1 Introduction

Random numbers have a long history. In the acient world, dices are the most popular instrument to generate them that the oldest dices were discovered in a 24th century B.C. tomb in the Middle East. Meanwhile, the crack of heated turtle shell was regarded as another random number in ancient China. Nowadays, Lottery machines are typical random number generators.

All mentioned above are true random numbers, which are taken from physical factors. In this way people can get perfect distributed random numbers. However, as people's need for random number increases, the disadvantages of true ones become obvious. They need extra hardwares and the generating speed is relatively slow since numbers should be taken from hardware values. Moreover, they are surely not reproducible.

For disadvantages above, the idea of pseudorandom numbers are promoted. They are produced with a pseudorandom number generator(PRNG), which is a kind of algorithm. If a random number as a seed is input, a generator can produce a sequence of numbers that can be nearly seen as random ones. This way is efficient and doesn't need any devices. Meanwhile, it is replicable if the seed is available.

In this report, we will focus on the pseudorandom numbers generators and some ways to test their randomness.

2 Theorem

2.1 Principle of PRNG

A pseudorandom number generator, or PRNG, is any program, or function, which uses math to simulate randomness. The math can sometimes be complex, but in general, using a PRNG requires only two steps:

1. Provide the PRNG with an arbitrary seed.

2. Ask for the next random number.

Let $f(x)$ be a function as a PRNG. Take x_0 arbitrarily as a seed. Then