

# Python Programming @ The department of Computer Science



## Random Number Generator

### Background

To generate sequence of random numbers a common equation used is:

$$N_{i+1} = (K \times N_i) \% M$$

where  $K$  and  $M$  are constants,  $N_i$  is the current term (random number) and  $N_{i+1}$  is the following term (remember  $\%$  is the modulo operator).

The equation requires a start term ( $N_0$ ), often referred to as the *seed*, after which subsequent terms can be generated. To ensure realistic operation of the equation appropriate values for  $K$  and  $M$  are required.

It is suggested that:  $K=5^5=3125$  and  $M=2^{13}=8192$ ; and a seed with an odd number value within the range of  $1..M-1$  (i.e.  $1..8191$ ) be used.

### Requirements

Write a Python programme that generates and outputs a sequence of five random numbers starting with a seed input by the user. Use  $K=3125$  and  $M=8192$  as suggested.

Remember, by convention we variable names for constants are written in upper case.

### Example

Seed ( $N_0$ ) = 11

$$N_1 = (3125 \times N_0) \% 8192 = 1607$$

$$N_2 = (3125 \times N_1) \% 8192 = 179$$

$$N_3 = (3125 \times N_2) \% 8192 = 2319$$

$$N_4 = (3125 \times N_3) \% 8192 = 5147$$

$$N_5 = (3125 \times N_4) \% 8192 = 3479$$

### Alternatives

Try using different seed values.

See what happens when  $K=5$ ,  $M=4$  and  $N_0=3$ !

Using the above will produce a series of "random" numbers within the range of 1 and 8191. If we wished to produce random numbers between say  $0..100$  or  $0..10$  or  $0..1$  we would have to apply appropriate corrections:

$100/M$       or       $10/M$       or       $1/M$



[1] Figure from <https://spin.atomicobject.com/2012/08/09/rspec-thank-you-for-running-my-tests-in-random-order/> (sampled 24 September 2016)