Metody Probabilistyczne i Statystyka

Zadanie domowe 3

Arina Lazarenko

257259

Zadanie 1 (Testy NIST)

- słaby generator liczb losowych

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.8212014203279661	Passed
2. Frequency Test within a Block	0.38232523884681685	Passed
3. Runs Test	1.7712336155758526	Failed
4. Test for the Longest Run of Ones in a Block	0.48152178448416894	Passed
5. Binary Matrix Rank Test	0.40399103016220805	Passed
6. Non-overlapping Template Matching Test	0.4264255379584908	Passed
7. Overlapping Template Matching Test	0.2531156403851712	Passed
8. Maurer's "Universal Statistical" Test	0.4038269121400919	Passed
9. Linear Complexity Test	0.21796974086852366	Passed
10. Serial Test	P-value 1: 0.48132623285233855 P-value 2: 0.234833447710184	Passed
11. Approximate Entropy Test	0.09287263700511576	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.5272163770886866 P-value Reverse: 1	Passed
13. Random Excursions Test	0.021566348721240504	Passed
14. Random Excursions Variant Test	0.0633941673048164	Passed

- dobry generato liczb losowych

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.6891565167793516	Passed
2. Frequency Test within a Block	0.7615885085482635	Passed
3. Runs Test	0.8055583478501485	Passed
4. Test for the Longest Run of Ones in a Block	0.5978793914725387	Passed
5. Binary Matrix Rank Test	0.442117885343669l4	Passed
6. Non-overlapping Template Matching Test	0.9450781777899219	Passed
7. Overlapping Template Matching Test	0.5060918859477542	Passed
8. Maurer's "Universal Statistical" Test	0.9584889867979294	Passed
9. Linear Complexity Test	0.3133741182793879	Passed
10. Serial Test	P-value 1: 0.8960419929572063 P-value 2: 0.8072308296564806	Passed
11. Approximate Entropy Test	0.0601588782691102	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.315854415012945 P-value Reverse: 1	Passed
13. Random Excursions Test	0.11827758171251951	Passed
14. Random Excursions Variant Test	0.11646701783569213	Passed

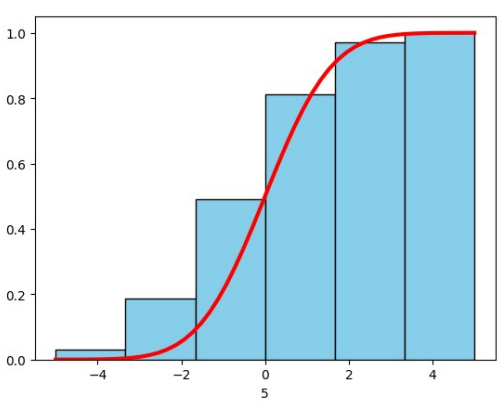
- SHA1 dla „Lazarenko”

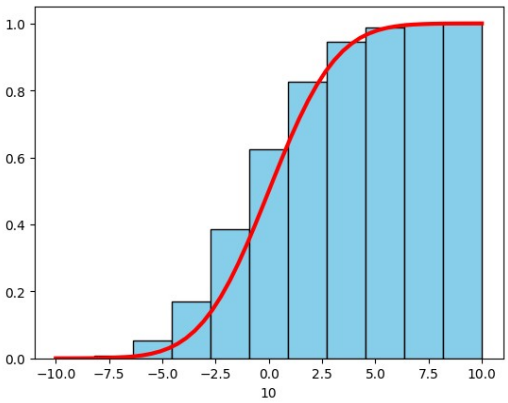
Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.8743670611628919	Passed
2. Frequency Test within a Block	0.5958831106435742	Passed
3. Runs Test	1.3633987675420585	Failed
4. Test for the Longest Run of Ones in a Block	0.6155021366433862	Passed
5. Binary Matrix Rank Test		Error
6. Non-overlapping Template Matching Test		Error
7. Overlapping Template Matching Test		Error
8. Maurer's "Universal Statistical" Test		Error
9. Linear Complexity Test		Error
10. Serial Test		Error
11. Approximate Entropy Test	0.17837744833600316	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.6040491568129147 P-value Reverse: 0.8754344246250818	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

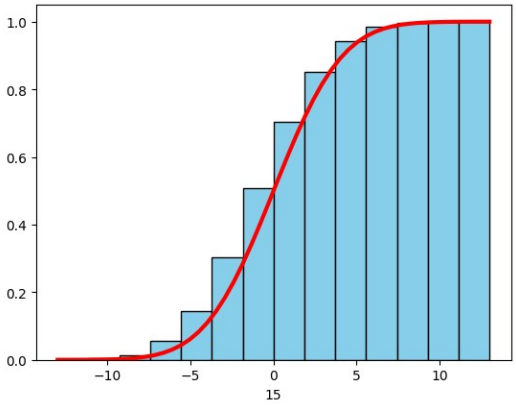
Wniosek:

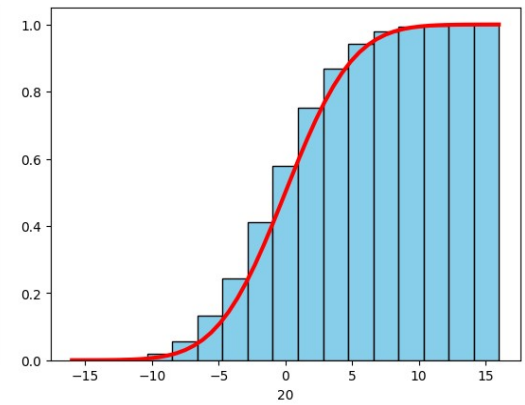
Możemy zobaczyć, że „słaby” generator liczb losowych nie przeszedł 3 test, natomiast „dobry” generator przeszedł go, widzimy również, że SHA1 przeszedł nie wszystkie testy, a na niektórych albo wystąpił błąd albo ich nie przeszedł. Spowodowano to jest zbyt małą ilością bitów do testów.

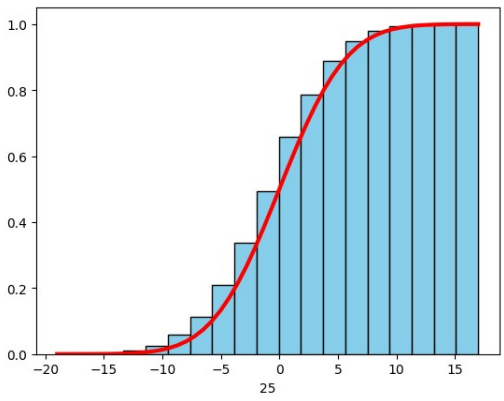
Zadanie 2 (Błądzenie losowe)

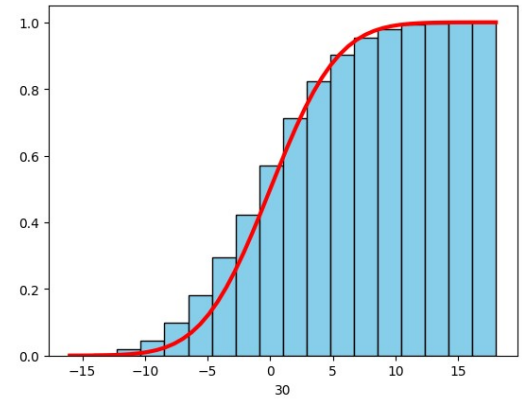


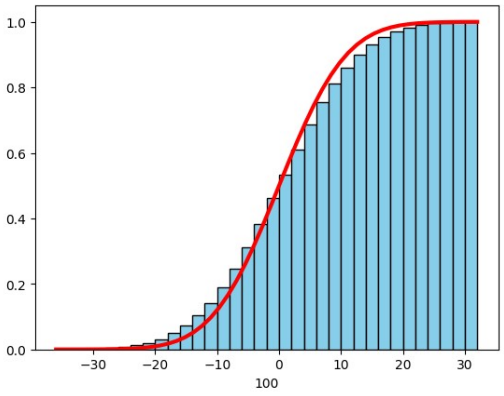








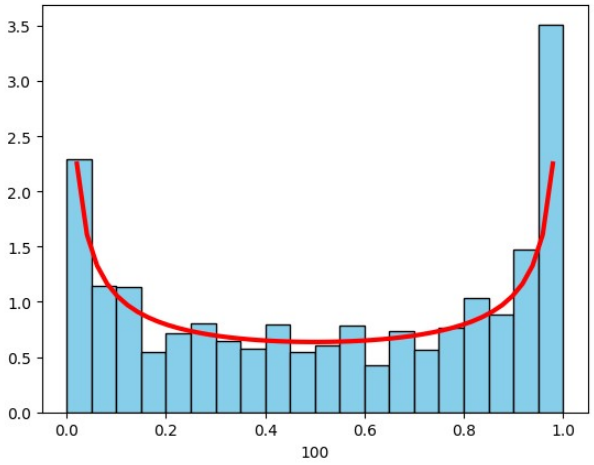


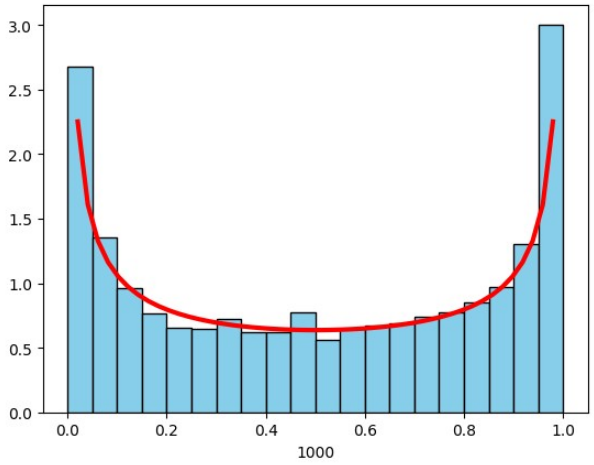


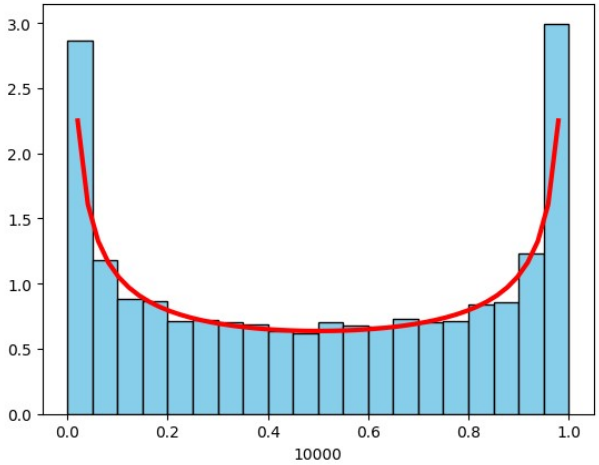
Wniosek:

Możemy zobaczyć, że aproksymacja rozkładem normalnym jest lepsza im zwiększa się N.

Zadanie 3 (Błądzenie losowe na Z – rozkład czasu nad osią OX)







Wniosek:

Patrząc na wykresy, możemy zaobserwować, że rozkład naszego eksperymentu ma właśnie rozkład arcsin, lub bardzo do niego podobny.