CENX570: Simulation and Modelling

Dr. Nasser-Eddine Rikli

HW #3

Submitted by:

Mohammed Shahzad

444105788@student.ksu.edu.sa

Exercise One

1. Find the period for $x_n = (17x_{n-1} + 43) \bmod 100$ with the following seeds:

(a) x0 = 27;

(b) x0 = 3;

(c) Check if any of the two seeds exist in the other sequence. Why?

2. Given the following LCG generator: $x_n = 7^5\, x_{n-1} \bmod 2^{31} - 1$:

(a) Is the maximum period achievable?

(b) What is the period?

(c) Is this a good generator? Why?

3. Check if the previous two generators pass the Chi-square test?

Answer:

1(a) Seeds:

$x_0 = 27$;

Given, $x_n = (17x_{n-1} + 43) \bmod 100$

$x_1 = (17(x_0) + 43) \bmod 100 = (17(27)+43) \bmod 100 = 2$

$x_2 = (17(x_1)+43) \bmod 100 = (17(2)+43) \bmod 100 = 77$

$x_3 = (17(x_2)+43) \bmod 100 = (17(77)+43) \bmod 100 = 52$

$x_4 = (17(x_3)+43) \bmod 100 = (17(52))+43 \bmod 100 = 27$ ……end

We have series 27,2, 77, 52. Therefore the period is 4 with seed x0 = 27

1(b) $x_0 = 3$;

Given, $x_n = (17x_{n-1} + 43) \bmod 100$

$x_1 = (17(x_0) + 43) \bmod 100 = (17(3)+43) \bmod 100 = 94$
$x_2 = (17(x_1)+43) \bmod 100 = (17(94)+43) \bmod 100 = 41$
$x_3 = (17(x_2)+43) \bmod 100 = (17(41)+43) \bmod 100 = 40$
$x_4 = (17(x_3)+43) \bmod 100 = (17(40))+43 \bmod 100 = 23$
$x_5 = (17(x_4) + 43) \bmod 100 = (17(23)+43) \bmod 100 = 34$
$x_6 = (17(x_5)+43) \bmod 100 = (17(34)+43) \bmod 100 = 21$
$x_7 = (17(x_6)+43) \bmod 100 = (17(21)+43) \bmod 100 = 0$
$x_8 = (17(x_7)+43) \bmod 100 = (17(0))+43 \bmod 100 = 43$
$x_9 = (17(x_8) + 43) \bmod 100 = (17(43)+43) \bmod 100 = 74$
$x_{10} = (17(x_9)+43) \bmod 100 = (17(74)+43) \bmod 100 = 1$
$x_{11} = (17(x_{10})+43) \bmod 100 = (17(1)+43) \bmod 100 = 60$
$x_{12} = (17(x_{11})+43) \bmod 100 = (17(60))+43 \bmod 100 = 63$

$x_{13} = (17(x_{12}) + 43) \bmod 100 = (17(63)+43) \bmod 100 = 14$
$x_{14} = (17(x_{13})+43) \bmod 100 = (17(14)+43) \bmod 100 = 81$
$x_{15} = (17(x_{14})+43) \bmod 100 = (17(81)+43) \bmod 100 = 20$
$x_{16} = (17(x_{15})+43) \bmod 100 = (17(20))+43 \bmod 100 = 83$
$x_{17} = (17(x_{16}) + 43) \bmod 100 = (17(3)+43) \bmod 100 = 54$
$x_{18} = (17(x_{17})+43) \bmod 100 = (17(94)+43) \bmod 100 = 61$
$x_{19} = (17(x_{18})+43) \bmod 100 = (17(41)+43) \bmod 100 = 80$
$x_{20} = (17(x_{19})+43) \bmod 100 = (17(40))+43 \bmod 100 = 3$ …..end

The series is : 3, 94,41,40,23,34,21,0,43,74,1,60,63,14,81,20,83,54,61,80,

and the period is 20

1(c) No, there are no common elements in the two series. This is due to choice of seed value. Due to larger difference between them, they don't have common elements.

2(a)

Given LCG, $x_n = 7^5\ x_{n-1} \bmod 2^{31} - 1$; This of the form a x_{n-1} + b mod m

➔ $M=2^{31} - 1 = 2147483647$, $a = 7^5$, $b = 0$

2(a) Yes, Maximum period is achievable.

Since,

The LCG has full period if and only if the following conditions hold:

it is possible to get a period of m-1 if:

1. m is a prime number,
2. a is a primitive root of the modulus m.
3. a is a primitive root of m if and only if:
4. $a^n \bmod m \neq 1$ for $n = 1, 2, \ldots, m-2$.

2(b) What is max period?

According To LCG rules, for :

- When m != 2^k
- m is a prime (m = 2147483647 is a prime)
- a (a= 16807 is a primitive root of m)
- b=0;

Max period = (m - 1)

Which is $(2^{31} - 1)-1 = 2147483646$

2(c) It is a good generator; Full period (m-1) is achievable.

3. Chi-square test for LCG in 1 and 2

$$\chi_0^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

For LCG $x_n = (17x_{n-1} + 43) \bmod 100$, x0 = 27 [27,2,77,52]

Interv	Upper limit	Oi	Ei	|(Oi - Ei)|	(Oi - Ei) square	[(Oi - Ei) squared] / Ei
1	10	25	10	10	100	10
2	20	0	10	10	100	10
3	30	25	10	15	225	22
4	40	0	10	10	100	10
5	50	0	10	10	100	10
6	60	25	10	15	225	22
7	70	0	10	10	100	10
8	80	25	10	15	225	22
9	90	0	10	10	100	10
10	100	0	10	10	100	10
Sum		100	100			136

$X^2_{(0.05,9)} = 16.92$

Therefore, the generator fails the chi square test

………

$$\chi_0^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

For LCG $x_n = (17x_{n-1} + 43) \bmod 100$, x0 = 3;

[3, 94,41,40,23,34,21,0,43,74,1,60,63,14,81,20,83,54,61,80]

Interv	Upper limit	Oi	Ei	|(Oi - Ei)|	(Oi - Ei) square	[(Oi - Ei) squared] / Ei
1	10	15	10	5	25	2.5
2	20	10	10	0	0	0
3	30	10	10	0	0	0
4	40	10	10	0	0	0
5	50	10	10	0	0	0
6	60	10	10	0	0	0
7	70	10	10	0	0	0
8	80	10	10	0	0	0
9	90	10	10	0	0	0
10	100	5	10	5	25	2.5
Sum		100	100			5

$X^2_{(0.05,9)} = 16.92$,

$X^2 = 5 < X^2_{(0.05,9)}$

Therefore, the generator PASSES the chi square test with 9 degree freedom and 95% confidence.

Exercise Two

Given the following LCG generator: $x_n = ax_{n-1} \bmod 2^4$.

1. What is the maximum obtainable period?

2. What should be the value of a to get this period?

3. What restrictions are required on the seed?

4. Compute the period of the following generator: $x_n = 13x_{n-1} \bmod 2311$.

Answer:

1. Given LCG, $x_n = ax_{n-1} \bmod 2^4$.

   ➔ $m = 2^4$
   ➔ $b=0$

Maximum period is 2^{k-2}; which is $2^{4-2} = 4$

2. a = (8i - 3) OR (8i + 3)

3. Seed should be odd number.

4. Given generator, $x_n = 13x_{n-1} \bmod 2311$

   -> m = 2311 , a = 13, b = 0;

   - m is a prime number,

   - b = 0

Therefore period = (m -1) = 2310

Exercise Three

1. Determine $24^n \bmod 31$ for $n = 1, \cdot\cdot\cdot, 30$.

2. Find the smallest n for which the mod operation's result is 1.

3. Is 24 a primitive root of 31?

4. Determine all primitive roots of 11.

Answer:

1. Given series: $x_n = 24^n \bmod 31$ for n = 1…..30

   $x_1 = 24^1 \bmod 31 = 24 \bmod 31 = 24$

   $x_2 = 24^2 \bmod 31 = 18$

   $x_3 = 24^3 \bmod 31 = 29$

   $x_4 = 24^4 \bmod 31 = 14$

$x_5 = 24^5 \bmod 31 = 26$

$x_6 = 24^6 \bmod 31 = 4$

$x_7 = 24^7 \bmod 31 = 3$

$x_8 = 24^8 \bmod 31 = 10$

$x_9 = 24^9 \bmod 31 = 23$

$x_{10} = 24^{10} \bmod 31 = 25$

$x_{11} = 24^{11} \bmod 31 = 11$

$x_{12} = 24^{12} \bmod 31 = 16$

$x_{13} = 24^{13} \bmod 31 = 12$

$x_{14} = 24^{14} \bmod 31 = 9$

$x_{15} = 24^{15} \bmod 31 = 30$

$x_{16} = 24^{16} \bmod 31 = 7$

$x_{17} = 24^{17} \bmod 31 = 13$

$x_{18} = 24^{17} \bmod 31 = 2$

$x_{19} = 24^{19} \bmod 31 = 17$

$x_{20} = 24^{20} \bmod 31 = 5$

$x_{21} = 24^{21} \bmod 31 = 27$

$x_{22} = 24^{22} \bmod 31 = 28$

$x_{23} = 24^{23} \bmod 31 = 21$

$x_{24} = 24^{24} \bmod 31 = 8$

$x_{25} = 24^{25} \bmod 31 = 6$

$x_{26} = 24^{26} \bmod 31 = 20$

$x_{27} = 24^{27} \bmod 31 = 15$

$x_{28} = 24^{28} \bmod 31 = 19$

$x_{29} = 24^{29} \bmod 31 = 22$

$x_{30} = 24^{30} \bmod 31 = 1$

There fore the series is: 24, 18 , 29, 14, 26 ,4, 3, 10, 23 , 25, 11, 16, 12, 9, 30, 7 , 13, 2, 17, 5, 27, 28, 21, 8, 6, 20, 15, 19, 22, 1.

2. Smallest number n where mod operation result is 1 is 30.

3. Yes, 24 is primitive root of 31. [For n = 1 ….. 29, a^n mod 31=! 1]

4. Primitive roots of 11;

For primitive root,

a mod 11 such that ;

a^n mod 11 != 1 for n = 1- 9

[a^n mod m != 1 for n = 1 ………(m-2), then a is said to be primitive root of m]

We find out that, - 2,6,7,8 are primitive roots of 11

Exercise Four

1. Implement the following LCG using Schrage's method to avoid overflow:

$$x_n = 40014x_{n-1} \bmod 2147483563$$

2. Using a seed of $x_0 = 1$, determine x_{10000}.

3. Check if this generator passes the Chi-square test?

Answer:

1. Schrage method:

Given,

$x_n = 40014x_{n-1} \bmod 2147483563$ can be written as (using Schrage's method)

➔ $x_n= g(x_{n-1}) + m*h(x_{n-1})$

Where,

$g(x_{n-1}) = a(x_{n-1} \bmod q) - r(x_{n-1} \operatorname{div} q)$

$h(x_{n-1}) = (x_{n-1} \operatorname{div} q) – (a* x_{n-1} \operatorname{div} m)$

$q = m \operatorname{div} a$

$r = m \bmod a.$

when a =40014 , m = 2147483563

q = 2147483563 div 40014 = 53668

r = 2147483563 mod 40014 = 12211

r < q ; Therefore possible

2. PYTHON code

seed of x_0 = 1, determine x_{10000}.

#Schrage's method for x10000

```
def randVal(seed):
    n = 1 # counter variable
    xN = seed #x0 = 1
    xNextn = 0

    # loop till we reach x10000
    while n<10001:
        xNextn = schrage(xN)
        xN = xNextn
        n=n+1
    print(xN)

# Schrage's method calculation of parameters for xN
def schrage(xNold):

    a = 40014
    m = 2147483563
    q = 53668
    r = 12211
    xDivq = 0
```

```
    xModq = 0
    gX = 0
    hX = 0
    xDivq = xNold // q
    axDivm = (a*xNold) // m
    xModq = xNold % q
    gX = (a * xModq) - (r * xDivq)
    hX = xDivq - axDivm
    xNew = gX + m*hX

    return xNew # return xN+1

def main():
    print("Hello World!")

if __name__ == "__main__":
    main()
    randVal(1)
```

< See attached file - schrage.py >
Output: 1919456777

Therefore, x_{10000} = 1919456777

3. Chi-square test

$$\chi_0^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

***