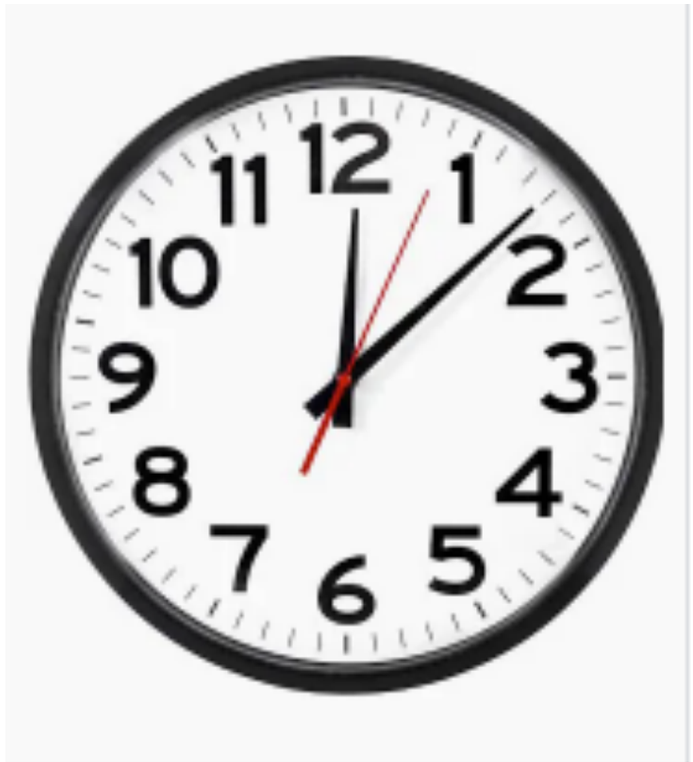
Math Teacher Circle.

November 2024

Random vs Deterministic?

(Dynamics)

Linear Congruence Generators



Modular (clock) arithmetic.

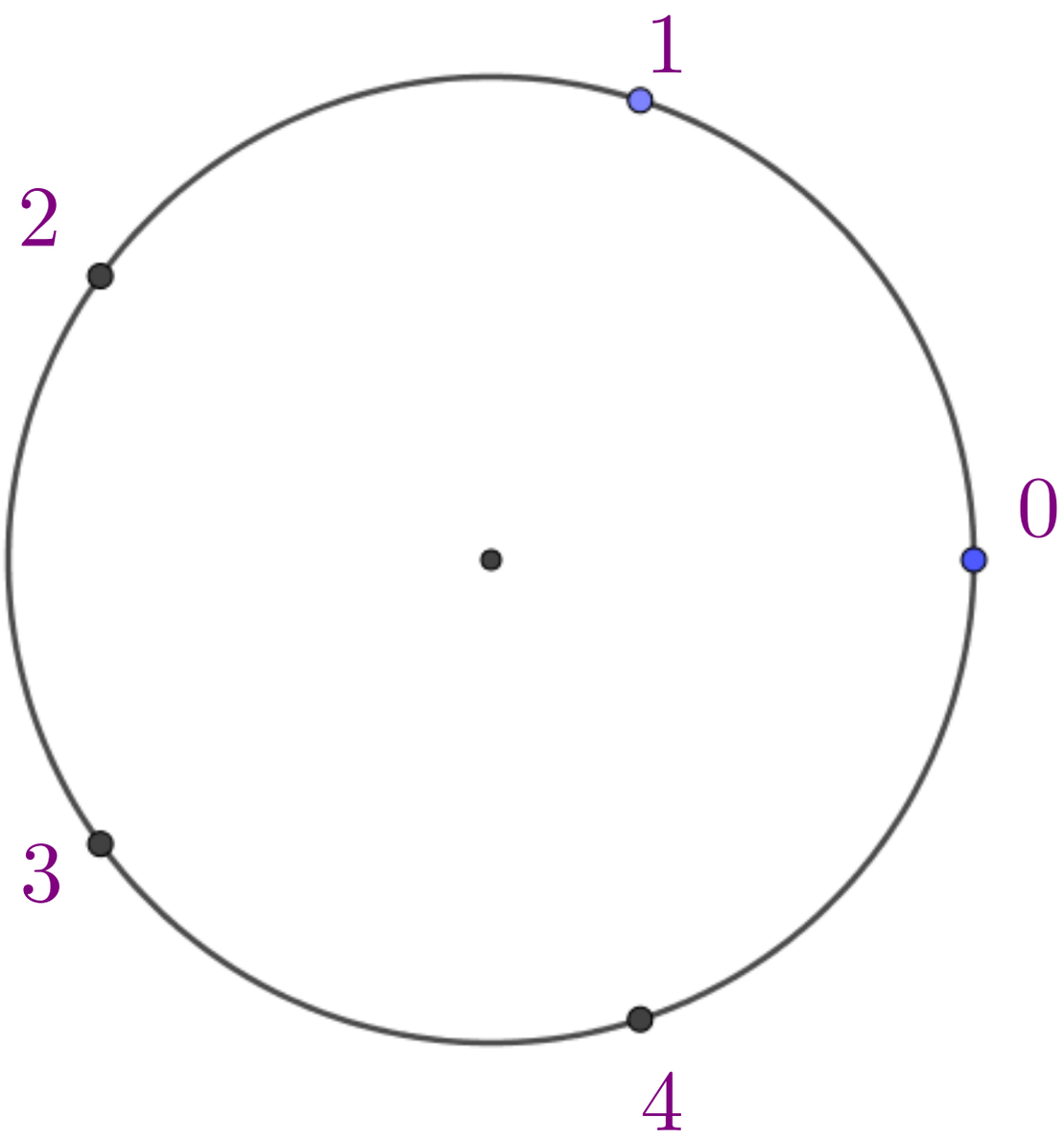
$$12 = 0.$$

$$13 = 1$$

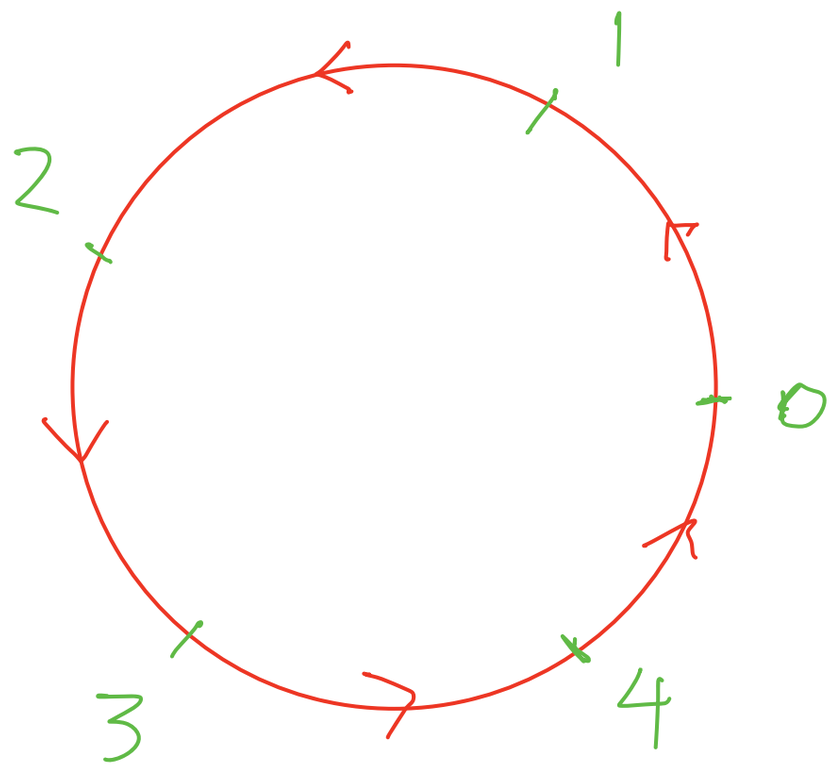
$3 \text{ x } 4 = ?$

$7 + 8 = ?$

Mod 5



$x \to x+1 \pmod 5$



$0 \to 1 \to 2 \to 3 \to 4 \to 0$

A simple dynamical system on the clock:

Iterate the map

$$f(x) = 3x + 1 \qquad (mod \qquad 5)$$

in other words $x_{n+1} = 3x_n + 1 \qquad (mod \qquad 5)$

with $x_i = 0, 1, 2, 3$ or 4

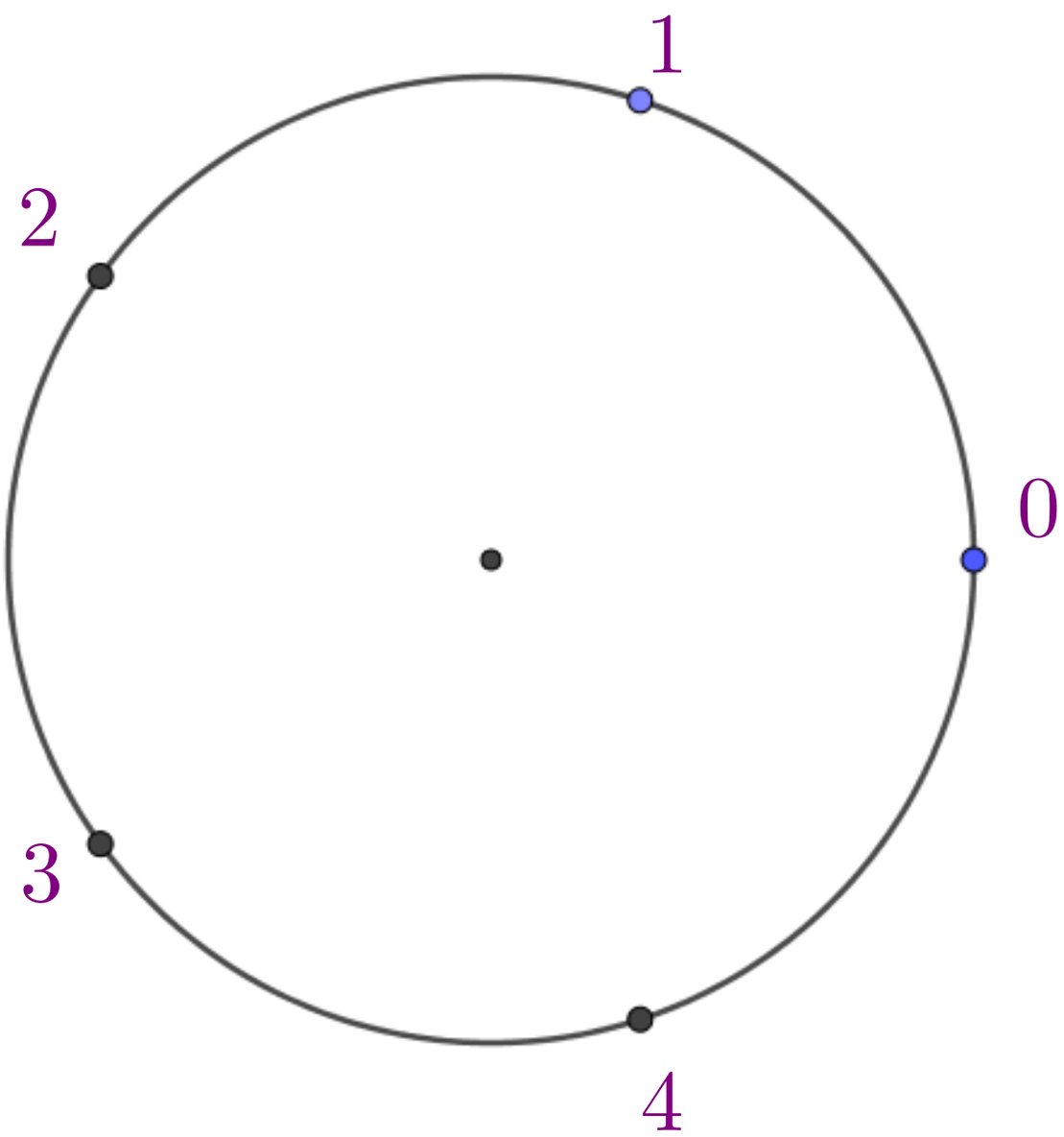
What happens?

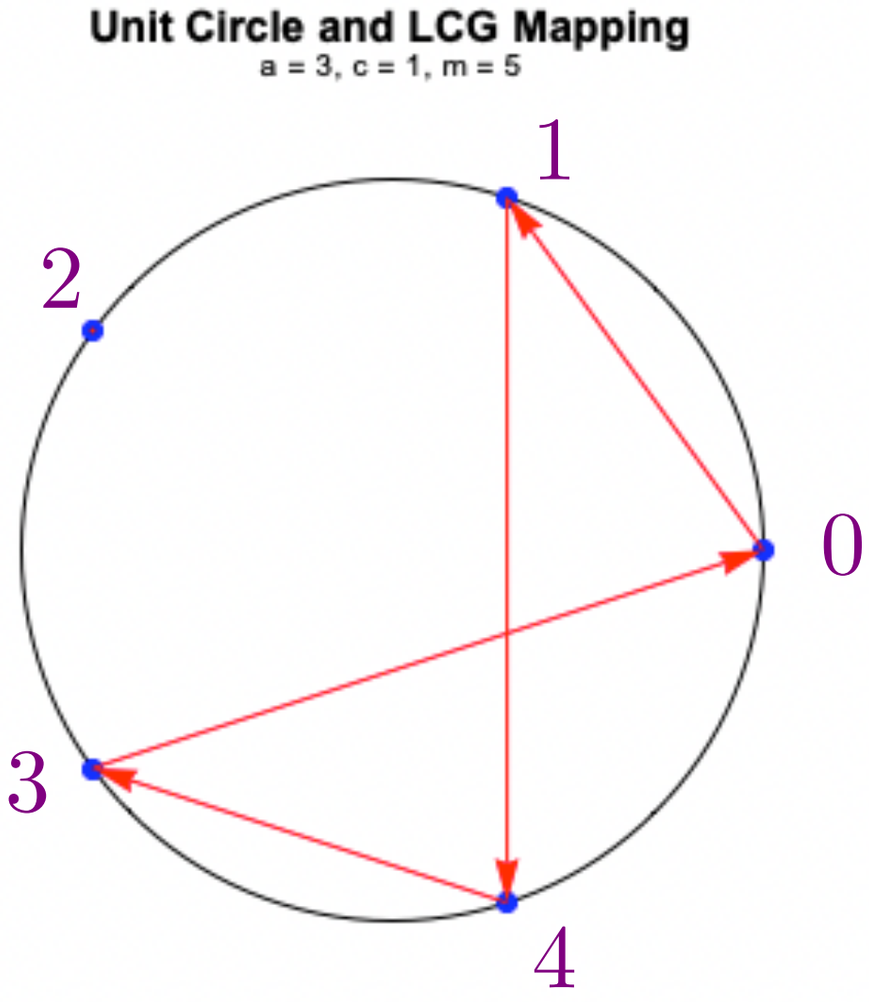
Where does 0 go? i.e what is $f(0)$?

1?

2,3 ,4 ?

Mod 5




Unit Circle and LCG Mapping
a = 3, c = 1, m = 5
1
2
3
4
0

Linear Congruence Generators, or LCGs :

$$x_{n+1} = ax_n + c \qquad (mod\ \ m)$$

with x_n, a, c and m all integers

$f(x) = ax + c;$ with $x \in \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

so $f : \mathbb{Z}_m \to \mathbb{Z}_m$

"seed" $x_0 \in \mathbb{Z}_m$

$x_1 = f(x_0), x_2 = f(x_1), \ldots$

PROBLEMS.

Assume $a \neq 1$ in the following.

1. Working modulo 5:
Describe the orbit structure of $x \mapsto 4x + 1 \bmod 5$.

2. Working modulo 8:
Describe the orbit structure of $x \mapsto 5x + 1 \ (\bmod 8.)$

3. Work modulo $m = 5$. Show that every LCG

$$x_{n+1} = ax_n + c \qquad (mod \qquad 5)$$

has a fixed point with the single exception of $x_{n+1} = x_n + 1$.

4. Generalize the statement of problem 3 by replacing 'm = 5' by m = any prime.

5. Prove it

Terminology, so far

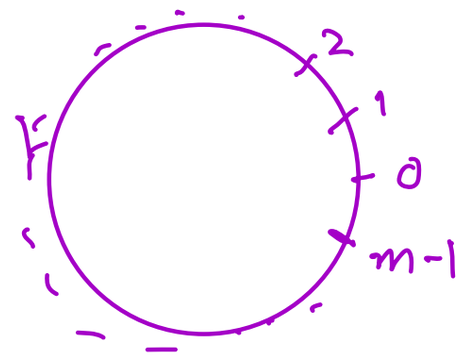
- "orbit" "fixed point"
- "transitive"

& from number theory:

"modulo" "modular arithmetic"

$\mathbb{Z}_m$ or $\mathbb{Z}/m\mathbb{Z}$

which we represent by $\{0, 1, 2, 3, \ldots, m-1\}$ or a clock:



From the late 1950 to the late 1980
most random number generators were LCGs

"By far the most successful random number generators known today [1968] are special cases of the following scheme .." WHAT WE JUST DESCRIBED! LCGs

– Donald Knuth, "The Art of Computer Programming", vol. 2, p. 9.

Common choices of parameters m (modulus) and a, c

$m = 2^{31} - 1$ (a Mersenne prime) $\quad a = 7^5 = 16,807$
$c = 0$

$m = 2^{31} \quad a = 65539, c = 0 \quad$ (RANDU)

to get random numbers u in the unit interval $0 \leq u \leq 1$
divide the "random outputs" x_n by m, the modulus ; ie
set $u_n = x_n/m$

Questions.

Why would these work?

Do they work?

How could you even tell if they work?

(What does it mean for a sequence of numbers to be "random"?)

Why do we want the orbits of the LCG to be long?

How can we make "good" choices of the parameters a, c, m? Of the seed x_0?

Can a deterministic process yield a random output?

LCGs have the form: $x_{n+1} = f(x_n) \bmod m$

where $f : \mathbb{Z}_m \to \mathbb{Z}_m$ is a map
applied iteratively starting with some "seed" $x_0 \in \mathbb{Z}_m$

The resulting sequence $x_0, x_1, x_2, \ldots, x_n, \ldots$
is called the "orbit" of x_0.

Eventually, the sequence must repeat:
$x_i = x_n$ for some pair $i < n$, with $0 \leq i$.

Why?

If f is invertible, $n = i + k$ and $x_n = x_i$
THEN, upon applying f^{-1} we get:

$$x_{k+i-1} = x_{i-1}$$

$$\dots$$

$$x_k = x_0$$

which means the whole sequence is periodic with period k.

If f is not invertible, every orbit still eventually settles down to a periodic one: $x_{n+k} = x_n$ for all n after some point on.

SHORTER ORBITS : MORE PREDICTIBLE

eg: $x_0, x_1, x_2, \ldots, x_n, = 3, 3, 3, \ldots, 3,$
(period 1 or a fixed point !)

LONGER ORBITS : MORE RANDOM

N. B.: LONG -ish is NECESSARY but not SUFFICIENT for randomness
(eg: the sequence generated by $f(x) = x + 1$ is LONG but not random)

PROBLEM:

Show that ANY `random number generator'of the form:

$$x_{n+1} = f(x_n) \bmod m$$

for any $f : \mathbb{Z}_m \to \mathbb{Z}_m$

yields sequences $x_0, x_1, \ldots, x_n, \ldots$

whose period is AT MOST m.

We want long orbits.

Can we find orbits as long as possible,

which is to say, of length m?

A nice theorem on transitive LCGs.

$$x_{n+1} = ax_n + c \bmod m$$

with m a power of 2: thus $m = 2^d$.

Theorem. This LCG acts transitively on $\mathbb{Z}_m$ if and only if and 4 divides $a - 1$ and c is odd.

Example: earlier we went through the special case $m; a, c = 8; 5, 1,$ of this theorem

REFS.

Theorem A, p. 15, vol 2 of Knuth's "The Art of Scientific Programming"
(The 'nice theorem" is a special case of this more general theorem)

Martin Greenberger, JACM (Journal of the Association of Computing Machinery),
"Notes on a New Pseudo-Random Number Generator", 1961.

LCGs are single step recursion relations:

$$x_{n+1} = f(x_n) \bmod m$$

Consider two-step recursion relations.
For example

$$x_{n+1} = x_n + x_{n-1} \bmod m$$

Seed with:

$$x_0 = 0 \qquad x_1 = 1$$

$$x_2 = ?, x_3 = ?$$

The Fibonacci numbers modulo m
!!

Problem.
For modulus $m = 5$ work out this mod 5 Fibonacci sequence until it begins to repeat itself.
What is its period?

Problem. Consider ANY two-step recursion relation:

$$x_{n+2} = f(x_{n+1}, x_n) mod m$$

for generating sequences $x_0, x_1, x_2, \ldots$ in $\mathbb{Z}_m$
What is the maximum possible period of such a sequence?

Back to the Fibonacci's mod 5.
We found that they form an orbit of length 20.

Of what? Of the "Fibonacci map"

$$(x, y) \to (x + y, x)$$

acting on the space $X = \mathbb{Z}_5 \times \mathbb{Z}_5$ of pairs (x,y) of integers mod 5.

Now (0,0) is a fixed point of this map, so an orbit of length 1 while X has 25 elements total and the orbits of the 'Fibonacci map" partition X up.

But $25 = 20 + 1 + 4$. This suggests that there ought to be an orbit of length 4 for the Fibonacci map acting on X.

PROBLEM.
Find it! Find a length 4 orbit for the Fibonacci map acting on $X = \mathbb{Z}_5 \times \mathbb{Z}_5$.

Examples
Pictures; Gallery
Questions

EXAMPLES

Coin Flips!

The Random Number Generators of a computer!

Linear Congruence Relations:

$$x_{n+1} = ax_n + c \text{ taken mod } m$$

Fibonacci scheme

$$x_{n+1} = x_n + x_{n-1} \text{ mod } m$$

Baker's transformation

Cat map

from physics:
Newton's equations.

Flow is area (volume) preserving and reversible:

suggests: study invertible area preserving maps

eg. Standard Map

REFERENCES

Wiki pages:
Linear Congruence generators, Random Number Generators
RANDU

Knuth's "The Art of Scientific Programming"
see esp. volume 2, page 15, Theorem A

Martin Greenberger, JACM (Journal of the Association of Computing Machinery),
"Notes on a New Pseudo-Random Number Generator", 1961.

Does Theorem A in the special case where m has the form $m = 2^d$

REFS.

Theorem A, p. 15, vol 2 of Knuth's "The Art of Scientific Programming"

(The 'nice theorem" is a special case of this more general theorem)

https://www.youtube.com/watch?v=thmnJXfoIYA&t=693s

on Linear Feedback Shift Registers. by a guy named Tarnoff.

I liked it! 11 min 33 seconds long youtube.