BAB II

TEORI BILANGAN

Dalam bab II akan dibahas mengenai teori bilangan yang meliputi bilangan prima, bilangan komposit, algoritma pembagian, kesamaan bilangan bulat, pembagi bersama terbesar, bilangan bulat prima relatif dan metode pembangkitan bilangan random linier congruential generators yang mempunyai peranan sangat penting dalam aplikasi algoritma Monte Carlo, karena dengan berdasarkan hal tersebut diatas penggunaan bilangan random sebagai sampling buatan dalam aplikasi algoritma Monte Carlo.

2.1. Bilangan Prima Dan Komposit

Teori bilangan mempunyai banyak aplikasi, khususnya pada ilmu komputer yang merupakan bagian dari matematik diskret. Diasumsikan bilangan bilangan bulat Z = { . . . , -3 , -2, -1, 0 , 1 , 2 , 3 , . . . }.

Sifat 2.1

Diberikan a sebarang bilangan bulat (positif, negatif, atau nol). Diberikan X adalah himpunan semua bilangan bulat x dengan $x \geq a$. Maka setiap himpunan bagian tidak kosong S pada X mempunyai bilangan bulat terkecil.

Definisi 2.1 (Prima di Z)

Sebuah bilangan bulat p yaitu bukan { 1, -1 } dan hanya mempunyai faktorisasi trivial p = p . 1 = (-p) (-1) disebut prima di Z.

Berdasarkan definisi tersebut maka sebuah bilangan bulat p disebut prima jika dan hanya jika p tidak mempunyai timbal balik di Z dan sebarang persamaan p = b c, dengan b dan c adalah bilangan bulat, berimplikasi bahwa b dan c keduanya dalam himpunan { -p, -1, 1 , p }. Contoh 10 bilangan prima pertama dalam Z :

2, 3, 5, 7, 11, 13, 17, 19, 23 dan 29.

Definisi 2.2 (Komposit pada Z)

Sebuah bilangan bulat tidak nol yang mempunyai sebuah faktorisasi nontrivial disebut bilangan bulat komposit.

Contoh : 15 adalah komposit karena 15 $\neq$ 0 dan 15 = 5 . 3 adalah sebuah faktorisasi nontrivial. Bilangan bulat komposit lainnya adalah $\pm$4, $\pm$6, $\pm$8, $\pm$9, $\pm$10, $\pm$12 dan $\pm$14. Dicatat bahwa 0, 1, -1 adalah bukan prima dan juga bukan komposit.

2.2. Algoritma Pembagian

Perkalian pada bilangan bulat positif adalah sebuah bentuk penjumlahan, sebagai ilustrasi 4 . 5 mungkin dapat digambarkan sebagai :

5 + 5 + 5 + 5 atau 4 + 4 + 4 + 4 + 4.

Secara sama, pembagian pada bilangan bulat positif dapat diselesaikan dengan mengulang pengurangan. Jadi satu tes apakah 8 adalah sebuah bilangan bulat pembagi pada 48 atau bukan, dilakukan dengan berkali - kali mengurangi dengan 8 dan dilihat apakah 0 dihasilkan setelah beberapa langkah. Dalam kasus ini, 0 dihasilkan setelah 6 kali pengurangan 8 dari 48, karena $48 = 6 . 8$ dan $8 | 48$.

Jika dimulai dengan 53 dari 48, sebuah sisa positif yaitu kurang dari 8 dicapai setelah 6 kali pengurangan 8, dan diperoleh bahwa $53 = 6 . 8 + 5$. Selanjutnya jika dikurangi lagi dengan 8 akan diperoleh hasil negatif, bukan 0. Oleh karena itu 8 bukan pembagi 53 dalam Z.

Teorema 2.1 (Algoritma Pembagian)

Jika a dan b bilangan bulat dan b adalah positif, ada bilangan bulat q dan r sedemikian sehingga:

$a = q\,b + r, \quad 0 \leq r < b.$

Juga, $b \mid a$ jika dan hanya jika $r = 0$. (q adalah quotient dan r adalah sisa pembagian a dengan b).

Bukti :

Diberikan N himpunan { 0, 1 , 2 , . . . } dari bilangan bulat non negatif. Diberikan S himpunan bagian N dari semua bilangan bulat non negatif yang dapat diekspresikan dalam bentuk a - qb, dengan q bilangan bulat. Selanjutnya diperlihatkan bahwa himpunan S tidak kosong karena b bilangan bulat positif, maka $b \geq 1$, dan

$|a| . b \geq |a| . 1 = |a| \geq -a$, yaitu

$|a| . b \geq - a$.

Dengan mengikutinya maka: $a + |a| . b \geq a - a = 0$, dan karenanya :

$a - (- |a|) b \geq 0$.

Pertidaksamaan tersebut menggambarkan bahwa satu harga q, yang mana a - qb dalam S, yaitu $q = - |a|$; sehingga S tidak kosong. Kemudian berdasarkan sifat 2.1 himpunan tidak kosong S mempunyai paling sedikit sebuah bilangan bulat r. Berhubungan dengan ini r adalah sebuah bilangan bulat q sedemikian sehingga a-qb=r.

Dengan definisi S, paling sedikit bilangan bulat r memenuhi $0 \leq r$. Terlihat bahwa r juga memenuhi $r < b$ dengan asumsi $r \geq b$ dan menghasilkan kontradiksi. Diberikan $r' = r - b$ dan $q' = q + 1$. Jika $r \geq b$, maka $r' \geq 0$ dan

$r' = r - b = (a - qb) - b = a - (q + 1) b = a - q' b$.

$r' \geq 0$ dan $r' = a - q' b$ termasuk bahwa r' dalam S. Karena $r' = r - b < r$, kontradiksi ini menyatakan bahwa r adalah bilangan bulat terkecil dalam S.

Karena itu $r < b$ yaitu $0 \leq r < b$.

Selanjutnya dibuktikan bahwa r dan q adalah tunggal. Dimulai dengan mengasumsikan bahwa $a = qb + r = q_1 b + r_1$, $0 \leq r < b$, $0 \leq r_1 < b$.

Diasumsikan bahwa $r \geq r_1$. Maka :

$0 \leq r - r_1 < b$

$r - r_1 = (q_1 - q) b$ (1)

Karena tidak ada perkalian pada b antara 0 dan b. Berdasarkan (1) yaitu $r - r_1 = 0$.

Maka $r = r_1$

$qb = q_1 b$ dan akhirnya $q = q_1$, karena $b \neq 0$. Jadi r dan q secara tunggal ditentukan dengan a dan b.

Jika $r = 0$, maka $a = qb + r = qb$, dan dipunyai $b \mid a$. Sebaliknya, jika $b \mid a$, maka ada bilangan bulat m sedemikian sehingga $a = mb$, dan karena itu q dan r adalah berturut - turut m dan 0. Terlihat bahwa $b \mid a$ jika dan hanya jika $r = 0$.

Terbukti. ■

Akibat teorema 2.1 (Extended Division Algorithm / Perluasan Algoritma Pembagian)

Jika a dan c dalam Z dan $c \neq 0$, maka ada q dan r dalam Z sedemikian hingga :

$$a = qc + r \text{ dan } 0 \leq r < | c |.$$

Akibat ini dibuktikan dengan mengambil $b = | c |$ dan kemudian pemakaian

teorema. Diberikan m sebuah bilangan bulat positif tetap. Maka teorema 2.1 (teorema pembagian) menyatakan bahwa setiap bilangan bulat a adalah satu bentuk pada

qm, qm + 1, qm + 2, . . . , qm + (m - 1), dengan q bilangan bulat, yaitu setiap bilangan bulat tepat satu pada himpunan - himpunan

mZ, 1 + mZ, 2 + mZ, . . . , (m - 1) + mZ.

Jika m = 2, statemen ini menjadi pernyataan yang sudah lazim bahwa setiap bilangan bulat dalam himpunan 2Z={ . . . , -4, -2, 0, 2 , 4, . . . }pada bilangan bulat genap atau dalam himpunan 1 + 2Z = { . . . , -3 , - 1 , 1 , 3, 5, . . . } pada bilangan bulat ganjil, tetapi tidak dalam keduanya. Dengan m = 3, diperoleh pernyataan bahwa setiap bilangan bulat secara tepat terdapat dalam satu dari himpunan - himpunan 3Z, 1 + 3Z, 2 + 3Z.

Definisi 2.3 (Kesamaan Bilangan Bulat)

Diberikan a dan c bilangan bulat. Maka a dan c mempunyai kesamaan jika keduanya genap atau keduanya ganjil. Jika satu dari bilangan bulat ini genap dan lainnya ganjil, maka dikatakan mempunyai kesamaan yang berlawanan *(opposite parity).*

Jadi 15 dan 17 mempunyai kesamaan karena keduanya ganjil. Demikian juga -4 dan 6 mempunyai kesamaan karena keduanya genap. Tetapi 6 dan 15

mempunyai kesamaan yang berlawanan.

Notasi 1 (Congruence Module m)

Diberikan a, c dan m bilangan bulat dengan m positif. Maka notasi $a \equiv c \pmod{m}$ mempunyai arti bahwa a dan c mempunyai sisa yang sama jika dibagi dengan m. " $a \equiv c \pmod{m}$ " dibaca sebagai a kongruen dengan c modulo m. Hubungan ini disebut kongruen dan m disebut modulus pada kongruen.

Contoh :

Persamaan $28 = 5.5. + 3$ dan $73 = 14 . 5 + 3$, terlihat bahwa 28 dan 73 mempunyai sisa yang sama jika dibagi dengan 5, sehingga $28 \equiv 73 \pmod{5}$. Setiap 28 dan 73 dalam $3 + 5Z$.

Teorema 2.2 (Two ways of showing equal remainders)

Diberikan a, c dan m bilangan bulat dengan m positif. Maka $a \equiv c \pmod{m}$ jika dan hanya jika $m \mid (a - c)$.

Bukti :

Dibuktikan 2 bentuk dibawah ini :

(i) Jika $a \equiv c \pmod{m}$, maka $m \mid (a - c)$

(ii) Jika $m \mid (a - c)$, maka $a \equiv c \pmod{m}$

Untuk kedua bagian ini, dengan algoritma pembagian bahwa $a = qm + r$ dan $c = q' m + r'$ dengan q, r, q' dan r' dalam Z, $0 \leq r < m$ dan $0 \leq r' < m$.

(i) $\Rightarrow$

Diberikan $a \equiv c \pmod m$. Berdasarkan definisi kongruen, mempunyai arti bahwa $r = r'$, sehingga diperoleh :

$$a - c = (qm + r) - (q'm + r') = (q - q') m.$$

Oleh karena itu, $m \mid (a - c)$. Terbukti. ■

(ii) $\Leftarrow$

Diberikan $m \mid (a - c)$, yaitu $a - c = tm$ dengan t dalam Z, maka

$tm = a - c = (qm + r) - (q'm + r') = (q - q') m + (r - r')$, sehingga

$r - r' = (t - q + q') m$, artinya bahwa $r - r'$ adalah sebuah perkalian bilangan bulat pada m. Tetapi r dan r' dalam $\{ -(m - 1), -(m - 2), \ldots, 0, \ldots, m - 2, m - 1 \}$.

Karena perkalian bilangan bulat hanya pada m dalam himpunan ini adalah 0, terlihat bahwa $r - r' = 0$

Akhirnya $r = r'$ yang berimplikasi bahwa $a \equiv c \pmod m$. Terbukti. ■

Teorema 2.3 (Closure under substraction)

Diberikan S sebuah hinpunan bilangan bulat tertutup dibawah pengurangan,

maka:

(a) Jika S tidak kosong, 0 dalam S

(b) Jika a dalam S, -a juga dalam S

(c) Jika a dan b dalam S dan q adalah sebuah bilangan bulat, a - qb dalam S

(d) S terdiri atas semua perkalian bilangan bulat pada beberapa t dalam Z atau S adalah kosong

(e) Jika ada bilangan bulat tidak nol terkecil dalam S, maka S terdiri atas semua perkalian pada bilangan bulat positif terkecil dalam S, yaitu S = tZ.

Bukti :

Jika S tidak kosong, ada sebuah bilangan bulat a dalam S, dan a - a = 0 dalam S dengan *closure under substraction*. Maka 0 - a = - a dalam S. Sehingga (a) dan (b) terbukti. ■

Diberikan a dan b dalam S. Maka a - qb adalah hasil pengurangan qb dari a (jika q positif) atau pengurangan -b pada -q kali (jika q negatif). Dalam tiap kasus, a - qb dalam S dengan *closure under substraction.* Terbukti ■

Jika S adalah himpunan dengan elemen tunggal { 0 }, S atas semua perkalian bilangan bulat pada 0. Karena itu dianggap ada elemen c tidak nol dalam S. Maka satu pada c atau -c adalah positif dalam S. Himpunan bagian T pada bilangan bulat positif dalam S adalah sebuah himpunan nonnegatif, dan berdasarkan sifat 2.1 maka T mempunyai sebuah bilangan bulat terkecil t.

Diberikan a sebarang bilangan bulat dalam S. Algoritma pembagian memberikan bilangan bulat q dan r sedemikian hingga :

$a = qt + r , 0 \leq r < t.$

Maka r = a - qt dalam S berdasarkan (c). Karena r lebih kecil dari bilangan bulat positif terkecil t dalam S, maka r bukan positif, karena $0 \leq r$ maka r = 0. Karena itu a = qt, yaitu setiap a dalam S adalah sebuah perkalian bilangan bulat qt pada bilangan bulat positif terkecil t dalam S, maka a = 0 = 0 - (-q)t dalam S berdasarkan (a) dan (c), karena itu S adalah himpunan tZ pada semua perkalian bilangan bulat pada t. Terbukti. ■

2.3. Pembagi Bersama

Diberikan a dan b bilangan bulat nonnegatif. Sebuah pembagi bilangan bulat bersama t pada a dan b, yaitu sebuah bilangan bulat t sedemikian bahwa $t|a$ dan $t|b$ memenuhi ketidaksamaan :

$-|a| \leq t \leq |a|$

$-|b| \leq t \leq |b|.$

Karena itu himpunan T pada pembagi bilangan bulat bersama adalah finite. Karena 1 dalam T, ada satu bilangan bulat positif terkecil dalam T. Dengan mengikuti dari dua pernyataan terakhir bahwa ada bilangan bulat positif terbesar dalam T. Jika c adalah sebuah bilangan bulat tidak nol, bilangan bulat positif

terbesar d sedemikian sehingga d|c dan d|0 adalah d = | c |.

Definisi 2.4 (Pembagi bersama terbesar)

Diberikan a dan b bilangan bulat,keduanya tidak nol. Diberikikan bilangn bulat positif terbesar d sedemikian sehingga d|a dan d|b disebut pembagi bersama terbesar (gcd) pada a dan b dan dinotasikan dengan gcd(a,b). Juga diberikan gcd(0,0) = 0.

Himpunan pembagi bilangan bulat positif 10 adalah A ={1,2,5,10} dan himpunan pembagi bilangan bulat positif 12 adalah B={1,2,3,4,6,12}. Himpunan pembagi bilangan bulat positif bersama 10 dan 12 adalah :

$$C = A \cap B = \{ 1, 2 \}$$

dan karena itu gcd(10 , 12) = 2.

Contoh lain adalah : gcd(15 ,6) = 3, gcd(26, -10)=2.

Definisi 2.5 (Bilangan Bulat Prima Relatif)

Jika gcd(r , s) = 1, bilangan bulat r dan s adalah prima relatif atau coprima.

Contoh :

22 dan -15 adalah prima relatif , karena gcd(22 , -15) = 1, demikian juga 7 dan 24 adalah prima relatif meskipun satu atau setiap r dan s komposit. Contoh gcd(17, 51) = 17 dan gcd(19, -19) = 19 memperlihatkan bahwa r dan s tidak

perlu prima relatif walaupun satu atau setiap r dan s adalah prima.

2.4. Linier Congruential Generators

Sebagian besar pembangkitan bilangan random yang digunakan adalah *Linier Congruential Generators (LCGs)*. Sebuah barisan bilangan bulat Z_1 , Z_2 , . . . didefinisikan dengan formula rekursif :

$$Z_i = (a Z_{i-1} + c) (\text{mod } m) \qquad (2 - 1)$$

dimana m adalah modulus , a pengali , c pertambahan dan Z_0 benih atau nilai awal. Maka persamaan (2 - 1) dikatakan menghasilkan Z_i , pembagian $a Z_{i-1} + c$ dengan m dan diberikan Z_i adalah sisa dari pembagian. Oleh karena itu, $0 \leq Z_i \leq m - 1$, dan menghasilkan bilangan random yang dikehendaki U_i untuk $i = 1 , 2 , \ldots$ pada [0 , 1], dan diberikan $U_i = Z_i / m$. Pada penjumlahan nonnegatif, bilangan bulat m, a , c dan Z_0 seharusnya memenuhi $0 < m$, $a < m$, $c < m$ dan $Z_0 < m$. Banyak percobaan komputer membutuhkan pembangkitan bilangan pseudorandom antara 0 dan 1. Sebagai ilustrasi, barisan bilangan pseudorandom dibangkitkan dengan memilih $m = 9$, $a = 7$, $c = 4$ dan $Z_0 = 3$, dapat ditemukan:

$$Z_1 = 7 Z_0 + 4 = 7 . 3 + 4 = 25 \text{ mod } 9 = 7 ,$$

$$Z_2 = 7 Z_1 + 4 = 7 . 7 + 4 = 53 \text{ mod } 9 = 8 ,$$

$$Z_3 = 7 Z_2 + 4 = 7 . 8 + 4 = 60 \text{ mod } 9 = 6 ,$$

$$Z_4 = 7 Z_3 + 4 = 7 . 6 + 4 = 46 \text{ mod } 9 = 1 ,$$

$$Z_5 = 7 Z_4 + 4 = 7 . 1 + 4 = 11 \text{ mod } 9 = 2 ,$$

$Z_6 = 7\ Z_5 + 4 = 7\ .\ 2 + 4 = 18 \bmod 9 = 0$,

$Z_7 = 7\ Z_6 + 4 = 7\ .\ 0 + 4 = 4 \bmod 9 = 4$,

$Z_8 = 7\ Z_7 + 4 = 7\ .\ 4 + 4 = 32 \bmod 9 = 5$,

$Z_9 = 7\ Z_8 + 4 = 7\ .\ 5 + 4 = 39 \bmod 9 = 3$,

Karena $Z_9 = Z_0$, dan karena setiap bagian tergantung hanya pada bagian sebelumnya, maka barisan yang dibangkitkan adalah :

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, . . .

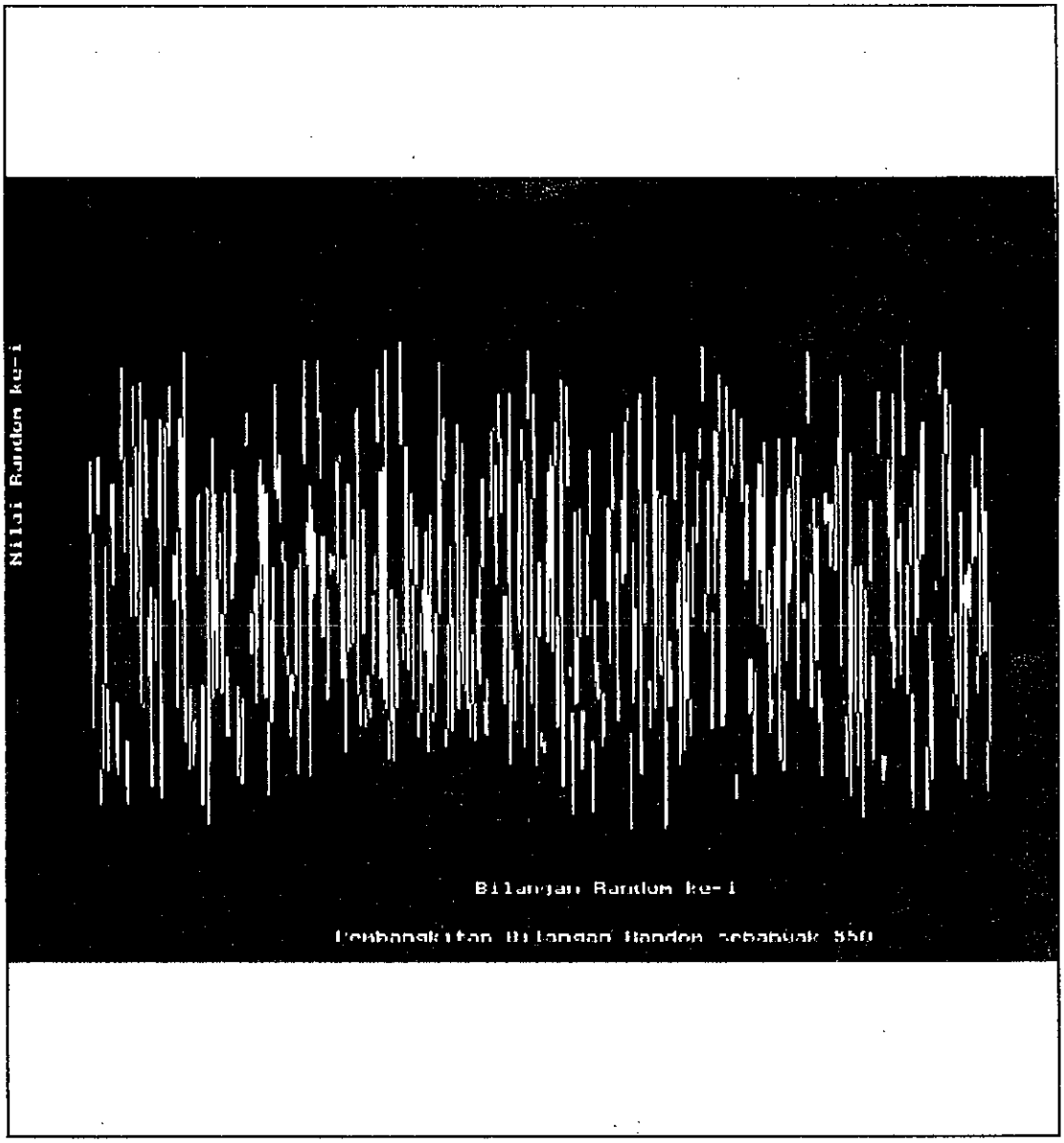
Barisan ini mempunyai 9 bilangan berbeda sebelum diulang kembali. Kenyataannya banyak komputer menggunakan *linier congruential generators* untuk membangkitkan bilangan pseudorandom. Seringkali, sebuah *linier congruential generators* dengan pertambahan c = 0 digunakan. Generator ini disebut **pure multiplicative generators**. Sebagai gambaran, pure multiplicative generators dengan modulus $2^{31} - 1$ dan pengali $7^5 = 16.807$ secara luas digunakan. Disamping itu, metode pembangkitan bilangan random lain yang digunakan adalah *prime modulus multiplicative Linier Congruential Generators*, dan digunakan $m = 2^b$, dan pada kasus ini b = 31 sehingga m adalah bilangan prima terbesar yang lebih kecil dari 2^{31} adalah $2^{31} - 1 = 2.147.483.647$. Untuk m prima mempunyai periode m -1 jika a adalah sebuah element primitif modulo m, dan lebih kecil daripada bilangan bulat l dimana $a^l - 1$ dapat dibagi dengan m adalah $l = m - 1$. Dengan memilih a dan m melalui metode tersebut dihasilkan setiap bilangan bulat 1, 2, 3, . . . , m - 1 tepat satu kali dalam setiap periode, sehingga Z_0 dapat sebarang bilangan bulat gelombang - gelombang dari 1 sampai m - 1 dengan periode

m - 1 akan dihasilkan.

Untuk kasus implementasi Algoritma Monte Carlo di implementasikan *Prime Modulus Multiplicative Linier Congruential Generators* yang telah disusun oleh Marse dan Roberts, yang dirumuskan $m = 2^b - q$ untuk sebarang bilangan bulat positif q. Menghasilkan $Z_i = (a Z_{i-1}) (\text{mod } 2^b)$, dimana dihasilkan overflow tanpa pembagian. Jika k adalah bilangan bulat terbesar dan lebih kecil atau sama dengan $a Z_{i-1} / \text{mod } 2^b$, maka :

$$Z_i = \begin{cases} Z_i' + kq & \text{jika } Z_i' + kq < 2^b - q \\ Z_i' + kq - (2^b - q) & \text{jika } Z_i' + kq \geq 2^b - q \end{cases}$$

Sebagai gambaran, grafik dari pembangkitan bilangan random sebanyak 550 kali dengan metode *prime modulus multiplicative linier congruential generators* sebagai berikut :



Dari grafik diatas terlihat distribusinya adalah uniform.