Lehmer RNGs: Introduction

CMSC 326: Simulation
Spring 2018

29 January 2018
Start R, then `library(simEd)`, then `?ssq`

Under “Examples”: show use of (simple) trace data

Use interarrival and service times from Lecture 1 table

```r
interarrivalTimes <<- c(15,32,24,40,12,29,80,13)
serviceTimes <<- c(43,36,34,30,38,30,31,29)
# <<- does global assignment in R
```

Do output stats match Lecture 1?
Want more data?
Changes to model?
Input data set too small or unavailable?

RNG addresses these problems

**Ideal** random number generator
- each value in $0.0 < u < 1.0$ is *equally likely*

**Good** random number generator
- output statistically indistinguishable from an ideal generator

Convert to **random variate** via mathematical transformations
Conceptual Model:

1. Choose a large positive integer $m$:
   $$\mathcal{X}_m = \{1, 2, \ldots, m - 1\}$$

2. Fill (conceptual) urn with the elements of $\mathcal{X}_m$

3. Each time a random number $u$ is needed:
   - draw an integer $x$ “at random” from the urn
   - let $u = x/m$

Possible values are $1/m, 2/m, \ldots, (m - 1)/m$. 
Want $m$ large: values are densely distributed $\in (0.0, 1.0)$

- We would like to draw from the urn with replacement
- For practical reasons, we will draw without replacement
  - If $m$ is large...
Lehmer’s Algorithm

- *Lehmer’s algorithm:*
  - modulus \( m \), a fixed large *prime* integer
  - multiplier \( a \), a fixed integer in \( \mathcal{X}_m \)

- The equation
  \[ g(x) = ax \mod m \]

  defines integer sequence \( x_0, x_1, \ldots \)

- \( x_0 \in \mathcal{X}_m \) is called the *initial seed*

- \( x_{i+1} = g(x_i) \)

- Nothing random about a Lehmer generator
  - called a *pseudo-random* generator
Choice of $m$ is dictated, in part, by system considerations
- 32-bit system: $2^{31} - 1$ is a natural choice
- 16-bit, 64-bit systems: not as obvious

Choose $m$ to be the largest representable prime integer
Given $m$, choice of multiplier $a$ must be made with great care
You Try It

Let \( m = 17 \)

\( \mathcal{X}_m = \{1, 2, \ldots, 16\} \)

Pick a multiplier \( a \neq 1 \in \mathcal{X}_m \) (AVOID: \( a = 4, 13, 16 \))

Pick any initial seed \( x_0 \) then generate sequence
Example

- If $m = 17$ and $a = 3$ with $x_0 = 1$ then the sequence is $1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1, \ldots$

- If $m = 17$ and $a = 14$ with $x_0 = 1$ then the sequence is $1, 14, 9, 7, 13, 12, 15, 6, 16, 3, 8, 10, 4, 5, 2, 11, 1, \ldots$

- If $m = 17$ and $a = 4$ with $x_0 = 1$ then the sequence is $1, 4, 16, 13, 1, \ldots$

- What happens with $m = 17, a = 4, x_0 = 2$?
- What happens with $m = 17, a = 4, x_0 = 3$?
Central Issues

- For given \((a, m)\) pair, is the sequence full-period?
- If full-period, how random does the sequence appear to be?
- Can \(ax \mod m\) be evaluated efficiently and correctly?
  - Integer overflow can occur when computing \(ax\)
  - More on this later...
Consider $m = 17$, $a = 14$, $x_0 = 6$

Compute:

$a^1 x_0 \mod m$ vs. $g(x_0)$

$a^2 x_0 \mod m$ vs. $g(x_1)$

$a^3 x_0 \mod m$ vs. $g(x_2)$

$a^4 x_0 \mod m$ vs. $g(x_3)$

\[ \vdots \]
Consider $m = 17$, $a = 14$, $x_0 = 6$

Compute:

$a^1 x_0 \mod m$ vs. $g(x_0)$

$a^2 x_0 \mod m$ vs. $g(x_1)$

$a^3 x_0 \mod m$ vs. $g(x_2)$

$a^4 x_0 \mod m$ vs. $g(x_3)$

... 

If $m = 17$ and $a = 14$ with $x_0 = 6$ then the sequence is

6, 16, 3, 8, 10, 4, 5, 2, 11, 1, 14, 9, 7, 13, 12, 15, 6, ...
Theorem (2.1.1)

If the sequence $x_0, x_1, x_2, \ldots$ is produced by a Lehmer generator with multiplier $a$ and modulus $m$ then

$$x_i = a^i x_0 \mod m$$

- It is an eminently bad idea to compute $x_i$ by first computing $a^i$.
- Theorem 2.1.1 has significant theoretical value...
$m = 17$ Example: What Do You Notice?

<table>
<thead>
<tr>
<th>multiplier</th>
<th>sequence</th>
<th>period</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a = 2$</td>
<td>1, 2, 4, 8, 16, 15, 13, 9, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>$a = 3$</td>
<td>1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 4$</td>
<td>1, 4, 16, 13, 1, ...</td>
<td>$p = 4$</td>
</tr>
<tr>
<td>$a = 5$</td>
<td>1, 5, 8, 6, 13, 14, 2, 10, 16, 12, 9, 11, 4, 3, 15, 7, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 6$</td>
<td>1, 6, 2, 12, 4, 7, 8, 14, 16, 11, 15, 5, 13, 10, 9, 3, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 7$</td>
<td>1, 7, 15, 3, 4, 11, 9, 12, 16, 10, 2, 14, 13, 6, 8, 5, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 8$</td>
<td>1, 8, 13, 2, 16, 9, 4, 15, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>$a = 9$</td>
<td>1, 9, 13, 15, 16, 8, 4, 2, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>$a = 10$</td>
<td>1, 10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 11$</td>
<td>1, 11, 2, 5, 4, 10, 8, 3, 16, 6, 15, 12, 13, 7, 9, 14, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 12$</td>
<td>1, 12, 8, 11, 13, 3, 2, 7, 16, 5, 9, 6, 4, 14, 15, 10, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 13$</td>
<td>1, 13, 16, 4, 1, ...</td>
<td>$p = 4$</td>
</tr>
<tr>
<td>$a = 14$</td>
<td>1, 14, 9, 7, 13, 12, 15, 6, 16, 3, 8, 10, 4, 5, 2, 11, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>$a = 15$</td>
<td>1, 15, 4, 9, 16, 2, 13, 8, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>$a = 16$</td>
<td>1, 16, 1, ...</td>
<td>$p = 2$</td>
</tr>
</tbody>
</table>
Fermat’s little theorem states that if $p$ is a prime which does not divide $a$, then $a^{p-1} \mod p = 1$.

$$x_{m-1} = (a^{m-1} \mod m)x_0 \mod m = x_0$$

**Theorem (2.1.2)**

If $x_0 \in \mathcal{X}_m$ and the sequence $x_0, x_1, x_2 \ldots$ is produced by a Lehmer generator with multiplier $a$ and (prime) modulus $m$ then:

- $\exists p \in \mathbb{Z}^+ \text{ with } p \leq m - 1 \mid x_0, x_1, \ldots, x_{p-1}$ are all different
- $x_{i+p} = x_i \quad i = 0, 1, 2, \ldots$

That is, the sequence is periodic with fundamental period $p$.

In addition $(m - 1) \mod p = 0$. 
Full-Period Multipliers

- Pick any initial seed $x_0 \in \mathcal{X}_m$ and generate $x_0, x_1, x_2, \ldots$ $\implies x_0$ will reappear
- $x_0$ reappears at index $p$ and either
  - $p = m - 1$ or $p \mid m - 1$
- The pattern will repeat forever
- Want full-period multipliers where $p = m - 1$
Full-period multipliers generate a virtual *circular list* with \( m - 1 \) distinct elements.
## Full-Period Multipliers for $m = 17$

<table>
<thead>
<tr>
<th>a</th>
<th>sequence</th>
<th>period</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1, 2, 4, 8, 16, 15, 13, 9, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>3</td>
<td>1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>4</td>
<td>1, 4, 16, 13, 1, ...</td>
<td>$p = 4$</td>
</tr>
<tr>
<td>5</td>
<td>1, 5, 8, 6, 13, 14, 2, 10, 16, 12, 9, 11, 4, 3, 15, 7, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>6</td>
<td>1, 6, 2, 12, 4, 7, 8, 14, 16, 11, 15, 5, 13, 10, 9, 3, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>7</td>
<td>1, 7, 15, 3, 4, 11, 9, 12, 16, 10, 2, 14, 13, 6, 8, 5, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>8</td>
<td>1, 8, 13, 2, 16, 9, 4, 15, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>9</td>
<td>1, 9, 13, 15, 16, 8, 4, 2, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>10</td>
<td>1, 10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>11</td>
<td>1, 11, 2, 5, 4, 10, 8, 3, 16, 6, 15, 12, 13, 7, 9, 14, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>12</td>
<td>1, 12, 8, 11, 13, 3, 2, 7, 16, 5, 9, 6, 4, 14, 15, 10, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>13</td>
<td>1, 13, 16, 4, 1, ...</td>
<td>$p = 4$</td>
</tr>
<tr>
<td>14</td>
<td>1, 14, 9, 7, 13, 12, 15, 6, 16, 3, 8, 10, 4, 5, 2, 11, 1, ...</td>
<td>$p = 16$</td>
</tr>
<tr>
<td>15</td>
<td>1, 15, 4, 9, 16, 2, 13, 8, 1, ...</td>
<td>$p = 8$</td>
</tr>
<tr>
<td>16</td>
<td>1, 16, 1, ...</td>
<td>$p = 2$</td>
</tr>
</tbody>
</table>
Algorithm to find full-period multipliers?
Algorithm 2.1.1

\[ p = 1; \]
\[ x = a; \]
\[ \text{while } (x \neq 1) \{ \]
\[ \quad p++; \]
\[ \quad x = (a \times x) \mod m; \quad \text{/* beware of } a \times x \text{ overflow */} \]
\[ \} \]
\[ \text{if}(p == m - 1) \]
\[ \quad \text{/* } a \text{ is a full-period multiplier */} \]
\[ \text{else} \]
\[ \quad \text{/* } a \text{ is not a full-period multiplier */} \]

- Slow-but-sure way to test for a full-period multiplier
Given prime modulus $m$, how many corresponding FPMs?

**Theorem (2.1.3)**

If $m$ is prime and $p_1, p_2, \ldots, p_r$ are the (unique) prime factors of $m - 1$ then the number of full-period multipliers in $\mathcal{X}_m$ is

$$\frac{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)}{p_1 p_2 \cdots p_r} (m - 1)$$

- Find number of FPMs for $m = 17, 19, 23, 29, 31$
If \( m = 2^{31} - 1 = 2 \, 147 \, 483 \, 647 \), then the prime decomposition of \( m - 1 \) is

\[
m - 1 = 2^{31} - 2 = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331
\]

and the number of FPMs is

\[
\left( \frac{1 \cdot 2 \cdot 6 \cdot 10 \cdot 30 \cdot 150 \cdot 330}{2 \cdot 3 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331} \right) (2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331) = 534 \, 600 \, 000
\]

So, approximately 25% of the multipliers are full-period
Good news: find one FPM, can generate all others

**Theorem (2.1.4)**

If $a$ is any FPM relative to prime modulus $m$ then each of

$$a^i \mod m \in \mathcal{X}_m \quad i = 1, 2, 3, \ldots, m - 1$$

is also a FPM relative to $m$ if and only if $i$ and $m - 1$ are relatively prime (i.e., $\gcd(i, m - 1) = 1$)
Finding All Full-Period Multipliers

- Once one full-period multiplier has been found, then all others can be found in $O(m)$ time

**Algorithm 2.1.2**

\[
i = 1; \\
x = a; \\
\text{while } (x \neq 1) \{ \\
\quad \text{if}(\text{gcd}(i, m - 1) == 1) \\
\quad \quad /* a^i \text{ mod } m \text{ is a full-period multiplier}*/ \\
\quad \quad i++ \\
\quad x = (a \times x) \mod m; \quad /* \text{beware } a \times x \text{ overflow} */ \\
\}\]
If $m = 13$, there are 4 FPMs, and $a = 6$ is one.

Since 1, 5, 7, and 11 are relatively prime to $m - 1 = 12$

- $6^1 \mod 13 = 6$
- $6^5 \mod 13 = 2$
- $6^7 \mod 13 = 7$
- $6^{11} \mod 13 = 11$

Equivalently, if we knew $a = 2$ to be a FPM

- $2^1 \mod 13 = 2$
- $2^5 \mod 13 = 6$
- $2^7 \mod 13 = 11$
- $2^{11} \mod 13 = 7$
FPMs for $m = 2^{31} - 1$

- If $m = 2^{31} - 1$, there are 534 600 000 integers rel. prime to $m - 1$.
- The first first few are $i = 1, 5, 13, 17, 19$.
- $a = 7$ is a FPM relative to $m$, so

\[
\begin{align*}
7^1 \mod 2147483647 &= 7 \\
7^5 \mod 2147483647 &= 16807 \\
7^{13} \mod 2147483647 &= 252246292 \\
7^{17} \mod 2147483647 &= 52958638 \\
7^{19} \mod 2147483647 &= 447489615
\end{align*}
\]

are full-period multipliers relative to $m$
In-class Exercise

Let $m = 29$.

- How many corresponding FPMs are there?
- What is the lowest-value FPM?
- Using that FPM, use Alg 2.1.2 to find all others.
In-class Exercise

Let \( m = 29 \).

- How many corresponding FPMs are there?
  \[
  \frac{1 \cdot 3}{2 \cdot 7} (28) = 12
  \]

- What is the lowest-value FPM?
  *Fortunately, \( a = 2 \) is the first FPM…*

- Using that FPM, use Alg 2.1.2 to find all others.
  *The values of \( i \) rel. prime to \( m - 1 = 28 \) are*
  
  \[3, 5, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27\]

  *so, using R, the remaining FPMs are:*

  \[
  \text{> ival} = c(3,5,9,11,13,15,17,19,21,23,25,27) \\
  \text{> sort(2^ivals \%\% 29)} \\
  [1]  \ 3 \ 8 \ 10 \ 11 \ 14 \ 15 \ 17 \ 18 \ 19 \ 21 \ 26 \ 27
  \]