Random Numbers

> *A random sequence is a vague notion ... in which each term is unpredictable to the uninitiated and whose digits pass a certain number of tests traditional with statisticians ...*

Uniform distribution

$$x_{k+1} = ax_k + c \text{ mod } m$$

$a = 13$, $c = 0$, $m = 31$, $x_0 = 1$

1, 13, 14, 27, 10, 6, 16, 22, 7, 29, 5, 3, ...

Divide by m

0.0323, 0.4194, 0.4516, 0.8710, 0.3226, 0.1935, 0.5161, ...

`randu`. IBM SSP.

$$
\begin{aligned}
a &= 65539 \\
c &= 0 \\
m &= 2^{31}
\end{aligned}
$$

The following are mod 2^{31}

$$
\begin{aligned}
x_{k+2} &= (2^{16}+3)x_{k+1} = (2^{16}+3)^2 x_k \\
&= (2^{32} + 6 \cdot 2^{16} + 9)x_k \\
&= [6 \cdot (2^{16}+3) - 9]x_k
\end{aligned}
$$

$$x_{k+2} = 6x_{k+1} - 9x_k, \quad \text{for all } k$$

`randu`. MATLAB before V5.

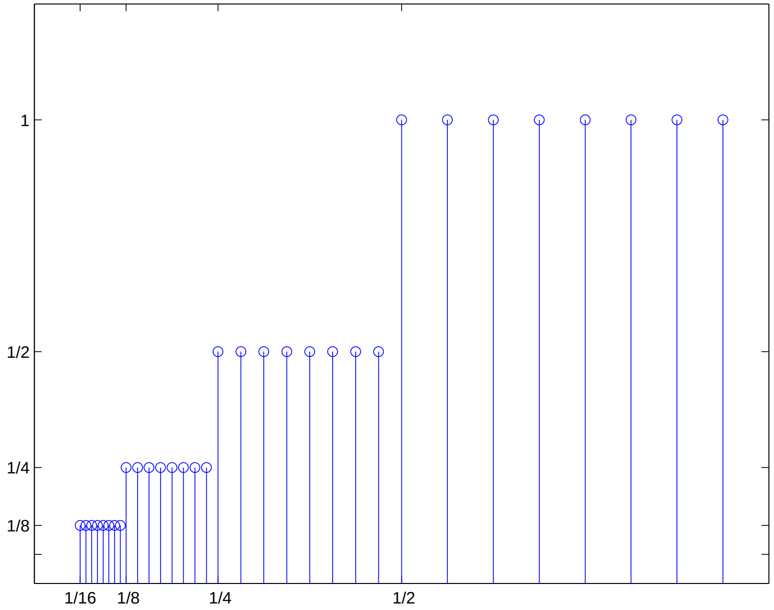
$$\begin{aligned} a &= 7^5 = 16807 \\ c &= 0 \\ m &= 2^{31} - 1 = 2147483647 \end{aligned}$$

George Marsaglia

Thirty-two words form a cache of floating-point numbers z, between 0 and 1.

$$z_i = z_{i+20} - z_{i+5} - b$$

i, $i + 20$, and $i + 5$, mod 32



The period of the new generator is 2^{1492}.

Normal Distribution

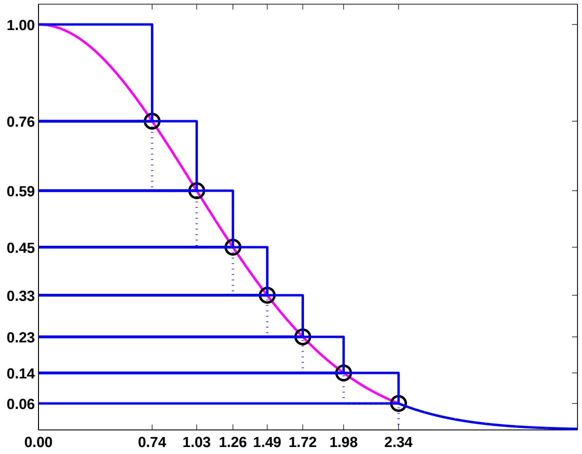
```
    sum(rand(m,n,12),3) - 6
```

polar algorithm

```
r = Inf;
while r > 1
   u = 2*rand(2,1)-1
   r = u'*u
end

v = sqrt(-2*log(r)/r)*u
```

ziggurat



```
j = ceil(128*rand);
u = 2*rand-1;
if abs(u) < sigma(j)
   r = u*z(j);
else
   r = randntips(...)
end
```

randtx

```
U = zeros(m,n);
for k = 1:m*n
   x = z(mod(i+20,32)+1) - z(mod(i+5,32)+1) - b;
   if x < 0
      x = x + 1;
      b = ulp;
   else
      b = 0;
   end
   z(i+1) = x;
   i = i+1;
   if i == 32, i = 0; end
   [x,j] = randbits(x,j);
   U(k) = x;
end
```

randntx

```
R = zeros(m,n);
for k = 1:m*n
   [u,j] = randuni;
   rk = u*z(j+1);
   if abs(rk) < z(j)
      R(k) = rk;
   else
      R(k) = randntips(rk,j,z);
   end
end
```