

Andrew Burkus

1. Done.

Let's assume  $m = 2^{32}$ .

$$j(x) = ax + b \text{ (m)}$$
$$S_1 = S_0 \cdot a + b \text{ (m)}$$
$$S_2 = S_1 \cdot a + b \text{ (m)}$$

---

$$S_2 - S_1 = S_1 - S_0 \cdot a \text{ (m)}$$
$$y = S_2 - S_1, \quad c = S_1 - S_0$$
$$(c^{-1})y = a \cdot c(c^{-1}) \text{ (m)}$$
$$(c^{-1})(y) = a \text{ (m)}$$
$$\boxed{a = 214013}$$
$$S_2 = S_1(214013) + b \text{ (m)}$$
$$d = S_1 \cdot 214013$$
$$S_2 - d = b \text{ (m)}$$
$$\boxed{b = 2531011}$$

2.

```
cmd - python
C:\Users\agb
^ python
Python 3.6.5 (v3.6.5:f59c0932b4, Mar 28 2018, 16:07:46) [MSC v.1900 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> m = 2 ** 32
>>> a = 214013
>>> b = 2531011
>>> s1 = 1255958651
>>> s2 = 3837989202
>>> ((s1 * a) + b) % m
3837989202
>>> ((s1 * a) + b) % m == s2
True
>>>
```

Here's the values being checked in Python.

3.

```
cmd
Register: 0001 Output: 1
00011000110001100011

C:\Users\agb\Documents\GitHub\CSC333\HW3 (master)
^ python lfsr.py
Register: 1000 Output: 0
Register: 1100 Output: 0
Register: 1110 Output: 0
Register: 0111 Output: 1
Register: 1011 Output: 1
Register: 0101 Output: 1
Register: 0010 Output: 0
Register: 1001 Output: 1
Register: 1100 Output: 0
Register: 1110 Output: 0
Register: 0111 Output: 1
Register: 1011 Output: 1
Register: 0101 Output: 1
Register: 0010 Output: 0
Register: 1001 Output: 1
Register: 1100 Output: 0
Register: 1110 Output: 0
Register: 0111 Output: 1
Register: 1011 Output: 1
Register: 0101 Output: 1
0001101001110100111

C:\Users\agb\Documents\GitHub\CSC333\HW3 (master)
^
```

B. The maximal period is  $2^m - 1$  where  $m$  is the number of registers or 'flip flops'. This means the period should be  $2^4 - 1$ , or 15.

C. The first repeating sequence is 1110100, which is 7 bits long. The period is 7.

D. Yes, there is a pre-period. It is 000. The LFSR will print out its initial input always. This means that regardless of the program, the initial output will be some arbitrary sequence of bits which may or may not be part of the period. If it is part of the period, it is by coincidence.

$S = 1110001001101011100$   
 $m = 4$

$$0 = P_3 \cdot 1 + P_2 \cdot 1 + P_1 \cdot 1 + P_0 \cdot 0$$
$$0 = P_3 \cdot 1 + P_2 \cdot 1 + P_1 \cdot 0 + P_0 \cdot 0$$
$$1 = P_3 \cdot 1 + P_2 \cdot 0 + P_1 \cdot 0 + P_0 \cdot 0$$
$$0 = P_3 \cdot 0 + P_2 \cdot 0 + P_1 \cdot 0 + P_0 \cdot 1$$

$P_3 P_2 P_1 P_0 = 1100$

4.

I did the algebra mentally. A lot of it zeroes out line by line, so you can find the values of the program that way quite easily.

```
cmd
C:\Users\agb\Documents\GitHub\CSC333\HW3 (master)
λ atom lfsr.py

C:\Users\agb\Documents\GitHub\CSC333\HW3 (master)
λ python lfsr.py
Register: 0111 Output: 1
Register: 0011 Output: 1
Register: 0001 Output: 1
Register: 1000 Output: 0
Register: 0100 Output: 0
Register: 0010 Output: 0
Register: 1001 Output: 1
Register: 1100 Output: 0
Register: 0110 Output: 0
Register: 1011 Output: 1
Register: 0101 Output: 1
Register: 1010 Output: 0
Register: 1101 Output: 1
Register: 1110 Output: 0
Register: 1111 Output: 1
Register: 0111 Output: 1
Register: 0011 Output: 1
Register: 0001 Output: 1
Register: 1000 Output: 0
Register: 0100 Output: 0
11100010011010111100

C:\Users\agb\Documents\GitHub\CSC333\HW3 (master)
λ
```

Here are the reproduced results you gave us on the homework. They match up exactly.