Cubic congruential generator (CCG)

January 9, 2022

A given pseudo-random number generator is given by a formula:

$$x_{i+1} = 2x_i^3 \quad mod \quad M$$

Where M is given modulus

1 Input

In order to turn on the generator, given parameters must be given:

- –n is number of numbers we want to generate (default=1000);
- –M is given modulus (default=634386549);
- –a an optional parameter to modify the given recursive pattern (default=2);
- –output-file name of pickle file where generated number will be saved. If such a file already exists it will be replaced (default="generated-numbers.pkl");
- –seeds a csv file that stores different seed values, The seed file should have the word "seeds" on the first line and every line should contain only one seed. As we are dealing with a cubic generator. the seeds cannot be too large, as the generated numbers will not be interpreted by python;
- –output-dir directory where files with generated numbers are to be saved,the file must exist before starting the program

If seeds is empty, we just save the files to output-dir / output-file

2 Output

Creates files (quantity depending on the number of seeds given) with the generated numbers. They will be saved to a previously prepared folder or saved automatically if there is only one seed . Each plk file contains information about how it was generated, modulus and number of numbers

3 Example

```
python 4ccg_generator.py --seeds sample_seeds.csv --output-
file my_gen_nubmers.plk --output-dir results_sample

python 4ccg_generator.py --seeds --a 3 sample_seeds.csv --output-
file my_gen_nubmers.plk --output-dir results_sample

python 4ccg_generator.py --n 100 --M 34 --seeds sample_seeds.csv
--output-file my_gen_nubmers.plk --output-dir results_sample
```