# Assignment 6

***Due: 1 April.***

## 1 Pseudorandom number generators with linear structures

(*30 Points*) Visit *http://random.mat.sbg.ac.at/results/karl/server/*, choose one linear pseudorandom number generator and implement your own version of it in Python. Describe, briefly, its properties.

## 2 LCG Full Period Condition

(*20 Points*) Use the following theorem

**Theorem 1.** *An LCG has full period if and only if the following three conditions hold:*
*1. The only positive integer that (exactly) divides both m and c is 1 (i.e., c and m have no common factors other than* 1*).*
*2. If q is a prime number that divides m then q should divide* $(a-1)$ *(i.e.,* $(a-1)$ *is a multiple of every prime number that divides m).*
*3. If* 4 *divides m, then* 4 *should divide* $(a-1)$ *(i.e.,* $(a-1)$ *is a multiple of* 4 *if m is a multiple of* 4*).*

to check if the following LCGs

- $(m = 9, a = 3, c = 2, x_0 = 1)$
- $(m = 8, a = 5, c = 1, x_0 = 5)$

reaches its full period.