

Ch. 7

Exercise 20:

Write a computer program that will generate four-digit random numbers using the multiplicative congruential method. Allow the user to input values of X_0 , a , c and m .

Here is a matlab .m file that implements a multiplicative congruential random number generator function:

```
function [xi,xiq]=mcrand(x0,a,c,m)
% function [xi,xiq]=mcrand(x0,a,c,m)
% this function computes the next random number in sequence
% for a multiplicative congruential random number generator
% with multiplier a, offset c and modulus m. It returns two
% values, xi, which is the next integer in the sequence, xiq,
% which is xi, represented as a 4 digit number 0<=xiq<=1.
% sequential calls to mcrand should use the xi return value as
% the next x0 value. For instance, in a loop:
%
% ...
% [nextvalue,randomnumber] = mcrand(nextvalue,a,c,m);
% ...
%
xi=mod((x0*a+c),m);
xiq=floor(10000*xi/m)*.0001;
```

This program could have been implemented in any language that the student is comfortable with. What is important is (1) the multiplicative congruential formula needs to be implemented correctly, (2) there should be a way to generate consecutive numbers, e.g., the return of the xi state information and (3) the problem asked for 4 digit numbers – there should be some way to insure the numbers are 4 digit numbers. The problem did not ask them to be scaled from 0-9999 or 0-1. I chose to represent them as numbers with 4 significant digits that are less than 1.

Exercise 23:

Consider the multiplicative congruential generator under the following circumstances:

- (a) $a = 11, m = 16, X_0 = 7$.
- (b) $a = 11, m = 16, X_0 = 8$.
- (c) $a = 7, m = 16, X_0 = 7$.
- (d) $a = 7, m = 16, X_0 = 8$.

Generate enough values in each case to complete a cycle. What inferences can be drawn? Is maximum period achieved?

	Case (a)	Case (b)	Case (c)	Case (d)
i	X_i	X_i	X_i	X_i
0	7	8	7	8
1	13	8	1	8
2	15		7	
3	5			
4	7			

The maximum period (4) occurs when X_0 is odd and $a = 3 + 8k$ where $k = 1$. Even seeds have the minimum possible period, independent of a . The maximum period, 16, is not achieved with any of these cases.

Exercise 29:

In some applications it is useful to be able to quickly skip ahead in a pseudo-random number sequence without actually generating all of the intermediate values.

- (a) for a linear congruential generator with $c = 0$, show that $X_{i+n} = (a^n X_i) \bmod m$.

- (b) Next show that $(a^n X_i) \bmod m = (a^n \bmod m) X_i \bmod m$ (this result is useful because $a^n \bmod m$ can be precomputed, making it easy to skip ahead n random numbers from any point in the sequence).
- (c) In Example 7.3, use this result to compute X_5 starting with $X_0 = 63$. Check your answer by computing X_5 in the usual way.

Two results that are useful to solve this problem are:

$$(c + d) \bmod m = c \bmod m + d \bmod m$$

and

$$g = h - km \quad \text{for some } k \geq 0$$

The last result is true because, by definition, g is the remainder after subtracting the largest integer multiple of m that is less than or equal to h .

(a) Note that:

$$\begin{aligned} X_{i+2} &= aX_{i+1} \bmod m \\ &= a[aX_i \bmod m] \bmod m \\ &= a[aX_i - km] \bmod m \quad \text{for some } k \geq 0 \\ &= a^2 X_i \bmod m - akm \bmod m \\ &= a^2 X_i \bmod m \quad \text{since } akm \bmod m = 0 \end{aligned}$$

(b) Note that:

$$\begin{aligned} (a^n X_i) \bmod m &= \{(a^n \bmod m) + [a^n - (a^n \bmod m)]\} X_i \bmod m \\ &= \{(a^n \bmod m) X_i \bmod m\} + \{[a^n - (a^n \bmod m)] X_i \bmod m\} \\ &= \{(a^n \bmod m) X_i \bmod m\} + \{km X_i \bmod m\} \quad \text{for some integer } k \geq 0 \\ &= (a^n \bmod m) X_i \bmod m \end{aligned}$$

(c) In this generator $a = 19$, $m = 100$ and $X_0 = 63$. Therefore $a^5 \bmod 100 = 19^5 \bmod 100 = 99$. Thus, $X_5 = (99)(63) \bmod 100 = 37$.