With c=0, one cannot get the full period, but in order to get the maximum possible, the following should be satisfied:

i) I_0 is relatively prime to m
ii) a is a primative element modulo m

It is possible to obtain a period of length m-1, but usually the period is around m/4.

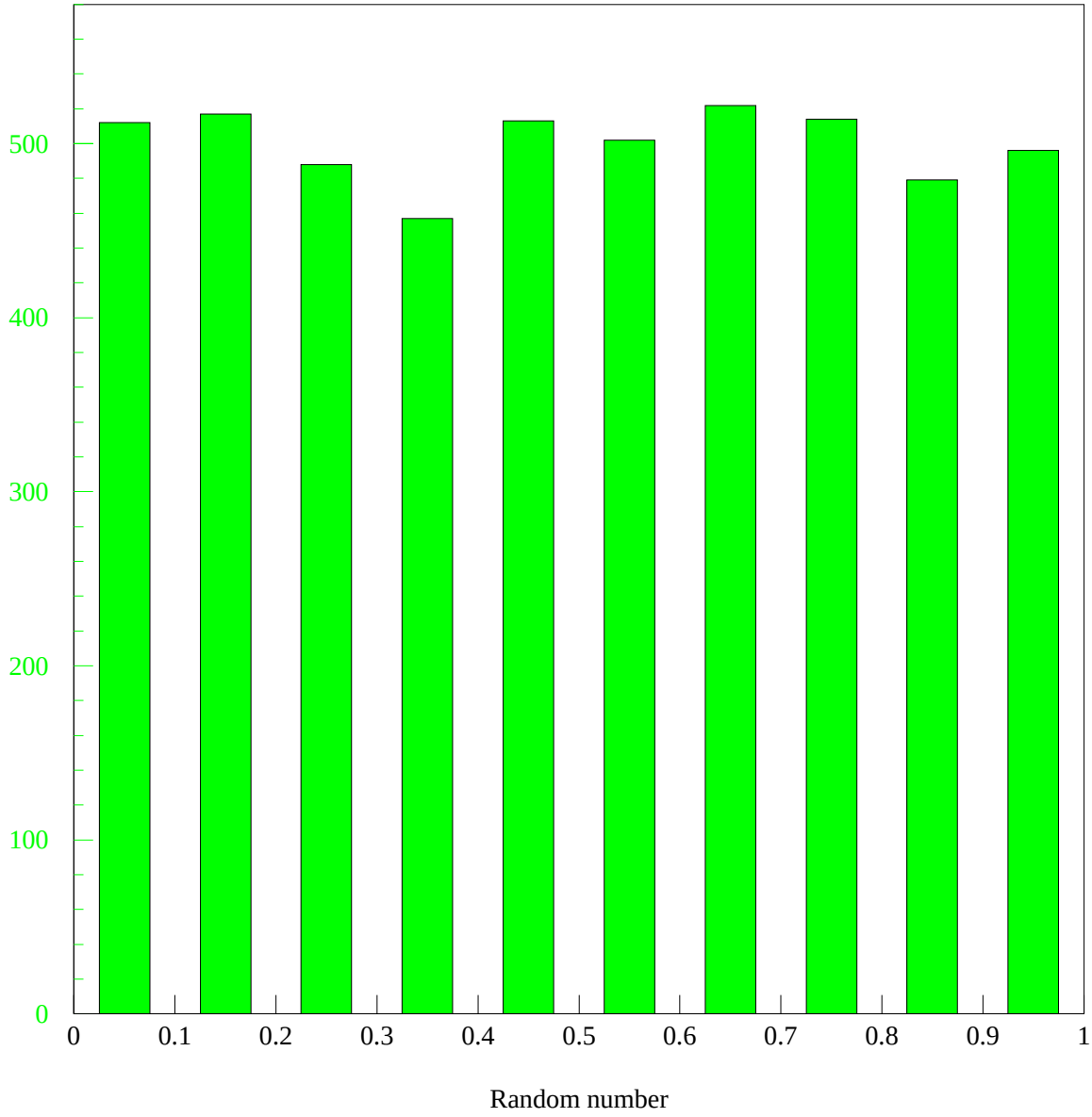
RANDU generator

A popular random number generator was distributed by IBM in the 1960's with the algorithm:

$$I_{n+1} = (65539 \times I_n) \bmod 2^{31}$$

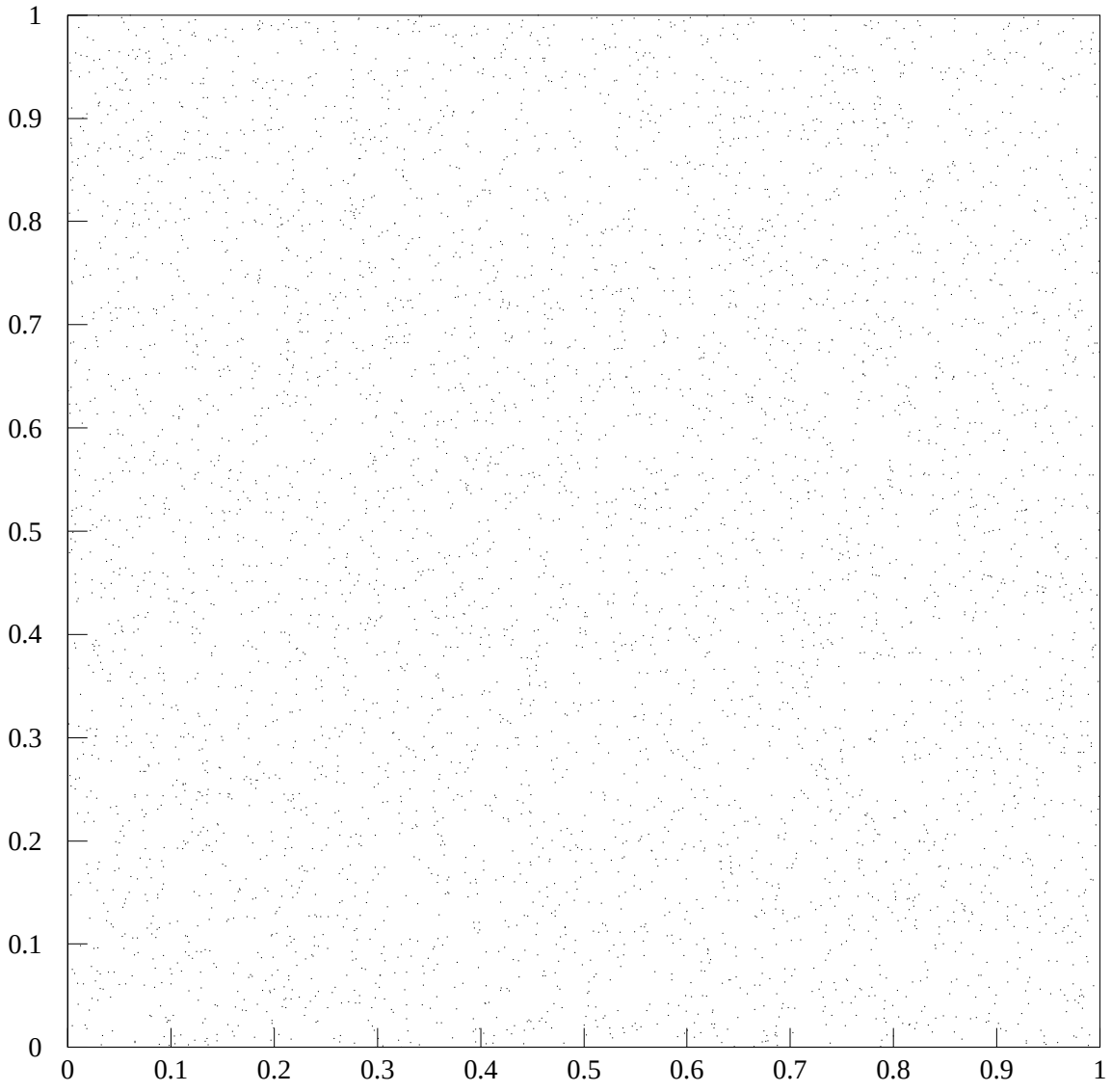
This generator was later found to have a serious problem...

Results from Randu: 1D distribution



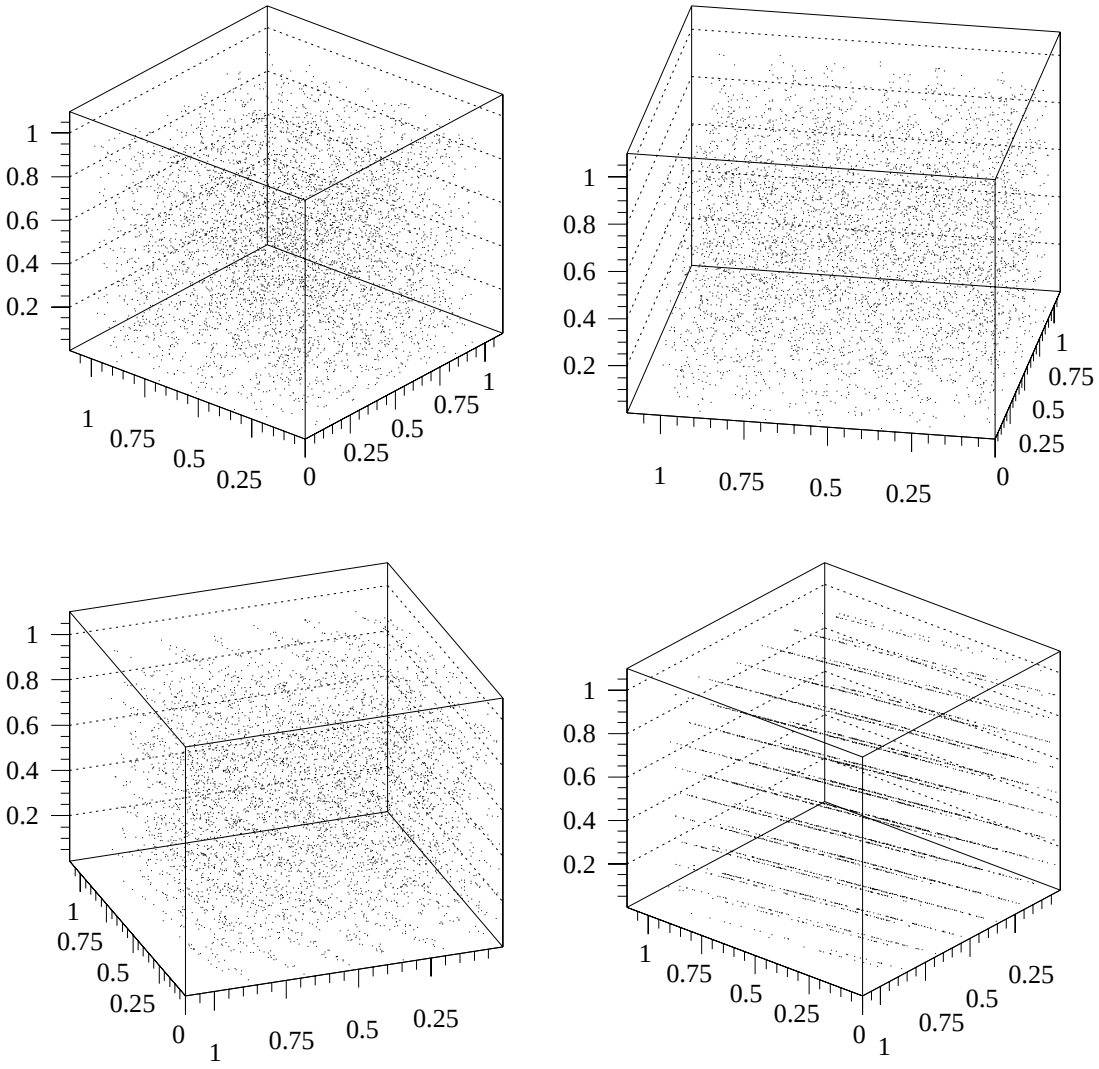
Looks okay

Results from Randu: 2D distribution



Still looks okay

Results from Randu: 3D distribution



Problem seen when observed at the right angle!