## Assignment 5



## 1 Monte Carlo Integration

• (15 Points) Some integrands are unbounded and yet their integrals exist. Evaluate the integrals

$$\int_0^1 \frac{dx}{\sqrt{x}}$$

and

$$\int_0^1 \frac{\sin\left(x\right)}{\sqrt{1-x}} dx,$$

using the Monte Carlo methdo. Estimate the accuracy of your results for different sample sizes.

## 2 Pseudorandom number generators with linear structures

- (15 Points) Crack, i.e., find  $(m, a, c, x_0)$ , the following sequence<sup>1</sup>:
  - [61., 262., 151., 304., 785., 122., 427., 228., 613., 110., 831., 280., 569., 226., 339., 460., 653., 470., 999., 768.]

Provide the code used.

• (20 Points) Together with this assignment you will find a sequence of 100.000 numbers ("Sequence.txt") generated with the brand new PPP algorithm. Your task will be to test if the algorithm passes the  $\chi^2$  Test.

<sup>&</sup>lt;sup>1</sup>Hint: In "Marsaglia, G. (2003). Random number generators. Journal of Modern Applied Statistical Methods, 2(1), 2.", Marsaglia describes an algorithm for identifying and cracking a PRNG based on a congruential generator. The attack determines the modulo *m* of the LCG by finding the greatest common divisor (GCD) of the volumes of parallelepipeds described by vectors taken from the LCG sequence. You may find that useful.