Simple Pseudo Random Number Generator

Want a PRNG to exhibit full period.

\[
\begin{array}{c}
\text{Tail} \xrightarrow{} \text{Cycle Length} \\
\hline
\text{Period}
\end{array}
\]

(I usually assume cycle = period)

Linear Congruent Generator (LCG)

Congruence is a kind of equivalence.

If 2 numbers \( b + c \) have the property that \( b - c \) is integrally divisible by a number \( m \) (i.e., \( (b - c)/m \) is an integer) then \( b + c \) are congruent modulo \( m \).

\[ b \equiv c \pmod{m} \]

Ex: \( 17 \equiv 6 \pmod{11} \)
mixed Linear Congruent Generator

\[ Z_n = (a \cdot Z_{n-1} + c) \mod m \]
\[ Z_0 = \text{the seed} \]

\[ m: \text{modulus} \]
\[ a: \text{multiplier} \]
\[ c: \text{increment} \]

Lots of rules to ensure desirable properties such as:

\[ a \cdot m + c \]
\[ Z_n < m \]

0 \leq Z_n < m

To get this to be a \( U_n \) normalize

\[ U_n = Z_n / m \]
Consider a mixed LCG defined by

\[ m = 16 \quad c = 5 \quad c = 3 \quad z_0 = 7 \]

\[ z_n = 5(z_{n-1} + 3) \mod 16 \]

\[ u_n = z_n / 16 \]

<table>
<thead>
<tr>
<th>Period</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( z_n )</td>
<td>7</td>
<td>16</td>
<td>1</td>
<td>8</td>
<td>11</td>
<td>10</td>
<td>5</td>
<td>15</td>
<td>14</td>
<td>9</td>
<td>10</td>
<td>9</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>13</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>( u_n )</td>
<td></td>
<td>0.375</td>
<td>0.063</td>
<td>0.50</td>
<td>0.682</td>
<td>0.625</td>
<td>0.313</td>
<td>0.750</td>
<td>0.938</td>
<td>0.875</td>
<td>0.563</td>
<td>0.0</td>
<td>0.188</td>
<td>0.125</td>
<td>0.843</td>
<td>0.025</td>
<td>0.438</td>
<td></td>
</tr>
</tbody>
</table>

The modulus controls how dense the \( u_i \) are in the interval \([0, 1]\).

The \( u_i \) can only take on the rational values \( 0, \frac{1}{m}, \frac{2}{m}, \ldots, \frac{m-1}{m} \).
Given an exponential RV

Continued, \( S_x \in [0, \infty] \)

\( f_x(x) = \frac{1}{2} e^{-\frac{x}{2}}, \quad x \geq 0, \quad 2 > 0 \)

CDF: \( F_x(x) = \begin{cases} 0 & x < 0 \medskip \vspace{2mm} \text{F(x)} \vspace{2mm} \end{cases} 1 - e^{-\frac{x}{2}}, \quad x \geq 0 \)

Inverse Transform Method

\[ u = U(0,1) \]

\[ u = F(x) + \text{solve for } x \]

Call \( B = \frac{1}{2} \)

(mean)

\[ u = 1 - e^{-\frac{x}{B}} \quad 1 - u = e^{-\frac{x}{B}} \]

\[ 2 \ln(1 - u) = -\frac{x}{B} \quad x = -B \ln(1 - u) \]

Trick: \( \frac{u}{(0,1)} = \frac{1 - u}{(1,0)} \) so we can substitute \( u \) by \( 1 - u \)

\[ x = -B \ln(u) \]

See also: inline double exponential

\[
\text{inline double exponential } \{
\text{ return } -\log (\text{uniform}()) \};
\]

\[
\text{inline double exponential (double) } \{
\text{ return } (u + \text{exponential}) \};
\]
Inverse Transform Method
For generating Random Variables

1) Generate a \( U \), \( U \sim U(0,1) \)

2) Find the inverse of the RV's CDF \( F_X \) using \( X = U \)

Remember:
- \( F_X(x) = P(X \leq x) \)
- Assumes \( F_X(x) \) is invertible

\[ X = F_X^{-1}(U) \]