Zadanie 1

1. Wyniki dla „słabego” generatora liczb losowych (użyłem domyślnego generatora w Javie):

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.06815207223903264	Passed
2. Frequency Test within a Block	0.1330542921555414	Passed
3. Runs Test	1.1715374425036418	Failed
4. Test for the Longest Run of Ones in a Block	0.6025364304392342	Passed
5. Binary Matrix Rank Test	0.390237351440765	Passed
6. Non-overlapping Template Matching Test	0.2145611583816548	Passed
7. Overlapping Template Matching Test	0.11161804315700152	Passed
8. Maurer's "Universal Statistical" Test	0.1955762778454776	Passed
9. Linear Complexity Test	0.651061276565746	Passed
10. Serial Test	P-value 1: 0.18494662666651995 P-value 2: 0.8258711632011311	Passed
11. Approximate Entropy Test	0.4372978400431651	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.0658494520875017 P-value Reverse: 1	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

2. Wyniki dla „przyzwoitego” generatora liczb losowych (Mersenne Twister w Matlabie):

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.8461758819031635	Passed
2. Frequency Test within a Block	0.2847955405095816	Passed
3. Runs Test	0.6184575021000557	Passed
4. Test for the Longest Run of Ones in a Block	0.6709036819184635	Passed
5. Binary Matrix Rank Test	0.681141591591349	Passed
6. Non-overlapping Template Matching Test	0.6432365089100992	Passed
7. Overlapping Template Matching Test	0.6210279047584862	Passed
8. Maurer's "Universal Statistical" Test	0.10867132392720258	Passed
9. Linear Complexity Test	0.13212720407281195	Passed
10. Serial Test	P-value 1: 0.8677722357137979 P-value 2: 0.6198944297964206	Passed
11. Approximate Entropy Test	0.8633420762371384	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.9694947036014687 P-value Reverse: 0.9209589696135696	Passed
13. Random Excursions Test	0.06373239926697914	Passed
14. Random Excursions Variant Test	0.05132719775649197	Passed

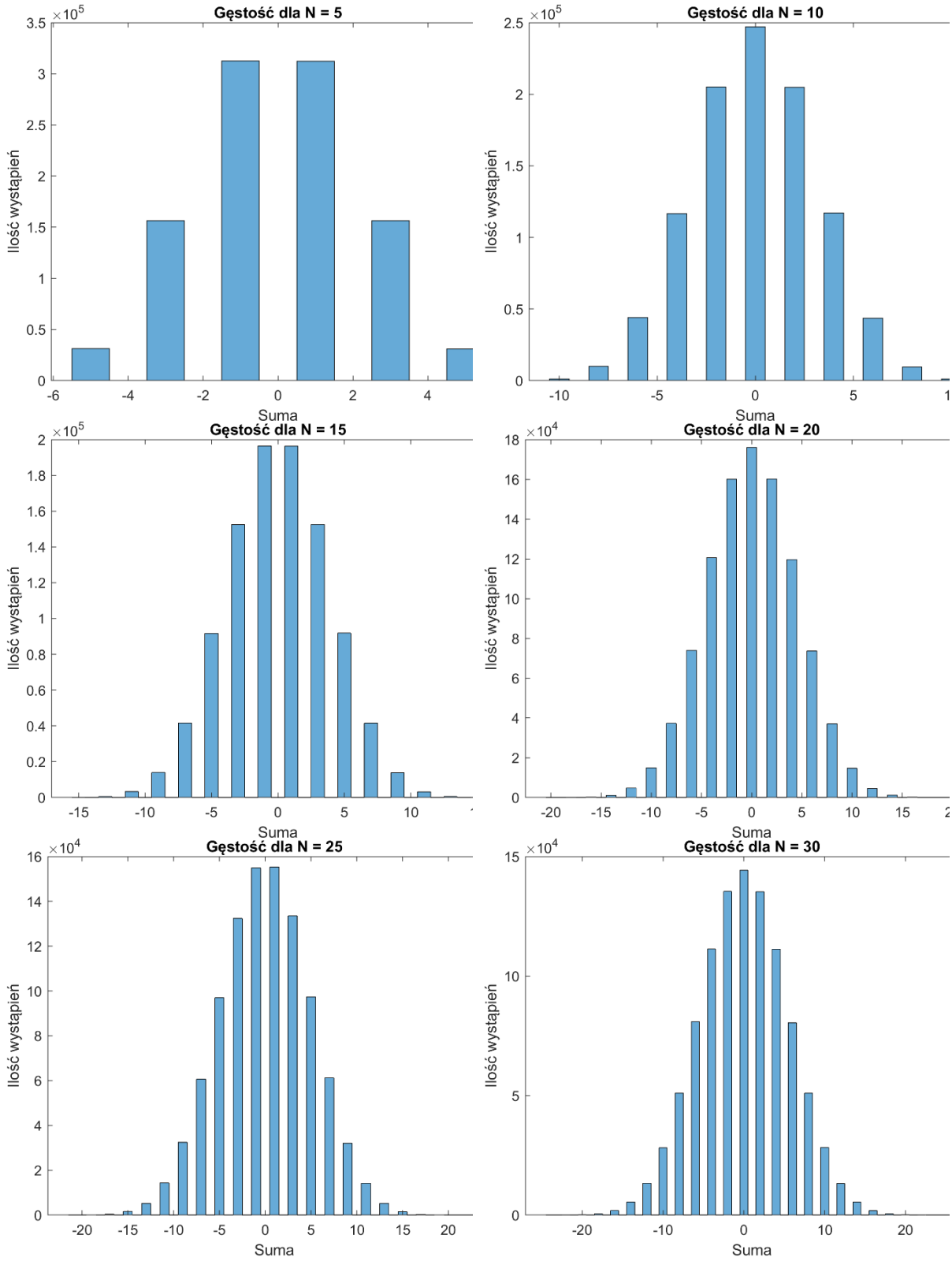
3. SHA-1 przekonwertowany na binarny:

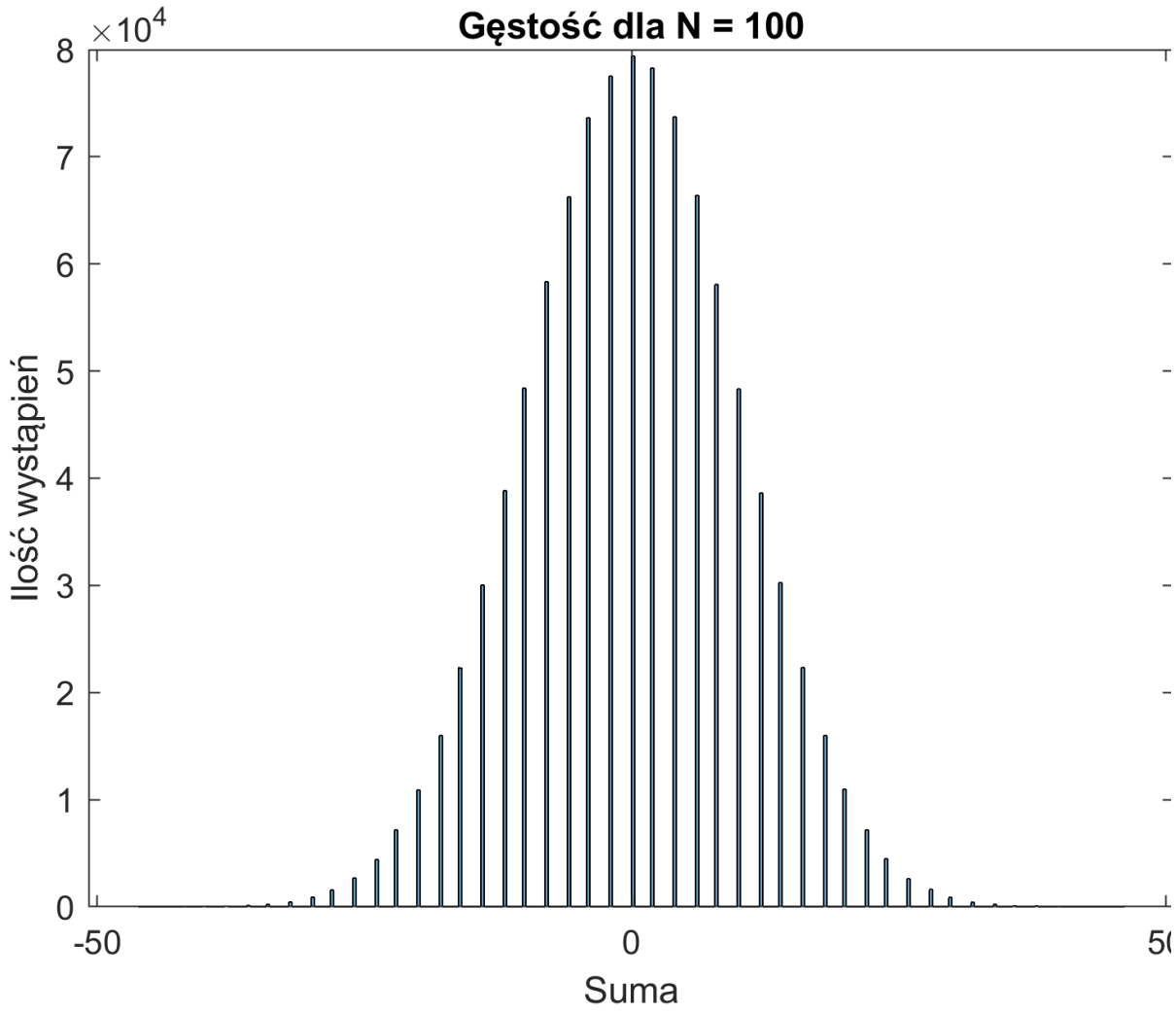
Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.6352562959972482	Passed
2. Frequency Test within a Block	0.37675914877707095	Passed
3. Runs Test	0.260094133057172	Passed
4. Test for the Longest Run of Ones in a Block	0.43971779444387715	Passed
5. Binary Matrix Rank Test		Error
6. 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	0.8674758610066466	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.7508688492501634 P-value Reverse: 0.8754344246250818	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

Zgodnie z oczekiwaniami najlepszy generator pomyślnie przeszedł wszystkie testy. SHA-1 przeszedł kilka testów ale z racji że był dosyć krótki (zdecydowanie krótszy niż zalecane przy niektórych testach milion bitów) to w pozostałych pojawiły się błędy. Zaskoczeniem może być że domyślny generator w Javie (biblioteka java.util) jest dość dobry – nie przeszedł tylko jednego testu i w dwóch zwrócił błąd jednak mimo przejścia testów jego wyniki są w większości (chociaż nie zawsze) gorsze niż w drugim przypadku.

Zadanie 2

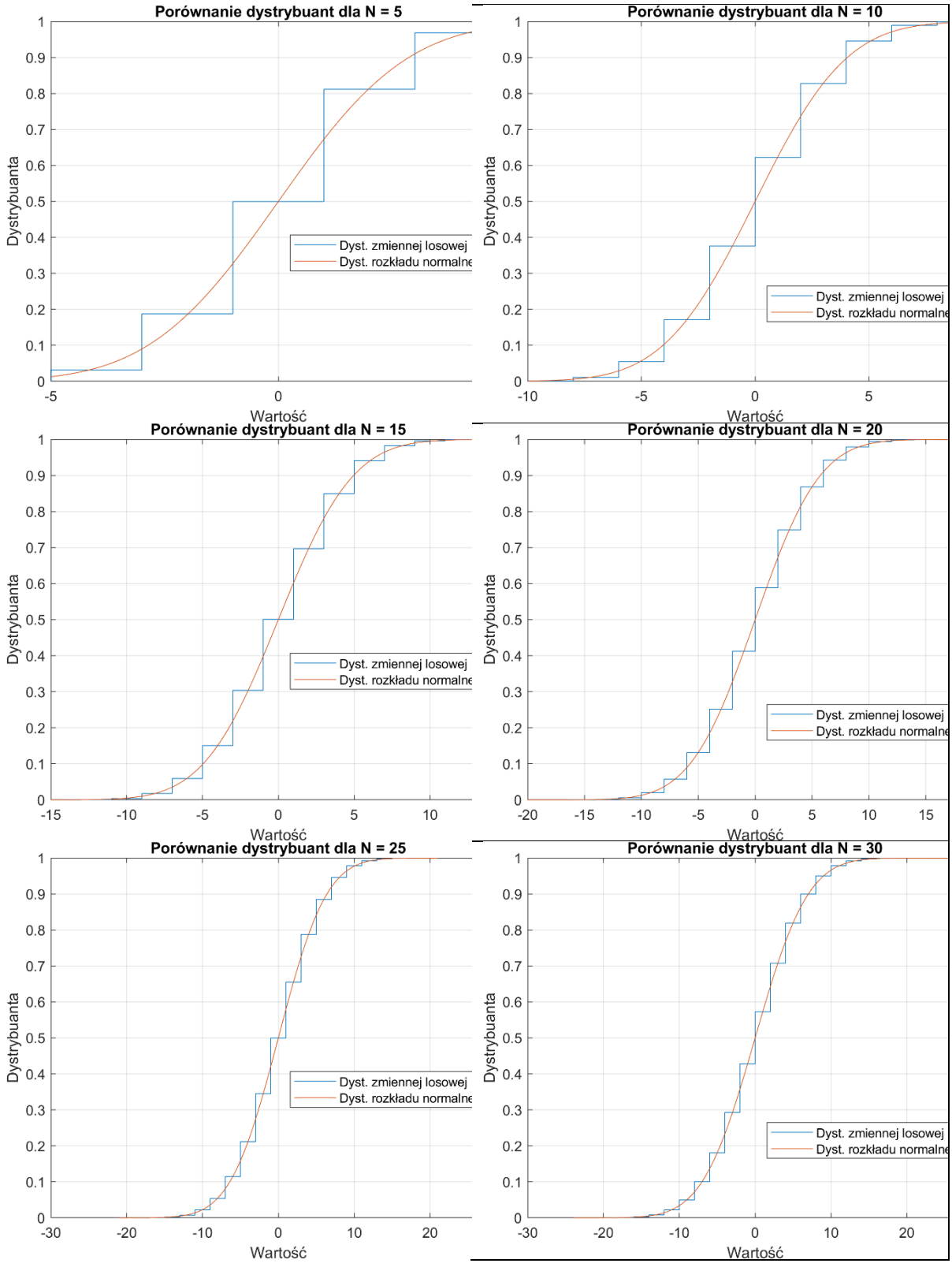
Histogramy dla poszczególnych N:

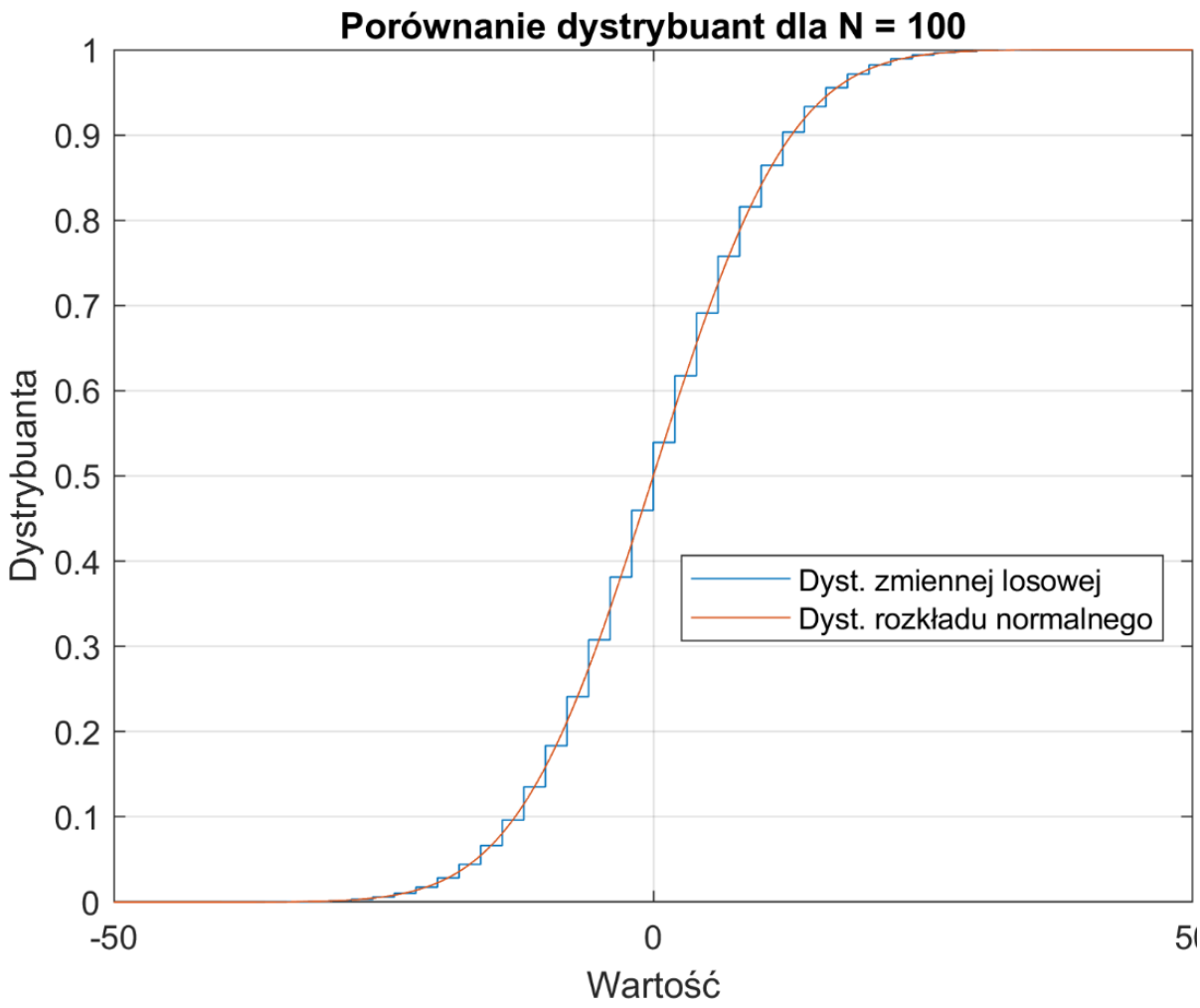




Im większe N tym bardziej gęstość przypomina rozkład normalny. Dla N = 100 widać już bardzo wyraźnie kształt „dzwonka”.

Dystrybuanty dla poszczególnych N:

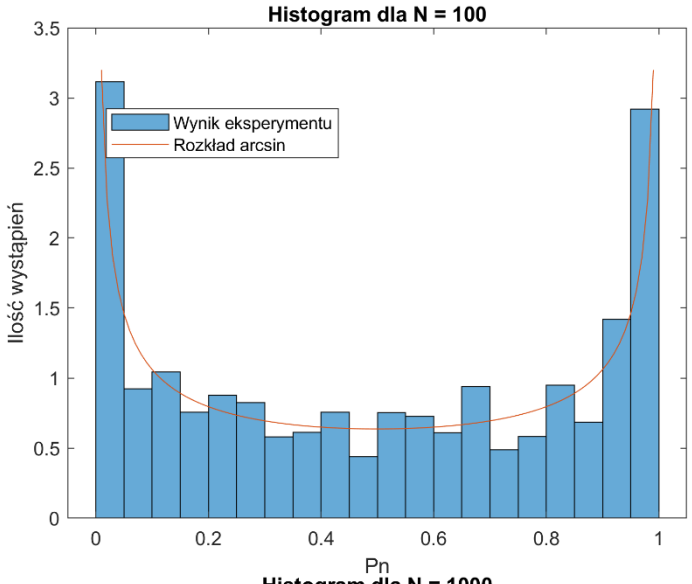


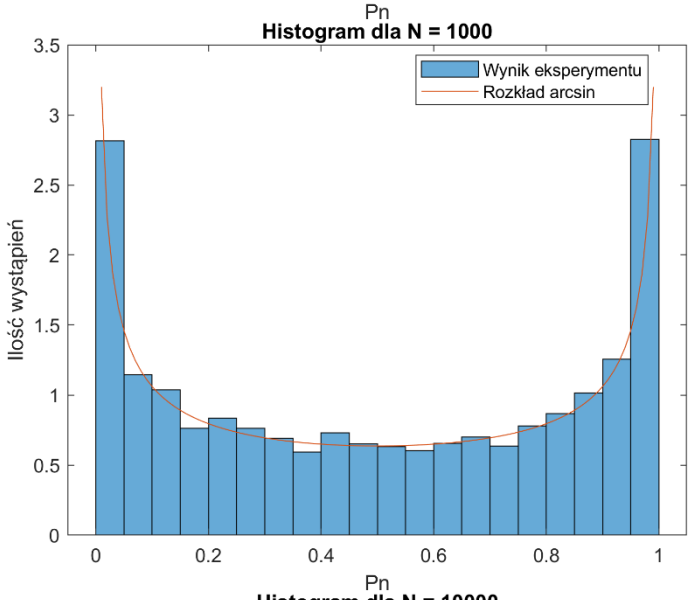


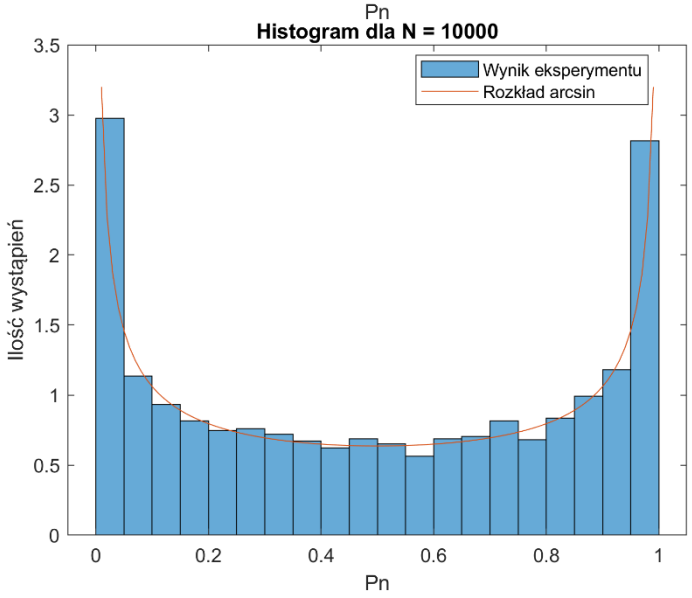
Im większe N tym bardziej dystrybuanta wygenerowanej zmiennej losowej przypomina dystrybuantę rozkładu normalnego.

Poziom podobieństwa w obu przypadkach zależy też od ilości wykonanych prób. Przedstawione wykresy zostały otrzymane po wykonaniu 1 000 000 prób dla każdego N. Im mniejsza ilość prób tym bardziej otrzymane wykresy różnią się od rozkładu normalnego.

Zadanie 3







Im większe N tym mniej spośród „kubełków” wygenerowanych w eksperymencie znacząco odbiega od rozkładu arcsin i tym mniejsze są ogólne różnice między oboma wykresami.