Analisis Periode Maksimum *Linear Congruential Generator* Menggunakan Teorema Hull-Dobell untuk Generasi Nomor Virtual Account

Raihan - 13525011
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: raihan210207@gmail.com , 13525011@std.stei.itb.ac.id

***Abstrak*—*Linear Congruential Generator* (LCG) adalah metode pembangkit bilangan *pseudorandom* yang banyak digunakan karena kesederhanaan dan efisiensinya. Kualitas utama LCG ditentukan oleh panjang periodenya—jumlah elemen unik yang dihasilkan sebelum barisan berulang. Teorema Hull-Dobell menyatakan syarat perlu dan cukup agar LCG mencapai periode penuh yang sama dengan nilai modulusnya. Makalah ini menganalisis ketiga kondisi Teorema Hull-Dobell secara matematis berdasarkan konsep teori bilangan: Pembagi Bersama Terbesar (PBB), bilangan relatif prima, dan aritmetika modular. Sebagai penerapan, dirancang parameter LCG berperiode maksimum untuk membangkitkan nomor Virtual Account (VA) yang unik pada sistem pembayaran perbankan. Verifikasi dilakukan melalui eksperimen komputasi menggunakan program Python yang mengonfirmasi bahwa parameter hasil analisis teorema menghasilkan periode m secara empiris.**

Kata kunci*—*Linear Congruential Generator, Teorema Hull-Dobell, periode maksimum, teori bilangan, Virtual Account, aritmetika modular

I. PENDAHULUAN

Pembangkit bilangan *pseudorandom* (*Pseudorandom Number Generator,* PRNG) merupakan komponen penting dalam berbagai sistem komputasi modern. Aplikasinya mencakup simulasi numerik, kriptografi ringan, pengujian perangkat lunak, hingga sistem informasi perbankan. Di antara berbagai algoritma PRNG yang ada, *Linear Congruential Generator* (LCG) merupakan salah satu yang pertama dikembangkan dan masih relevan hingga saat ini. LCG pertama kali diperkenalkan oleh D. H. Lehmer pada tahun 1951 dan dianalisis secara mendalam oleh berbagai peneliti [2].

Algoritma LCG menghasilkan barisan bilangan berdasarkan relasi rekurens linier dalam aritmetika modular. Kualitasnya sangat bergantung pada pemilihan tiga parameter: modulus m, pengali a, dan *increment* c. Pemilihan parameter yang tidak tepat dapat menghasilkan periode yang jauh lebih pendek dari nilai m, sehingga barisan bilangan cepat berulang dan tidak memenuhi kebutuhan sistem.

Teorema Hull-Dobell, yang dirumuskan oleh T. E. Hull dan A. R. Dobell pada tahun 1962, menetapkan kondisi perlu dan cukup agar LCG mencapai periode penuh (*full period*) sebesar m [3]. Seluruh kondisi dalam teorema ini berakar langsung pada konsep teori bilangan: Pembagi Bersama Terbesar (PBB), bilangan relatif prima, dan kekongruenan dalam aritmetika modular.

Dalam konteks perbankan Indonesia, nomor *Virtual Account* (VA) harus bersifat unik untuk setiap transaksi dalam suatu periode. Tabrakan nomor VA (collision) dapat menyebabkan kesalahan pembayaran atau celah keamanan. Penggunaan LCG berperiode maksimum menjadi pendekatan efisien dan deterministik untuk menjamin keunikan nomor VA.

Makalah ini bertujuan untuk: (1) menganalisis cara kerja LCG berbasis aritmetika modular; (2) membuktikan dan menginterpretasikan kondisi Teorema Hull-Dobell menggunakan konsep teori bilangan; (3) merancang parameter LCG berperiode maksimum untuk generasi nomor VA; dan (4) memverifikasi hasil analisis secara komputasional.

II. LANDASAN TEORI

Bagian ini merangkum konsep-konsep teori bilangan yang menjadi fondasi analisis LCG dan Teorema Hull-Dobell, mengacu pada materi kuliah IF1220 [1].

A. Teorema Euclidean dan Aritmetika Modular

Menurut Teorema Euclidean, untuk sembarang bilangan bulat a dan bilangan bulat positif n, terdapat bilangan bulat unik q (*quotient*) dan r (*remainder*) sedemikian sehingga:

$$a = nq + r, \text{ dengan } 0 \leq r \leq n$$

Operasi sisa pembagian ini didefinisikan sebagai $a \bmod n = r$. Aritmetika modular adalah sistem perhitungan dalam himpunan $\{0, 1, 2, \ldots, m-1\}$ dengan m disebut sebagai modulus.

B. *Pembagi Bersama Terbesar*

Pembagi Bersama Terbesar (PBB) dari dua bilangan bulat a dan b, dinotasikan $PBB(a,b)$ atau $GCD(a,b)$,adalah bilangan bulat positif terbesar yang habis membagi keduanya. Algoritma Euclidean menghitung PBB berdasarkan sifat: $PBB(m,n) = PBB(n,r)$, di mana $m = nq + r$. Sebagai contoh,

$$PBB(312,70) = 312$$
$$312 = 4 \times 70 + 32$$
$$70 = 2 \times 32 + 6$$
$$32 = 5 \times 6 + 2$$
$$6 = 3 \times 2 + 0$$

Sisa pembagian terakhir sebelum 0 adalah 2, sehingga $PBB(312,70) = 2$ [1].

C. *Bilangan Relatif Prima*

Dua bilangan bulat a dan b dikatakan relatif prima jika $PBB(a,b) = 1$. Jika a dan b relatif prima, maka balikan modulo a terhadap b ada, yaitu terdapat x sedemikian sehingga $ax = 1\ (mod\ b)$ [1].

D. *Kekongruenan*

Bilangan bulat a dikatakan kongruen dengan $b\ modulo\ m$, dinotasikan $a \equiv b\ (mod\ m)$, jika dan hanya jika $m|(a-b)$. Sifat kekongruenan kompatibel dengan penjumlahan dan perkalian [1].

Jika $a \equiv b\ (mod\ m)$ dan $c \equiv d\ (mod\ m)$, maka :

$$(a+c) \equiv (b+d)\ (mod\ m)$$
$$ac \equiv bd\ (mod\ m)$$

E. *Faktorisasi Prima*

Teorema Fundamental Aritmetika menyatakan bahwa setiap bilangan bulat positif $n > 1$ dapat dinyatakan secara unik sebagai perkalian bilangan prima. Misalnya, $10^6 = 2^6 \times 5^6$ memiliki faktor prima $\{2, 5\}$. Konsep ini digunakan untuk mengidentifikasi syarat kondisi Teorema Hull-Dobell pada modulus tertentu.

III. LINEAR CONGRUENTIAL GENERATOR

A. *Definisi dan Relasi Rekurens*

LCG mendefinisikan barisan bilangan $\{X_0,\ X_1,\ X_2, \dots\}$ menggunakan relasi rekurens:

$$X_{n+1} = (a\ .X_n + c)\ mod\ m \qquad (1)$$

dengan parameter:

m = modulus $(m > 0)$

a = pengali $(0 < a < m)$

$c = increment\ (0 \le c < m)$

X_0 = *seed* awal $(0 \le X_0 < m)$

LCG dengan $c = 0$ disebut *multiplicative* LCG, sedangkan LCG dengan $c \neq 0$ disebut *mixed* LCG. Makalah ini berfokus pada *mixed* LCG karena Teorema Hull-Dobell hanya berlaku untuk kasus ini [3].

B. *Konsep Periode*

Karena LCG menghasilkan nilai dalam himpunan terbatas $\{0, 1, \dots, m-1\}$, barisan yang dihasilkan pasti berulang setelah paling banyak m langkah. Panjang barisan sebelum nilai pertama kali muncul kembali disebut periode. Periode maksimum yang mungkin adalah m, di mana setiap elemen dalam $\{0, 1, \dots, m-1\}$ muncul tepat sekali sebelum siklus berulang.

Periode yang lebih pendek dari m berarti ada nilai dalam rentang $\{0, 1, \dots, m-1\}$ yang tidak pernah dihasilkan, sehingga LCG tidak bisa memenuhi kebutuhan sistem yang mengharuskan setiap nomor muncul tepat sekali. Dalam konteks generasi nomor VA misalnya, periode pendek berarti ada nomor VA yang tidak terpakai, sedangkan nomor lain bisa muncul berulang kali, ini dapat memunculkan masalah dalam sistem perbankan.

Periode LCG tidak bergantung pada nilai *seed* X_0. Dengan kata lain, jika suatu konfigurasi (m, a, c) memenuhi ketiga kondisi Teorema Hull-Dobell, maka $periode = m$ berlaku untuk semua nilai *seed* yang mungkin.

C. *Ilustrasi Perbandingan Periode*

Perhatikan dua konfigurasi LCG dengan $m = 8$ dan $X_0 = 0$

Konfigurasi 1: $a = 5, c = 3$

Konfigurasi 2: $a = 2, c = 3$

TABEL I. PERBANDINGAN DUA KONFIGURASI LCG

Langkah n	**Konfigurasi 1: $X_{n+1} = (5X_n + 3)\ mod\ 8$**	**Konfigurasi 2: $X_{n+1} = (2X_n + 3)\ mod\ 8$**
$n = 0$	$X_0 = 0\ (seed)$	$X_0 = 0\ (seed)$
$n = 1$	$X_1 = (5 \cdot 0 + 3)\ mod\ 8 = 3$	$X_1 = (2 \cdot 0 + 3)\ mod\ 8 = 3$
$n = 2$	$X_2 = (5 \cdot 3 + 3)\ mod\ 8 = 2$	$X_2 = (2 \cdot 3 + 3)\ mod\ 8 = 1$
$n = 3$	$X_3 = (5 \cdot 2 + 3)\ mod\ 8 = 5$	$X_3 = (2 \cdot 1 + 3)\ mod\ 8 = 5$
$n = 4$	$X_4 = (5 \cdot 5 + 3)\ mod\ 8 = 4$	$X_4 = (2 \cdot 5 + 3)\ mod\ 8 = 5 \leftarrow berulang!$

$n = 5$	$X_5 = (5 \cdot 4 + 3)\ mod\ 8 = 7$	— (barisan berhenti di sini)
$n = 6$	$X_6 = (5 \cdot 7 + 3)\ mod\ 8 = 6$	—
$n = 7$	$X_7 = (5 \cdot 6 + 3)\ mod\ 8 = 1$	—
$n = 8$	$X_8 = (5 \cdot 1 + 3)\ mod\ 8 = 0 \leftarrow kembali\ ke\ X_0$	—

Tabel I memperlihatkan apa yang terjadi di tiap langkah. Konfigurasi 1 menghasilkan 8 nilai berbeda $\{3, 2, 5, 4, 7, 6, 1, 0\}$ sebelum kembali ke $X_0 = 0$ di langkah ke-8, artinya $periode = 8 = m$. Konfigurasi 2 sudah berulang di langkah ke-4 karena $X_4 = X_3 = 5$, sehingga hanya 4 nilai unik yang muncul dan periodenya hanya $3 < m$. Perbedaan ini dapat diprediksi dari awal dengan memeriksa syarat Teorema Hull-Dobell terhadap parameter yang dipilih.

IV. TEOREMA HULL-DOBELL

A. Pernyataan Teorema

Teorema Hull-Dobell [3]. *Mixed* LCG dengan parameter m, a, c, dan seed X_0 sembarang akan menghasilkan periode penuh (periode = m) jika dan hanya jika tiga kondisi berikut terpenuhi secara bersamaan:

Kondisi 1: $PBB(c, m) = 1$ (c dan m relatif prima)

Kondisi 2: Untuk setiap faktor prima p dari m berlaku: $p|(a-1)$, atau $(a-1) \equiv 0\ (mod\ p)$

Kondisi 3: Jika $4|m$, maka $4|(a-1)$, atau $(a-1) \equiv 0\ (mod\ 4)$

B. Analisis Kondisi 1: $PBB(c, m) = 1$

Kondisi pertama mensyaratkan c dan m harus relatif prima. Dengan mengekspansi relasi rekurens LCG secara berulang mulai dari seed X_0, dapat ditunjukkan bahwa jika $PBB(c, m) = d > 1$, maka suku yang mengandung c selalu merupakan kelipatan d. Jika $X_0 = 0$, semua nilai X_n menjadi kelipatan d, sehingga nilai yang bukan kelipatan d tidak pernah muncul. Ini berarti $periode < m$, kontradiksi dengan asumsi periode penuh.

C. Analisis Kondisi 2: $p|(a-1)$ untuk setiap faktor prima p

Kondisi ini berkaitan dengan sifat pengali a dalam aritmetika modular. Misalkan p Adalah faktor prima dari m. Jika $a \not\equiv 1\ (mod\ p)$, maka a memiliki orde multiplikatif yang lebih kecil dari $p-1$ dalam Z_p. Akibatnya, barisan $X_n\ mod\ p$ bersiklus dengan periode yang lebih kecil dari p, sehingga tidak semua residu modulo p dapat dijangkau, dan periode LCG tidak penuh.

D. Analisis Kondisi 3: Jika $4|m$, maka $4|(a-1)$

Kondisi ini merupakan syarat tambahan khusus untuk modulus yang habis dibagi 4. Ketika m memiliki 4 sebagai faktor, bilangan prima 2 muncul dengan pangkat ≥ 2 dalam faktorisasi m. Kondisi 2 hanya mensyaratkan $2|(a-1)$, tetapi ini tidak cukup untuk mengatur distribusi nilai pada kelas residu modulo 4. Diperlukan $4|(a-1)$ agar barisan menjangkau semua elemen ruang keluaran [3].

E. Verifikasi

Tabel I adalah verifikasi Teorema Hull-Dobell pada dua konfigurasi berbeda dengan m = 8.

TABEL II. VERIFIKASI TEOREMA HULL-DOBELL (m = 8)

Kondisi	**Konfigurasi 1 ($a = 5, c = 3$)**	**Konfigurasi 2 ($a = 2, c = 3$)**
$PBB(c, m) = 1$	$PBB(3,8) = 1$ ✓	$PBB(3,8) = 1$ ✓
$p\|(a-1), p = 2$	$2\|4$ ✓	$2\|1$ ✗
$4\|m \rightarrow 4\|(a-1)$	$4\|4$ ✓	—
Periode	= 8 (maksimum)	$= 3 < m$

V. APLIKASI PADA GENERASI NOMOR VIRTUAL ACCOUNT

A. Konteks dan Persyaratan

Virtual Account (VA) adalah mekanisme pembayaran perbankan di mana setiap transaksi memiliki nomor tujuan unik yang dibuat secara dinamis. Nomor VA umumnya terdiri dari kode bank (3-4 digit), kode *merchant* (4-6 digit), dan sufiks unik (4-8 digit). Sufiks unik inilah yang perlu dibangkitkan secara otomatis dan tidak boleh berulang dalam satu sesi atau satu hari operasional.

Persyaratan untuk sufiks unik VA: (1) tidak boleh berulang dalam satu periode; (2) dibangkitkan secara deterministik dan cepat; (3) menjangkau seluruh ruang k-digit. LCG berperiode maksimum memenuhi persyaratan (1) dan (2). Untuk (3), meskipun LCG bukan generator kriptografis, dalam konteks VA yang mengutamakan keunikan, LCG sudah memadai [4].

B. Perancangan Parameter dengan Teorema Hull-Dobell

Dirancang LCG untuk membangkitkan sufiks unik 6 digit (000000–999999). Dipilih modulus $m = 10^6 = 1.000.000$.

Langkah 1: Faktorisasi m: $10^6 = 2^6 \times 5^6 \rightarrow$ faktor prima: {2, 5}

Langkah 2: Menentukan a: $(a-1)$ harus habis dibagi 2, 5, dan 4 (karena $4 \mid 10^6$).

Syarat gabungan: $(a-1)$ habis dibagi $KPK(4,5) = 20$, sehingga $a \equiv 1 \pmod{20}$. Dipilih $a = 40001$.

Verifikasi: $40001 - 1 = 40000 = 2^6 \times 5^4 \rightarrow 2|40000, 5|40000, 4|40000$.

Langkah 3: Menentukan c: Dipilih $c = 1$. $PBB(1, 10^6) = 1$

TABEL III. VERIFIKASI HULL-DOBELL UNTUK PARAMETER VA ($m = 10^6, a = 40001, c = 1$)

Kondisi	Nilai	Status
$PBB(c,m) = PBB(1,10^6)$	= 1	✓
$2 \mid (a-1) = 2 \mid 40000$	ya	✓
$5 \mid (a-1) = 5 \mid 40000$	ya	✓
$4 \mid m$ *dan* $4 \mid (a-1)$	$4 \mid 10^6$ *dan* $4 \mid 40000$	✓

Semua kondisi terpenuhi $\rightarrow$ $periode = 10^6 =$ 1.000.000 (dijamin Teorema Hull-Dobell).

C. *Contoh Pembangkitan Nomor VA*

Dengan $X_0 = 12345$:

$$X_1 = (40001 \times 12345 + 1) \bmod 10^6 = 812346$$

$$X_2 = (40001 \times 812346 + 1) \bmod 10^6 = 652347$$

$$X_3 = (40001 \times 652347 + 1) \bmod 10^6 = 494348$$

Nomor VA yang dihasilkan (kode bank BCA = 014, kode *merchant* = 88880):

Transaksi 1: 014-88880-812346

Transaksi 2: 014-88880-652347

Transaksi 3: 014-88880-494348

Semua nomor berbeda dan tidak akan berulang hingga transaksi ke-1000001.

VI. IMPLEMENTASI DAN EKSPERIMEN

Program berikut ditulis dalam Python untuk mengimplementasikan LCG sekaligus memverifikasi ketiga kondisi Teorema Hull-Dobell secara otomatis. Program ini juga menjalankan uji empiris untuk membuktikan bahwa nilai periode sama dengan m.

```python
from math import gcd
def prime_factors(n):
    factors, d = set(), 2
    while d * d <= n:
        while n % d == 0: factors.add(d); n //= d
        d += 1
    if n > 1: factors.add(n)
    return factors
```

Fig. 1. Fungsi Pencari Faktor Prima

Fig. 1. menampilkan fungsi prime_factors(n) yang mengembalikan himpunan semua faktor prima dari bilangan bulat n.

Cara kerjanya: mulai dari d=2, jika n habis dibagi d, maka d masuk himpunan dan n dibagi terus dengan d hingga tidak bisa lagi, lalu d dinaikkan. Jika setelah loop selesai n masih lebih dari 1, nilai n itu sendiri adalah faktor prima. Fungsi ini dibutuhkan untuk memeriksa Kondisi 2 Teorema Hull-Dobell.

Fungsi mengembalikan himpunan (*set*), bukan *list*, sehingga setiap faktor prima hanya muncul sekali meski ia membagi n berkali-kali. Untuk $n = 10^6 = 2^6 \times 5^6$, fungsi mengembalikan {2, 5}. Ini sesuai dengan kebutuhan Kondisi 2 yang mensyaratkan pengecekan faktor prima unik, bukan kemunculannya dalam faktorisasi.

```python
def verify_hull_dobell(a, c, m):
    if gcd(c, m) != 1: return False, "Kondisi 1 GAGAL"
    for p in prime_factors(m):
        if (a-1) % p != 0: return False, f"Kondisi 2 GAGAL: p={p}"
    if m % 4 == 0 and (a-1) % 4 != 0: return False, "Kondisi 3 GAGAL"
    return True, "Semua kondisi Hull-Dobell TERPENUHI"
```

Fig. 2. Fungsi Verifikasi Teorema Hull-Dobell

Fig. 2. menampilkan fungsi verify_hull_dobell(a, c, m) yang memeriksa apakah ketiga kondisi Teorema Hull-Dobell terpenuhi. Baris pertama mengecek Kondisi 1: gcd(c,m) harus sama dengan 1. Blok for mengecek Kondisi 2: untuk setiap faktor prima p dari m, (a-1) harus habis dibagi p. Baris terakhir mengecek Kondisi 3: jika 4|m, maka 4 harus membagi (a-1). Jika semua kondisi lolos, fungsi mengembalikan True beserta pesan konfirmasi. Fungsi berhenti saat kondisi pertama yang gagal ditemukan beserta pesan kondisi apa yang gagal.

```python
def lcg(seed, a, c, m, n):
    x, results = seed, []
    for _ in range(n): x = (a*x+c)%m; results.append(x)
    return results
```

Fig. 3. Implementasi Fungsi LCG

Fig. 3. menampilkan fungsi lcg(seed, a, c, m, n) yang membangkitkan barisan *pseudorandom* dengan relasi $X_{n+1} = (a \cdot X_n + c) \bmod m$.

```python
# Pengujian untuk generasi nomor VA
m, a, c, seed = 1_000_000, 40001, 1, 12345
print(verify_hull_dobell(a, c, m))
barisan = lcg(seed, a, c, m, m)
print(len(set(barisan)))
```

Fig. 4. Kode Utama Untuk Pengujian Pembangkitan Nomor VA

Fig. 4. adalah kode program utama untuk pengujian pembangkitan nomor VA. Output yang diharapkan adalah "(true, 'Semua kondisi Hull-Dobell TERPENUHI')" dan "1000000".

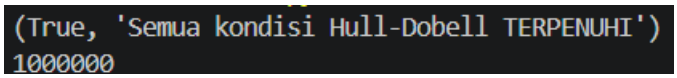


Fig. 5. Output Program Pada Terminal

Output tersebut mengonfirmasi bahwa dari $m = 1000000$ iterasi, tepat 1000000 nilai unik dihasilkan, ini membuktikan secara empiris $periode = m$ sesuai prediksi Teorema Hull-Dobell.

Sebagai pengujian pembanding, parameter yang melanggar kondisi 1 sengaja dicoba dengan $a = 40000, c = 2, m = 10^6$. Karena $PBB(2, 10^6) = 2 \neq 1$, hanya 500000 nilai unik yang dihasilkan, setengah dari nilai m. Ini membuktikan bahwa melanggar salah satu saja kondisi pada Teorema Hull-Dobell dapat berdampak langsung pada panjang periode.

VII. PEMBAHASAN

Hasil analisis dan eksperimen menunjukkan bahwa Teorema Hull-Dobell merupakan alat yang presisi dalam menentukan konfigurasi LCG berperiode maksimum. Fondasi matematis ketiga kondisi teorema berasal dari konsep PBB, relatif prima, dan kekongruenan: kondisi pertama memastikan *increment* c tidak membatasi jangkauan nilai; kondisi kedua mencegah siklus prematur dalam subgroup modular; kondisi ketiga menangani kasus khusus aritmetika bilangan genap.

Untuk konteks VA perbankan, solusi yang dirancang ($m = 10^6, a = 40001, c = 1$) menjamin tidak ada *collision* dalam 1 juta transaksi pertama. Jika *seed* diperbarui setiap hari menggunakan *timestamp*, keunikan terjaga tanpa perlu menyimpan *database* nomor yang sudah digunakan.

Keterbatasan LCG: LCG memiliki struktur korelasi linier yang dapat dideteksi secara statistik [2]. Untuk kebutuhan yang menuntut keamanan kriptografis (seperti token OTP), diperlukan PRNG yang lebih kuat. Namun untuk generasi nomor VA yang mengutamakan keunikan dan efisiensi, LCG berperiode maksimum adalah pilihan yang tepat.

Dari sisi pemilihan *seed*, nilai *seed* yang baik juga mempengaruhi keunikan nomor VA. Jika seed yang sama dipakai setiap hari, pola nomor akan berulang persis. Solusi praktisnya adalah mengombinasikan *Unix timestamp* dengan *ID merchant* sebagai *seed*, misalnya $seed = (timestamp + id\_merchant) \bmod m$. Dengan cara ini, pihak yang mengetahui a, c, m sekalipun tidak dapat memprediksi nomor VA yang dihasilkan hari ini tanpa mengetahui *seed* yang digunakan.

VIII. KESIMPULAN

Makalah ini telah menganalisis secara menyeluruh kondisi-kondisi Teorema Hull-Dobell untuk pencapaian periode maksimum pada LCG berdasarkan teori bilangan. Dapat disimpulkan beberapa hal berikut.

Pertama, LCG menghasilkan periode penuh sebesar m jika dan hanya jika: *increment* c relatif prima dengan m; pengali a memenuhi $(a-1) \equiv 0 \ (mod\ p)$ untuk setiap faktor prima p dari m; dan jika $4|m$ maka $(a-1) \equiv 0 \ (mod\ 4)$. Ketiga kondisi ini bersifat kumulatif, kegagalan satu kondisi saja dapat mengakibatkan periode tidak penuh.

Kedua, fondasi ketiga kondisi ini adalah konsep PBB, relatif prima, dan kekongruenan dalam aritmetika modular.

Ketiga, untuk generasi nomor VA 6-digit, parameter $m = 10^6, a = 40001, c = 1$ terbukti secara analitis dan empiris menghasilkan periode penuh 1000000, cukup untuk menjamin keunikan nomor VA dalam operasional sehari-hari sistem perbankan Indonesia.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas kelancaran yang diberikan selama proses pengerjaan makalah sehingga penulis dapat menyelesaikan makalah yang berjudul "Analisis Periode Maksimum *Linear Congruential Generator* Menggunakan Teorema Hull-Dobell untuk Generasi Nomor Virtual Account" tepat pada waktunya. Tak lupa juga penulis mengucapkan terima kasih kepada Bapak Rinaldi Munir selaku dosen pengampu IF1220 Matematika Diskrit atas bimbingan dan pengajaran yang telah dilakukan di kelas Matematika Diskrit serta sumber materi perkuliahan teori bilangan yang ada situs web beliau yang menjadi landasan teori untuk analisis dalam makalah ini. Penulis juga mengapresiasi berbagai sumber bacaan dan referensi yang telah memperkaya pengetahuan penulis untuk menyusun makalah ini. Terakhir, penulis mengucapkan terima kasih kepada orang tua, keluarga, dan seluruh pihak yang membantu penulis dalam menyelesaikan makalah ini. Penulis berharap makalah ini dapat memberikan manfaat dan dapat dijadikan referensi baik bagi orang lain atau bagi penulis kedepannya.

REFERENSI

[1] [1] R. Munir, "Teori Bilangan (Bagian 1)," Bahan Kuliah IF1220 Matematika Diskrit, Institut Teknologi Bandung, 2026. [Online]. Tersedia: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2025-2026/. [Diakses: 18 Juni 2026].

[2] [2] D. E. Knuth, The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, 3rd ed. Reading, MA: Addison-Wesley, 1997, pp. 10–26.

[3] [3] T. E. Hull dan A. R. Dobell, "Random Number Generators," SIAM Review, vol. 4, no. 3, pp. 230–254, Jul. 1962.

[4] [4] P. L'Ecuyer, "Good Parameters and Implementations for Combined Multiple Recursive Random Number Generators," Operations Research, vol. 47, no. 1, pp. 159–164, 1999.

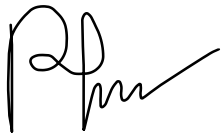
[5] [5] W. H. Press, S. A. Teukolsky, W. T. Vetterling, dan B. P. Flannery, Numerical Recipes: The Art of Scientific Computing, 3rd ed. Cambridge, UK: Cambridge University Press, 2007, pp. 340–360.

[6] [6] Bank Indonesia, "Pedoman Teknis Implementasi Virtual Account dalam Sistem Pembayaran Ritel," Jakarta, 2022. [Online]. Tersedia: https://www.bi.go.id. [Diakses: 18 Juni 2026].

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, 19 Juni 2026



Raihan - 13525011