PseudoRandom Number Generator
Shafeek Zakko
KTH | IV1013

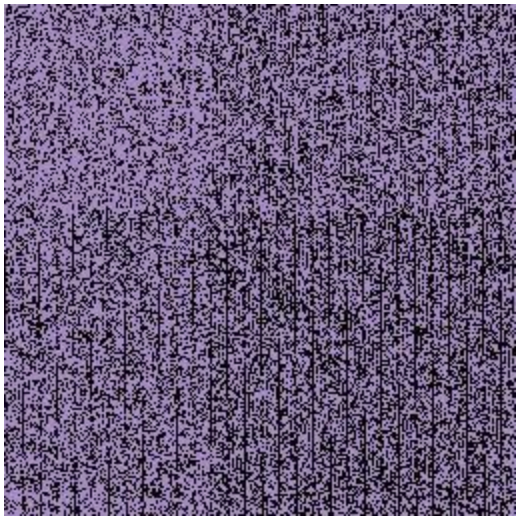
The pseudo random number generator was designed as Linear congruential generator (LCG) To maximize the period of this generator, m is chosen as a prime = 9462857623 and x_0 = 123 is selected as a primitive root to the prime m. This gives us a maximum period for the linear generator which is = m - 1. The variable c = 76135 is selected arbitrarily because it does not affect the statistical results.

$$X_{n+1} = (a\ X_n + c)\ b \bmod m$$

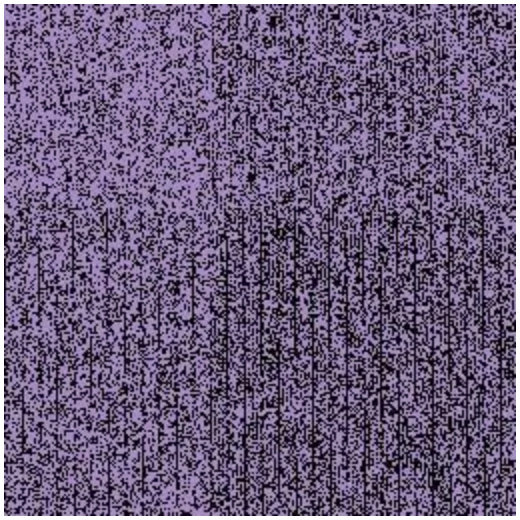
Four samples were generated for our report by creating four bitmaps of size 256*256, by filling randomly selected pixels of these bitmaps with white color (black pixeles for off and white for on). These pixels were selected for the first two bitmaps image by traversing through 265*265 pixels that were picked using the PseudoRandom Number Generator that was created in the second task, once with seed = 9345254 and once with seed = 5. Second two images were generated by doing the same procedure but using the standard library Random class provided by Java, also with the two seeds 9345254 and 5.

Looking at the first two images we can see a clear pattern where some columns in the bitmap were completely not selected by the generator. Another distinguished pattern is that most of the selected pixels were in the first quarter of the image, that is the upper left square of the bitmaps where the white pixels are more dominating as well as having a lighter shade of white (got selected more than once). At the same time the lower right square of the images was observed as having more black pixels. By comparing these with the bitmaps generated with the standard library Random class, we see a more random pattern and that white pixels are scattered with no specific pattern. This shows that the randomized numbers are more evenly distributed in the selected interval between [0 - 255].

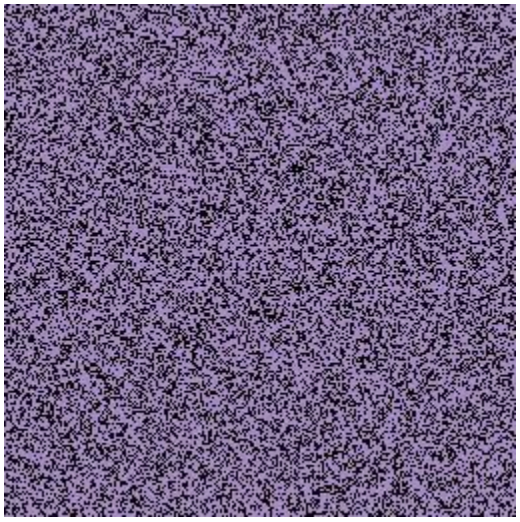
By choosing (a) in our algorithm as a bigger integer than the previously selected a = 123, the columns pattern disappeared but the squares one remind slightly visible.



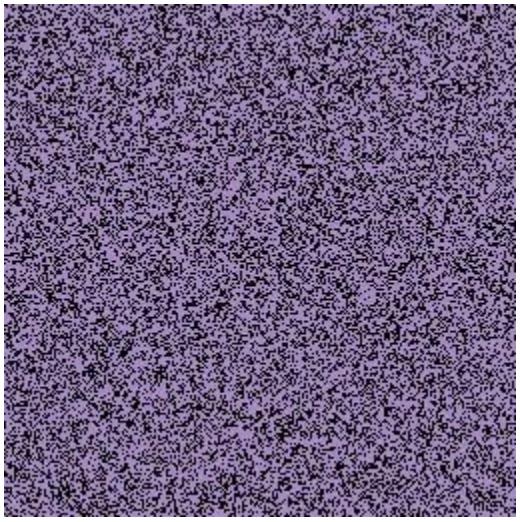
MyRandom with seed = 9345254



MyRandom with seed = 5



Random with seed = 9345254



Random with seed = 5