Linear Congruential Method

$X_{n+1} = (aX_n + c) \bmod m$

Examples

1. Consider a = c = 1.
The sequence produced is obviously not satisfactory.

2. Consider a = 7, c = 0, m = 32, and X0 = 1.

This generates the sequence {7, 17, 23, 1, 7, etc.}, which is also clearly unsatisfactory. Of the 32 possible values, only four are used; thus, the sequence is said to have a period of 4.

3. If, instead, we change the value of a to 5, then the sequence is {5, 25, 29, 17, 21, 9, 13, 1, 5, etc.}, which increases the period to 8.

Blub Blub Shub

The procedure is as follows.

1. First, choose two large prime numbers, *p* and *q*, that both have a remainder of 3 when divided by 4. That is,

$p = q = 3 \pmod 4$ it means ($p \bmod 4$) = ($q \bmod 4$) = 3.

For example, prime numbers 7 and 11 satisfy $7 = 11 = 3 \pmod 4$.

2. Let $n = p * q$.

3. Next, choose a random number *s*, such that *s* is relatively prime to *n*; this is equivalent to saying that neither *p* nor *q* is a factor of *s*.