Dalam konteks keterbagian, suatu bilangan a habis membagi bilangan b dapat juga dinyatakan bahwa pembagian bilangan b dengan bilangan a menghasilkan suatu bilangan bulat. Dengan kata lain, pernyataan bilangan a habis membagi bilangan b disebut juga dengan istilah b kelipatan a . Contoh dari kasus ini adalah $3 | 21$ karena $21 \div 3 = 7$ yang merupakan bilangan bulat. Namun, 4 tidak habis membagi 21 karena $21 \div 4 = 5.25$ (bukan bilangan bulat).

Sifat keterbagian ini menghasilkan teorema lainnya, yaitu ketika suatu hasil pembagian bilangan bulat dinyatakan sebagai bilangan bulat juga. Jika sembarang bilangan bulat dibagi dengan suatu bilangan bulat positif, akan terdapat dua hal. Pertama, selalu terdapat hasil bagi. Kedua, selalu terdapat sisa pembagian. Sisa hasil pembagian selalu lebih besar dari nol, tetapi lebih kecil dari pembagi bilangan tersebut. Dalam hal ini, terdapat suatu teorema yang diciptakan oleh ilmuwan Yunani, yaitu Euclid.

Teorema ini berbunyi “misalkan sebuah bilangan m dan n adalah dua buah bilangan bulat dengan syarat $n > 0$. Jika m dibagi dengan n , terdapat dua buah bilangan bulat unik q (*quotient*) dan r (*remainder*), sehingga

$$m = nq + r$$

Teorema ini disebut teorema Euclidean. Bilangan n disebut pembagi (*divisor*), bilangan m disebut yang dibagi (*dividend*), bilangan q disebut hasil bagi (*quotient*), dan r disebut sisa (*remainder*). Operasi untuk menghasilkan hasil bagi dapat menggunakan operator *div*. Operasi untuk menghasilkan sisa bagi dapat menggunakan operator *mod*.

Selain itu, dalam hal pembagian, terdapat beberapa dalil sebagai berikut.

- Setiap bilangan bulat membagi dirinya sendiri
 $n | n$
- Prinsip *transitivity*
 $d | n$ dan $n | m \rightarrow d | m$
- Prinsip linearitas
 $d | n$ dan $d | m \rightarrow d | an + bm$ untuk setiap $a, b \in \mathbf{Z}$
- Prinsip multiplikatif
 $d | n \rightarrow ad | an$
- Prinsip pembatalan
 $ad | an \rightarrow d | n$ jika $a \neq 0$
- Angka 1 membagi setiap bilangan bulat
 $1 | n$
- Setiap bilangan bulat membagi angka 0
 $d | 0$
- Untuk setiap bilangan bulat positif d dan n berlaku sifat
 $d | n \rightarrow d \leq n$
- Kombinasi linear
 $d | n$ dan $d | m \rightarrow d | n + m$ dan $d | n - m$
merupakan kombinasi linear

B. Aritmetika Modulo

Aritmetika modulo berperan penting dalam perhitungan bilangan bulat. Operator yang digunakan pada aritmetika modulo adalah operator *mod*. Operator *mod* ini memberikan sisa hasil pembagian. Dimisalkan sebuah bilangan a adalah bilangan bulat dan m adalah bilangan bulat yang lebih besar dari nol. Operasi $a \text{ mod } m$ yang dibaca “ a modulo m ” memberikan sisa hasil pembagian ketika a dibagi dengan m . Dengan kata lain, $a \text{ mod } m = r$ sedemikian, sehingga $a = mq + r$ dengan $0 \leq r < m$. Bilangan m ini disebut dengan modulus atau modulo. Hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \dots, m - 1\}$.

Untuk pencarian bilangan bulat yang bernilai negatif, diperlukan fungsi absolut (nilai mutlak). Untuk a negatif, bagi $|a|$ dengan m untuk mendapatkan sisa sebesar r' . Setelah itu, kurangi m dengan r' untuk mendapatkan hasil $a \text{ mod } m$.

C. Kongruen

Dua buah bilangan bulat, yaitu bilangan bulat a dan bilangan bulat b terkadang mempunyai sisa yang sama ketika dibagi suatu bilangan bulat positif m . Dalam hal ini, dapat kita katakan bahwa bilangan bulat a dan bilangan bulat b kongruen dalam modulo m . Modulo ini dapat kita lambangkan sebagai berikut.

$$a \equiv b \pmod{m}$$

Operator untuk menandakan kongruen atau tidaknya dua buah bilangan dapat ditandai dengan simbol “ \equiv ” yang dibaca “kongruen”. Terdapat juga suatu kasus jika bilangan bulat a tidak mempunyai sisa pembagian yang sama dengan bilangan bulat b apabila dibagi dengan m . hal tersebut dapat dinyatakan sebagai dua buah bilangan bulat yang tidak kongruen. Simbol untuk menyatakan dua buah bilangan yang tidak kongruen adalah simbol “ $\not\equiv$ ”. Misalnya sebagai berikut.

$$a \not\equiv b \pmod{m}$$

Definisi singkat dari kongruen ini adalah dimisalkan a dan b adalah bilangan bulat, serta m adalah bilangan bulat > 0 , maka $a \equiv b \pmod{m}$ apabila m habis membagi $a - b$. Selain itu, kekongruenan $a \equiv b \pmod{m}$ dapat juga kita tuliskan dalam bentuk sebagai berikut.

$$a = b + km$$

Dalam hal ini, angka yang menjadi k merupakan bilangan bulat. Selain itu, dalam konteks aritmetika modulo, kita juga dapat menuliskan sifat kongruen ini dalam bentuk sebagai berikut.

$$a \equiv r \pmod{m}$$

Dalam kalimat sederhana, hal ini dapat dianggap bila a dibagi m akan menghasilkan sisa sebesar r . Kongruen ini tentunya memiliki sifat-sifat yang dapat digunakan dalam mengerjakan operasi hitung aritmetika modulo, khususnya pada operasi perkalian dan penjumlahan. Sifat-sifat tersebut adalah sebagai berikut.

Pertama, jika $a \equiv b \pmod{m}$, untuk setiap bilangan bulat p berlaku sifat-sifat sebagai berikut.

- $a + p \equiv b + p \pmod{m}$
- $a - p \equiv b - p \pmod{m}$
- $ap \equiv bp \pmod{m}$

Kedua, jika terdapat dua kasus modulus $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka berlaku sifat-sifat berikut.

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $ac \equiv bd \pmod{m}$

Ketiga, jika bilangan bulat a , b , c , dan m memenuhi persamaan $ca \equiv cb \pmod{m}$, serta persekutuan bilangan terbesar (*greatest common divisor*) dari keduanya adalah 1 (dalam hal ini $\text{gcd}(c, m) = 1$), maka berlaku sifat sebagai berikut.

$$a \equiv b \pmod{m}$$

Akibat dari sifat yang ketiga ini, jika $a \equiv b \pmod{m}$, maka terpenuhi sifat-sifat sebagai berikut.

- Sifat perpangkatan dengan $k > 0$
 $a^k \equiv b^k \pmod{m}$
- Sifat dalam bentuk fungsi
 $f(a) \equiv f(b) \pmod{m}$

Sifat dalam bentuk fungsi tersebut menggunakan persamaan $f(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + \dots + a_n$

Keempat, jika a , b , c , dan m adalah bilangan bulat sedemikian, sehingga $m > 0$, selisih $(c,m) = d$, dan memenuhi persamaan $ac \equiv bc \pmod{m}$, dapat kita simpulkan bahwa bilangan bulat $a \equiv b \pmod{m/d}$.

D. Inversi Modulo (Modulo *Invers*)

Pada aritmetika bilangan riil, inversi sebuah perkalian adalah pembagian. Misalnya, inversi dari 3 adalah $1/3$. Hal ini disebabkan $3 \times 1/3 = 1$. Lain halnya dengan aritmetika modulo. Di dalam aritmetika modulo, perhitungan inversi dinilai lebih rumit.

Dimisalkan dua buah bilangan a dan m yang bersifat relatif prima dan $m > 1$. Dalam hal ini, kita dapat menemukan inversi dari a modulo m . Inversi dari a modulo m adalah bilangan bulat \bar{a} sedemikian, sehingga

$$a \bar{a} \equiv 1 \pmod{m}$$

Pembuktian untuk inversi modulo ini dinilai sangat mudah. Jika diketahui bahwa a dan m relatif prima (dalam hal ini $\text{gcd}(a,m) = 1$) dan terdapat bilangan bulat p dan q , akan terbentuk persamaan sebagai berikut.

$$pa + qm = 1$$

Hal ini mengimplikasikan bahwa

$$pa + qm \equiv 1 \pmod{m}$$

Karena $qm \equiv 0 \pmod{m}$, dapat disimpulkan bahwa

$$pa \equiv 1 \pmod{m}$$

Kekongruenan akhir ini menyatakan bahwa p adalah inversi dari a modulo m .

Berdasarkan persamaan di atas, dapat disimpulkan bahwa untuk mencari suatu inversi dari a modulo m , kita dapat membuat kombinasi linier dari a dan m sama dengan 1. Koefisien a dari kombinasi linier tersebut merupakan inversi dari a modulo m .

Metode lain untuk menghitung hasil inversi modulo adalah dengan menggunakan prinsip kekongruenan. Diketahui suatu persamaan sebagai berikut.

$$a \bar{a} \equiv 1 \pmod{m}$$

Persamaan tersebut dapat ditulis di dalam hubungan sebagai berikut.

$$a \bar{a} \equiv 1 + km$$

Oleh karena itu, persoalan menemukan inversi modulo merupakan persoalan yang ekuivalen dengan persoalan menemukan \bar{a} dan k sedemikian, sehingga

$$\bar{a} = \frac{1+km}{a}$$

Selain dua cara yang telah dipaparkan di atas, terdapat metode lain yang banyak digunakan untuk mencari inversi modulo, yaitu algoritma Euclidean yang diperluas (*extended Euclidean algorithm*).

Perhitungan untuk mencari inversi suatu modulo juga dapat dilakukan dengan cara lain, yakni mengalikan koefisien x , yaitu bilangan a dengan bilangan dari 1 sampai $m - 1$. Dimisalkan m bernilai 4, maka pencarian dilakukan dengan mengalikan a dengan bilangan bulat positif dari 1 sampai $m-1$, yaitu 3. Pencarian tidak perlu dilakukan secara menyeluruh, pencarian dihentikan apabila telah berhasil ditemukan hasil dari perkalian keduanya yang menghasilkan hasil yang kongruen dengan 1 ketika dimodulus dengan m . Cara ini dinilai cukup efisien karena dapat menemukan hasil inversinya secara langsung.

Dimisalkan suatu persamaan $4 \pmod{9}$. Untuk mencari inversinya, kita perlu menghitung persamaan $4x \equiv 1 \pmod{9}$. Setelah itu, kita dapat mengalikan 4 dengan suatu bilangan. Bilangan yang dikalikan dipilih dari angka 1 hingga angka 8. Perhitungan dihentikan jika ditemukan angka yang bernilai kongruen dengan 1 jika dimodulus dengan 9.

Jika dipilih angka 1, perhitungan dilanjutkan karena diketahui bahwa $4 \cdot 1 \not\equiv 1 \pmod{9}$. Jika dipilih angka 2, perhitungan dilanjutkan karena $4 \cdot 2 \not\equiv 1 \pmod{9}$. Dilakukan terus menerus hingga bertemu angka yang kongruen. Jika dipilih angka 7, perhitungan dapat dihentikan karena $4 \cdot 7 \equiv 1 \pmod{9}$. Dengan demikian, disimpulkan bahwa $x \equiv 7 \pmod{9}$.

E. Kongruensi Linear (Kekongruenan Lanjar)

Selain sifat-sifat di atas, di dalam kongruen terdapat juga kongruensi linear. Kongruensi linear dalam satu variabel dengan x variabel bilangan bulat dinyatakan dalam bentuk sebagai berikut.

$$ax \equiv b \pmod{m}$$

Dalam hal ini, disebut juga dengan kongruensi linear satu variabel. Bentuk dari $ax \equiv b \pmod{m}$ juga ekuivalen dengan persamaan Diophantine dalam dua variabel $ax - my = b$.

Oleh karena itu, solusi dari bilangan bulat x harus memenuhi persamaan Diophantine yang bersesuaian dengan nilai y yang memenuhi.

Kongruen dengan bentuk $ax \equiv b \pmod{m}$ dapat disebut dengan kongruen linjar. Dalam hal ini, m adalah bilangan bulat positif, a dan b adalah sembarang bilangan bulat, dan x merupakan bilangan peubah. Kongruen linjar ini memiliki arti cara menentukan nilai-nilai x yang memenuhi kekongruenan tersebut.

Untuk persamaan $ax \equiv b \pmod{m}$, dapat ditulis dalam suatu hubungan sebagai berikut.

$$ax = b + km$$

Hubungan ini dapat disusun sebagai berikut.

$$x = \frac{b+km}{a}$$

Dengan k merupakan sembarang bulangan bulat. Substitusikan k dengan bilangan bulat positif, negatif atau nol.

Metode lain dalam menyelesaikan solusi suatu kekongruenan linjar adalah dengan menggunakan inversi modulo. Cara yang digunakan persis dengan bagaimana mendapatkan solusi pada persamaan linjar biasa.

Dimisalkan suatu persamaan kongruen linjar adalah sebagai berikut.

$$4x \equiv 3 \pmod{9}$$

Untuk mencari suatu hasil persamaan kongruen linjar, kalikan kedua ruas persamaan di atas dengan inversi dari 4 (mod 9). Hasil inversi dari 4 (mod 9) diketahui adalah -2. Maka dari itu, dilakukan operasi perkalian dengan -2 di kedua buah ruas.

$$-2 \cdot 4x \equiv -2 \cdot 3 \pmod{9}$$

$$-8x \equiv -6 \pmod{9}$$

Dalam hal ini, diketahui bahwa $-8 \equiv 1 \pmod{9}$, berdasarkan prinsip kekongruenan, diperoleh hasil $x \equiv -6 \pmod{9}$. Oleh karena itu, solusi dari persamaan $4x \equiv 3 \pmod{9}$ merupakan suatu bilangan bulat x , sehingga $x \equiv -6 \pmod{9}$. Bilangan-bilangan yang memenuhi kekongruenan tersebut adalah 3, 12, ..., serta -6, -15, dan seterusnya.

F. Chinese Remainder Theorem

Bentuk asli dari teorema ini, terdapat di dalam buku yang ditulis oleh ahli matematika China, Qin Jiushao dan diterbitkan pada tahun 1247. Bentuk ini merupakan suatu pertanyaan tentang kongruensi simultan. Dimisalkan n_1, \dots, n_k merupakan bilangan bulat positif yang setiap pasangannya bersifat relatif prima (artinya $\gcd(n_i, n_j) = 1$ untuk setiap $i \neq j$). Oleh karena itu, untuk setiap bilangan bulat a_1, \dots, a_k selalu ada bilangan bulat x yang merupakan penyelesaian dari sistem kongruensi simultan.

Permasalahan tersebut secara umum dikenal dengan *Chinese Remainder Theorem*. Secara pemodelan matematika, pencarian bilangan n yang dimaksud dengan pembagian sejumlah bilangan yang bernilai m_1, m_2, \dots, m_k dapat ditulis sebagai berikut.

$$\begin{aligned} n &\equiv n_1 \pmod{m_1} \\ n &\equiv n_2 \pmod{m_2} \\ &\dots \\ n &\equiv n_3 \pmod{m_3} \end{aligned}$$

Pada abad pertama, terdapat suatu matematikawan China yang bernama Sun Tse. Beliau mengajukan pertanyaan mengenai suatu bilangan bulat yang bila dibagi dengan 5 menyisakan 4, bila dibagi dengan 7 menyisakan 5 dan bila dibagi dengan 11, menyisakan 7.

Dalam menjawab pertanyaan Sun Tse ini, kita dapat menyelesaikannya dengan sistem kongruen lanjar, yaitu sebagai berikut.

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 7 \pmod{11} \end{aligned}$$

Dimisalkan m_1, m_2, \dots, m_n merupakan bilangan bulat positif sedemikian, sehingga $\gcd(m_i, m_j) = 1$ untuk $i \neq j$. Maka, sistem kongruen lanjar $x \equiv a_k \pmod{m_k}$ mempunyai sebuah solusi unik dalam modulo $m = m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Untuk penyelesaian pertanyaan Sun Tse, kita dapat mengubah persamaan $x \equiv 3 \pmod{5}$ sebagai $x = 3 + 5k_1$. Setelah itu, substitusikan nilai x terhadap persamaan yang kedua. Diperoleh persamaan $3 + 5k_1 \equiv 5 \pmod{7}$. Melalui persamaan kedua, diperoleh $5k_1 \equiv 2 \pmod{7}$, berdasarkan kekongruenan lanjar diperoleh $k_1 \equiv 6 \pmod{7}$. Dari persamaan kedua diperoleh $k_1 = 6 + 7k_2$. Kita dapat mensubstitusikan persamaan k_1 tersebut ke dalam x , sehingga diperoleh $x = 3 + 5(6 + 7k_2) = 33 + 35k_2$. Setelah itu, kita dapat mensubstitusikan kembali persamaan x yang terakhir diperoleh kepada persamaan ketiga pada soal Sun Tse. Dalam hal ini, diperoleh $33 + 35k_2 \equiv 7 \pmod{11}$. Dengan operasi pengurangan, diperoleh $35k_2 \equiv -26 \pmod{11}$. Kita bisa menghitung sisa pembagian suatu bilangan negatif dengan memutlakkannya terlebih dahulu kemudian mengurangi pembagi dengan modulus hasil mutlak bilangan negatif tersebut. Dalam hal ini, diperoleh $35k_2 \equiv 7 \pmod{11}$. Berdasarkan inversi modulus, diperoleh $k_2 \equiv 9 \pmod{11}$ yang dalam hal ini bisa ditulis dengan $k_2 = 9 + 11k_3$. Jika persamaan k_2 tersebut disubstitusikan ke dalam x diperoleh hasil $x = 33 + 35(9 + 11k_3) = 348 + 385k_3$. Dengan demikian, diperoleh $x \equiv 348 \pmod{385}$. Dengan kata lain, 348 adalah solusi unik untuk modulo 385.

Terdapat cara lain yang dinilai lebih mudah untuk menghitung persamaan menggunakan *Chinese Remainder Theorem*. Cara ini menggunakan solusi sistem kekongruenan linier. Bentuk dari sistem kekongruenan linier ini adalah sebagai berikut.

$$x = a_1M_1y_1 + a_2M_2y_2 + \dots + a_nM_ny_n$$

Dalam hal ini, M_k adalah perkalian semua modulus kecuali m_k dan y_k adalah balikan atau inversi M_k dalam modulus m_k .

Selain itu, kita dapat menghitung suatu bilangan m yang merupakan hasil perkalian seluruh pembagi bilangan. Untuk notasinya adalah sebagai berikut.

$$m = m_1 \cdot m_2 \cdot \dots \cdot m_n$$

Berdasarkan pertanyaan Sun Tse, diperoleh bilangan m sebesar $m = 5 \cdot 7 \cdot 11 = 385$.

Selanjutnya, kita dapat menghitung nilai M_1 , yaitu hasil perkalian semua pembagi kecuali pembagi pertama, yaitu 5. Diperoleh hasil $M_1 = 7 \cdot 11 = 77$. Kita juga dapat menghitung nilai M_2 , yaitu hasil perkalian semua pembagi kecuali pembagi kedua, yaitu 11. Diperoleh hasil $M_2 = 5 \cdot 11 = 55$. Terakhir, menghitung nilai M_3 yang diperoleh dari hasil perkalian semua pembagi kecuali pembagi ketiga, yaitu 11. Maka, diperoleh nilai $M_3 = 5 \cdot 7 = 35$.

Setelah itu, kita dapat mencari bilangan y_1, y_2 , dan y_3 yang merupakan balikan dari M_1, M_2 , dan M_3 terhadap pembaginya masing-masing. Proses perhitungannya adalah sebagai berikut.

$$\begin{aligned} y_1 &= 3 \text{ karena } 77 \cdot 3 \equiv 1 \pmod{5} \\ y_2 &= 6 \text{ karena } 55 \cdot 6 \equiv 1 \pmod{7} \\ y_3 &= 6 \text{ karena } 35 \cdot 6 \equiv 1 \pmod{11} \end{aligned}$$

Melalui persamaan tersebut, diperoleh suatu solusi unik dari sistem kekongruenan tersebut. Solusi unik tersebut adalah sebagai berikut.

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\ x &= 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 \\ x &= 3813 \\ x &\equiv 348 \pmod{385} \end{aligned}$$

III. APLIKASI CHINESE REMAINDER THEOREM PADA PERMAINAN TEBAK UMUR ALA *HYAKUGO GEN*

Berbicara tentang permainan tebak angka, hal ini dapat dikatakan sebagai permainan yang menarik. Permainan ini dapat dimainkan dengan jumlah pemain sebanyak dua orang atau lebih. Seperti halnya sulap atau *magic*, kita dapat dengan mudah menebak angka yang dipikirkan oleh lawan main kita hanya dengan menanyakan sisa hasil pembagian bilangan tersebut dan memanfaatkan *Chinese Remainder Theorem* di dalamnya.

Dilansir dari buku *Memahami Teori Bilangan dengan Mudah dan Menarik* karya Khoe Yao Tung, salah satu implementasi dari teori bilangan itu sendiri adalah permainan tebak umur ala *Hyakugo Gen*. Permainan ini merupakan suatu permainan matematika ala masyarakat Jepang yang dikenal dengan *Hyakugo Gen*. Sebenarnya, permainan ini adalah implementasi dari *Chinese Remainder Theorem*.

Prinsip dari permainan ini adalah keterbagian. Keterbagian yang digunakan di dalam permainan ini adalah keterbagian dengan angka 3, 5, dan 7. Pemain dapat menanyakan berapa sisa pembagian dengan 3, 5, dan 7 kepada lawan mainnya guna mendapatkan angka yang dipikirkan oleh pemain.

Permainan ini membutuhkan dua orang pemain. Cara bermainnya adalah dengan menanyakan kepada pemain lawan tiga buah pertanyaan sederhana. Daftar pertanyaan yang perlu ditanyakan adalah sebagai berikut.

- Apakah usia atau bilangan yang dipikirkan dapat dibagi dengan 3? Jika tidak, mohon disebutkan sisa hasil pembagiannya.
- Apakah usia atau bilangan yang dipikirkan dapat dibagi dengan 5? Jika tidak, mohon disebutkan sisa hasil pembagiannya.
- Apakah usia atau bilangan yang dipikirkan dapat dibagi dengan 7? Jika tidak, mohon disebutkan sisa hasil pembagiannya.

Pemain yang bertanya perlu mencatat atau mengingat sisa hasil pembagian yang telah dijawab oleh pemain lawan. Untuk menemukan bilangan yang menjadi usia atau bilangan yang dipikirkan oleh pemain lawan, diperlukan tahap-tahap sebagai berikut.

- Mengalikan sisa hasil pembagian 3 dengan angka 70.
- Mengalikan sisa hasil pembagian 5 dengan angka 21.
- Mengalikan sisa hasil pembagian 7 dengan angka 15.
- Setelah semua bilangan tersebut dihitung, jumlahkan ketiganya. Apabila jumlahnya melebihi 105, hasil akhirnya perlu dikurangi 105. Itulah umur yang dimaksud.

Dimisalkan ada dua orang pemain, yaitu A, dan B. Pemain B berusia 25 tahun. Dalam hal ini, akan ada percakapan sebagai berikut.

A: "Apakah angka usiamu dapat dibagi dengan 3? Jika tidak, sebutkan sisa hasil pembagiannya."

B: "Tidak, angka usiamu tidak dapat dibagi 3. Sisa hasil pembagiannya adalah 1."

A: "Apakah angka usiamu dapat dibagi dengan 5? Jika tidak, sebutkan sisa hasil pembagiannya."

B: "Ya, angka usiamu dapat dibagi 5."

A: "Apakah angka usiamu dapat dibagi dengan 7? Jika tidak, sebutkan sisa hasil pembagiannya."

B: "Tidak, angka usiamu tidak dapat dibagi 7. Sisa hasil pembagiannya adalah 4."

A: (Di dalam pikirannya menghitung $1 \cdot 70 + 0 \cdot 21 + 4 \cdot 15$ dan menghitung hasil pengurangannya apabila hasil lebih besar dari 105. Diperoleh hasil $70 + 60 = 130$, $130 - 105 = 25$).

A: "Usiamu adalah 25 tahun."

B: "Ya, benar."

Contoh lainnya adalah ada dua orang pemain, yaitu A dan B. Pemain B memikirkan angka 100.

A: "Apakah angka yang kamu pikirkan dapat dibagi dengan 3? Jika tidak, sebutkan sisa hasil pembagiannya."

B: "Tidak, angka yang aku pikirkan tidak dapat dibagi 3. Sisa hasil pembagiannya adalah 1."

A: "Apakah angka yang kamu pikirkan dapat dibagi dengan 5? Jika tidak, sebutkan sisa hasil pembagiannya."

B: "Ya, angka usiamu dapat dibagi 5."

A: "Apakah angka yang kamu pikirkan dapat dibagi dengan 7? Jika tidak, sebutkan sisa hasil pembagiannya."

B: "Tidak, angka usiamu tidak dapat dibagi 7. Sisa hasil pembagiannya adalah 2."

A: (Dalam pikirannya menghitung $1 \cdot 70 + 0 \cdot 21 + 2 \cdot 15$. Diperoleh hasil perhitungan sama dengan 100)

A: "Bilangan yang kamu pikirkan adalah 100."

B: "Ya, benar."

Mengapa demikian? Mengapa dengan mengalikan sisa pertama dengan 70, mengalikan sisa kedua dengan 21, dan mengalikan sisa ketiga dengan 15, lalu dikurangi dengan 105 apabila hasilnya lebih besar dari 105 akan menghasilkan angka atau usia yang dipikirkan? Hal ini berkaitan dengan pembahasan *Chinese Remainder Theorem*.

Permainan ini menggunakan metode kedua untuk mencari hasil dari persamaan dalam *Chinese Remainder Theorem*, yaitu menggunakan solusi sistem kekongruenan linier yang berbentuk sebagai berikut.

$$x = a_1M_1y_1 + a_2M_2y_2 + \dots + a_nM_ny_n$$

Pemain A menanyakan sisa hasil pembagian usia atau angka yang dipikirkan pemain B dengan 3, kemudian pemain B menyebutkan sisa hasil pembagiannya. Dalam hal ini, diperoleh nilai a_1 yang merupakan sisa hasil pembagian bilangan yang dipilih oleh pemain B dengan angka 3. Setelah itu, pemain A menanyakan sisa hasil pembagian usia atau angka yang dipikirkan pemain B dengan 5, kemudian pemain B menyebutkan sisa hasil pembagiannya. Dalam hal ini, diperoleh nilai a_2 yang merupakan sisa hasil pembagian bilangan yang dipilih oleh pemain B dengan angka 5. Terakhir, pemain A menanyakan sisa hasil pembagian usia atau angka yang dipikirkan pemain B dengan 7, kemudian pemain B menyebutkan sisa hasil pembagiannya. Dalam hal ini, diperoleh nilai a_3 yang merupakan sisa hasil pembagian bilangan yang dipilih oleh pemain B dengan angka 7.

Selanjutnya adalah proses untuk mencari masing-masing nilai M . Nilai M_1, M_2, \dots, M_n diperoleh dengan melakukan operasi perkalian antarpembiagi. Nilai M_1 diperoleh dengan mengalikan seluruh pembiagi kecuali 3, sehingga diperoleh nilai $M_1 = 5 \cdot 7 = 35$. Nilai M_2 diperoleh dengan mengalikan seluruh pembiagi kecuali 5, sehingga diperoleh nilai $M_2 = 3 \cdot 7 = 21$. Nilai M_3 diperoleh dengan mengalikan seluruh pembiagi kecuali 7, sehingga diperoleh nilai $M_3 = 3 \cdot 5 = 15$.

Proses berikutnya adalah proses untuk mendapatkan nilai y . Seperti yang telah kita ketahui, nilai y_1, y_2, \dots, y_n diperoleh dengan melakukan operasi inversi nilai M_1, M_2, \dots, M_n terhadap masing-masing pembiaginya. Perhitungannya adalah sebagai berikut.

- $y_1 = 2$ karena $35 \cdot 2 \equiv 1 \pmod{3}$
- $y_2 = 1$ karena $21 \cdot 1 \equiv 1 \pmod{5}$
- $y_3 = 1$ karena $15 \cdot 1 \equiv 1 \pmod{7}$

Sekarang, kita telah memperoleh seluruh nilai yang dibutuhkan untuk mencari bilangan yang dipikirkan pemain B. Sebelum melanjutkan ke langkah berikutnya, kita dapat menghitung nilai m yang dapat diperoleh dari perkalian seluruh pembiagi. Dalam hal ini, dapat diperoleh nilai m melalui operasi sebagai berikut.

$$m = m_1 \cdot m_2 \cdot \dots \cdot m_n$$

Karena nilai $n = 3$, maka operasi hanya dilakukan sampai m_3 saja. Maka dari itu, diperoleh nilai m sebagai berikut.

$$\begin{aligned} m &= m_1 \cdot m_2 \cdot m_3 \\ m &= 3 \cdot 5 \cdot 7 \\ m &= 105 \end{aligned}$$

Maka dari itu, diperoleh nilai m . Dapat disimpulkan bahwa semua nilai yang dibutuhkan untuk menghitung hasil operasi *Chinese Remainder Theorem* dengan metode kedua ini telah ditemukan. Setelahnya adalah memasangkan nilai-nilai yang telah ditemukan tersebut ke dalam suatu persamaan kekongruenan $x = a_1M_1y_1 + a_2M_2y_2 + \dots + a_nM_ny_n$.

Berdasarkan perhitungan yang telah kita lakukan di atas, diperoleh nilai $M_1 = 35$, $M_2 = 21$, $M_3 = 15$, $y_1 = 2$, $y_2 = 1$, $y_3 = 1$, dan $m = 105$. Selanjutnya, kita dapat mensubstitusikan angka-angka yang telah kita peroleh ke dalam persamaan kekongruenan yang telah dipaparkan di atas. Diperoleh hasil sebagai berikut.

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n.$$

Karena $n = 3$, perhitungan hanya dilakukan sampai suku ketiga saja.

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ x &= a_1 \cdot 35 \cdot 2 + a_2 \cdot 21 \cdot 1 + a_3 \cdot 15 \cdot 1 \\ x &= 70 \cdot a_1 + 21 \cdot a_2 + 15 \cdot a_3 \end{aligned}$$

Kemudian bilangan x tersebut dimodulo dengan m .

$$x \equiv (70 \cdot a_1 + 21 \cdot a_2 + 15 \cdot a_3) \pmod{105}$$

Seperti itulah pembuktian dari permainan tebak umur ala masyarakat Jepang yang dikenal dengan *Hyakugo Gen*. Sebenarnya permainan ini adalah penerapan dari *Chinese Remainder Theorem* metode kedua. Pada awalnya mungkin yang menjadi pertanyaan orang banyak adalah mengapa sisa pembagian dengan 3 harus dikali dengan 70? Mengapa sisa pembagian dengan 5 harus dikali dengan 21? Mengapa sisa pembagian dengan 7 harus dikali dengan 15? Mengapa hasil akhirnya harus dikurangi dengan 105? Hal ini sudah dapat terjawab melalui pembuktian di atas.

Sisa pembagian bilangan dengan 3 perlu dikali dengan 70 karena 70 merupakan hasil perkalian dari 5, 7, dan inversi dari perkalian keduanya terhadap modulus 3. Begitu juga dengan kasus sisa pembagian bilangan dengan 5 yang hasilnya perlu dikali dengan 21 karena 21 merupakan hasil perkalian 3, 7, dan inversi dari perkalian keduanya terhadap modulus 5. Sisa pembagian bilangan dengan 7 perlu dikali dengan 15 sebab 15 merupakan perkalian 3, 5, dan inversi dari perkalian keduanya terhadap modulus 7. Hasil akhir ketiganya apabila lebih besar dari 105 perlu dikurang dengan 105 karena pada metode kedua *Chinese Remainder Theorem* terdapat modulus dengan perkalian ketiga pembagi. Dilakukan operasi pengurangan karena asumsinya, umur yang dipikirkan tidak akan terlalu besar.

IV. KESIMPULAN

Teori bilangan merupakan salah satu cabang dari matematika diskrit. Teori ini mempelajari sifat-sifat bilangan bulat. Teori ini mengandung berbagai permasalahan terbuka yang dapat dengan mudah dimengerti. Salah satu pembahasan dalam teori bilangan ini adalah *Chinese Remainder Theorem*, yaitu suatu teori yang memanfaatkan sifat keterbagian, aritmetika modulo, kongruen, inversi modulo, dan kekongruenan linier dalam proses pengerjaannya.

Chinese Remainder Theorem dapat diselesaikan dengan dua metode berbeda, yaitu dengan metode substitusi antarpersamaan (menggunakan variabel k_1, k_2, \dots, k_n) dan metode berupa solusi sistem kekongruenan linier yang berbentuk $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n$ dengan hasil akhir berupa bilangan x yang dikongruenkan dengan bilangan m yang merupakan perkalian dari seluruh pembagi di dalam seluruh persamaan. *Chinese Remainder Theorem* ini merupakan materi yang menarik karena kita dapat menemukan suatu bilangan hanya dengan mengetahui sisa pembagiannya.

Salah satu implementasi dari *Chinese Remainder Theorem* ini adalah permainan tebak umur ala masyarakat Jepang yang dikenal dengan *Hyakugo Gen*. Dengan cara mengalikan sisa hasil pembagian 3 dengan 70, mengalikan sisa hasil pembagian 5 dengan 21, mengalikan sisa hasil pembagian 7 dengan 15, menjumlahkan seluruhnya, dan mengurangi hasil akhirnya dengan 105 apabila dihasilkan suatu bilangan yang lebih besar dari 105, akan menghasilkan umur atau angka yang dipikirkan pemain lawan. Sejatinya, operasi-operasi yang dilakukan tersebut merupakan implementasi *Chinese Remainder Theorem* menggunakan metode solusi sistem kekongruenan linier dengan persamaan $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n$ disertai dengan kongruensi bilangan x dengan modulus perkalian ketiga pembagiannya, dalam hal ini $3 \cdot 5 \cdot 7 = 105$. Secara garis besar, persamaan tersebut adalah sebagai berikut.

$$x \equiv (a_1 M_1 y_1 + \dots + a_n M_n y_n) \pmod{(m_1 \cdot \dots \cdot m_n)}$$

V. UCAPAN TERIMA KASIH

Puji dan syukur mari kita panjatkan kepada Allah SWT, Tuhan semesta alam karena atas berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan makalah ini dengan tepat waktu guna memenuhi salah satu tugas mata kuliah Matematika Diskrit tahun ajaran 2021/2022. Selain itu, penulis juga mengucapkan terima kasih sebesar-besarnya kepada Bapak Dr. Ir. Rinaldi M. T., dosen pengajar mata kuliah Matematika Diskrit, yang telah membimbing penulis dalam mengerjakan makalah ini. Semoga kebaikan Bapak dapat dibalas oleh Allah SWT dengan sebaik-baiknya balasan. Penulis juga meminta maaf apabila dalam kepenulisan makalah ini, penulis memiliki banyak kesalahan karena sejatinya penulis adalah pembelajar yang masih harus terus belajar. Semoga makalah ini dapat menjadi manfaat untuk orang banyak, tidak hanya untuk mahasiswa informatika saja, tetapi juga untuk masyarakat umum. Harapan dari penulis, makalah ini dapat meningkatkan kecintaan banyak orang terhadap ilmu matematika karena sejatinya matematika adalah ilmu yang sangat penting dalam hidup ini.

REFERENSI

- [1] K.Y. Tung. 2008. *Memahami Teori Bilangan dengan Mudah dan Menarik*. Jakarta: Kompas Gramedia.
- [2] R. Munir. 2016. *Matematika Diskrit*. Bandung: Penerbit INFORMATIKA.

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, 14 Desember 2021



Hana Fathiyah 13520047