SOLUTION FOR HOMEWORK ASSIGNMENT NO. 04

Nils Hoyer, Maurice Morgenthaler

Exercise 4.1

We are asked to write our own pseudo random number generator. For this we will use the so called *Blum Blum Shub* generator which uses the equation

$$n_{i+1} = n_i^2 \ \% \ (p \cdot q) \tag{1}$$

to generate new numbers. p and q are large prime numbers.

To generate numbers between zero and one one has to divide by $p \cdot q$.

$$r_i = \frac{n_i}{M} \tag{2}$$

Please find the code in file `exercise4_1.C`. The 20th 'random' numbers of consecitive seeds are listed in table 1. Just by only looking at the twenty numbers below I can not see any correlation.

Table 1: The last twenty random numbers are listed given twenty consecutive seeds starting at 234 509 143.

seed i	**random number** r_i
234 509 143	0.389 45
234 509 144	0.052 98
234 509 145	0.555 13
234 509 146	0.310 14
234 509 147	0.828 52
234 509 148	0.539 09
234 509 149	0.419 62
234 509 150	0.100 40
234 509 151	0.153 32
234 509 152	0.457 29
234 509 153	0.530 53
234 509 154	0.474 94
234 509 155	0.014 97
234 509 156	0.325 98
234 509 157	0.905 85
234 509 158	0.014 88
234 509 159	0.683 29
234 509 160	0.253 34
234 509 161	0.463 13
234 509 162	0.903 14

Next we used the first seed to generate 10 000 random numbers. We filled a histogram with them which you

can see in figure 1.

Figure 1: 10 000 random number generated by our own random number generator. The seed which has been used is 234 509 143. We used 200 bins for plotting in the range between zero and one.
Note that the rather large differences in amounts of numbers persists even to higher total numbers of generated 'random' numbers (e.g. 1 000 000).