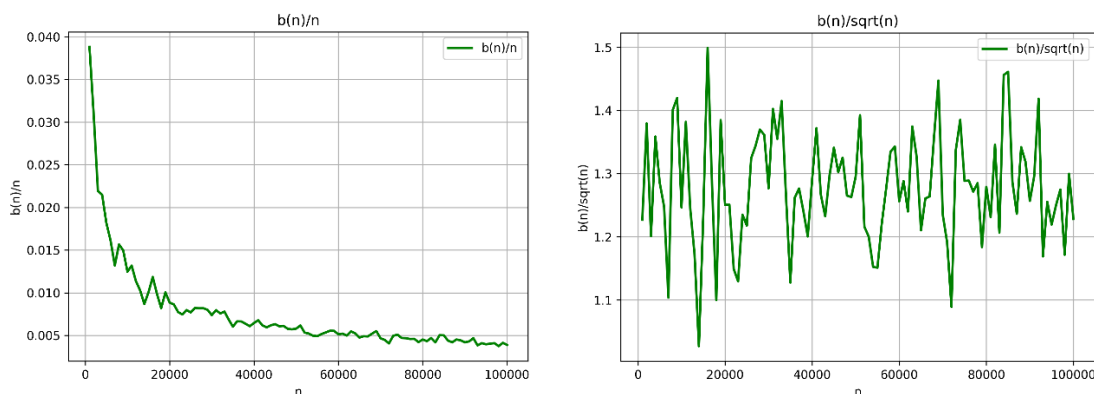
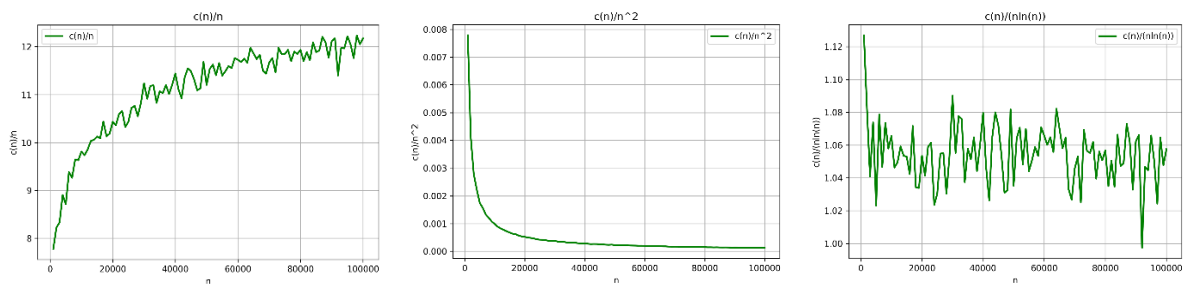


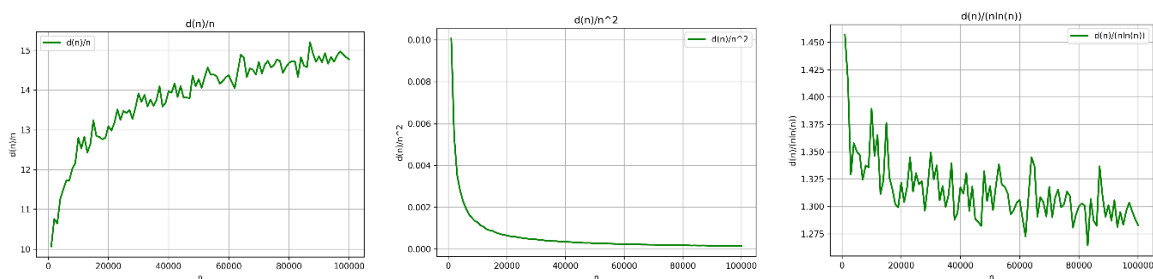
Poszczególne momenty pierwszej kolizji są najbardziej rozproszone (oddalone od średniej). W przeciwieństwie do wykresu pustych urn, który zdaje się przedstawiać linię prostą. Z wykresu U_n można wywnioskować, że liczba pustych urn po n rzutach wynosi około 37%. Wykresy C_n i D_n wydają się być podobne (oba w przybliżeniu przedstawiają prostą, a poszczególne próby są podobnie oddalone od średniej). Wartości przyjmowane przez D_n są nieco wyższe od C_n , co skutkuje przyjmowaniem niższych wartości dla ich różnicy.



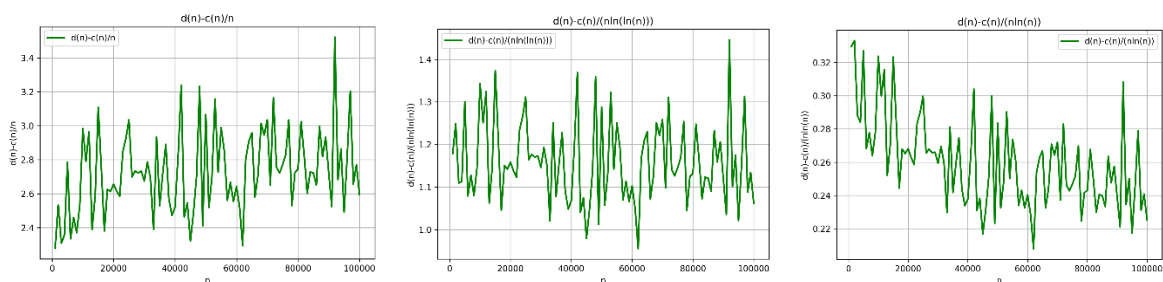
Funkcja $b(n)/n$ maleje (tempo mniejsze niż $\Theta(n)$) z kolei $b(n)/\sqrt{n}$ przyjmuje wartości w przybliżeniu od 1.1 do 1.5. Sugerować może to następującą asymptotykę $\Theta(\sqrt{n})$



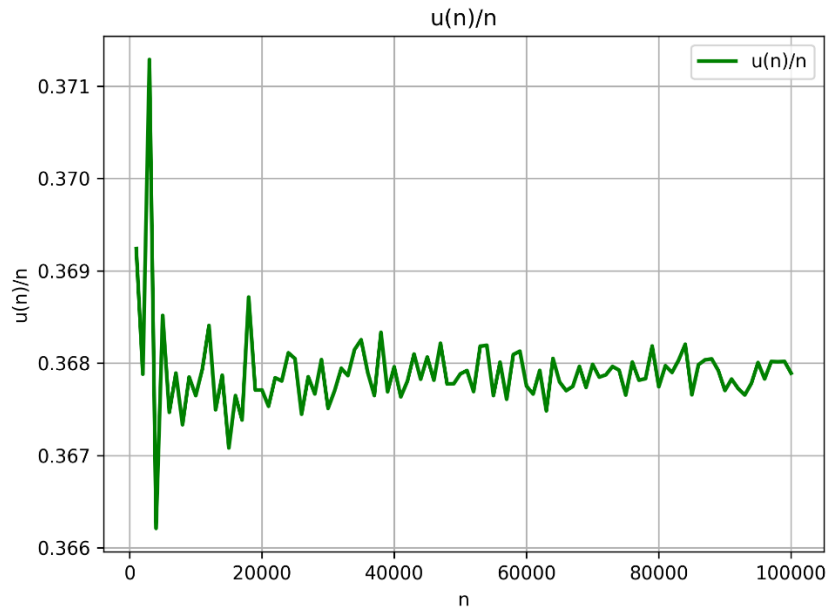
Funkcja rośnie wolniej niż n^2 a szybciej niż n . Z kolei $n \ln(n)$ wydaje się rosnąć w podobnym tempie.



Bardzo podobne tempo wzrostu do C_n . D_n i C_n mają wolniejsze tempo wzrosty niż $\Theta(n^2)$, ale większe niż $\Theta(n)$. Prawdopodobnie $\Theta(n \ln(n))$



Asymptotyką $D_n - C_n$ zdaje się być $\Theta(n \ln \ln n)$. Funkcja ma większe tempo wzrostu niż $\Theta(n)$, ale mniejsze niż $\Theta(n \ln(n))$



Wykres przypomina funkcję stałą (asymptotyka $\Theta(n)$), w przybliżeniu $u=0.37n$, co oznacza, że 73% urn zostaje wypełnione

Birthday paradox:

- **Paradox** prawdopodobnie dotyczy zaskakująco dużego prawdopodobieństwa, że w losowej grupie osób co najmniej dwie osoby będą miały tę samą datę urodzin. W kontekście urn i kul oznacza to, że przy odpowiednio dużej liczbie rzutów prawdopodobieństwo "kolizji" (tj. umieszczenia więcej niż jednej kuli w tej samej urnie) staje się bardzo wysokie.
- Zastosowanie w zadaniu: kiedy kule są przypisywane do urn losowo, "kolizje" kul w urnach (dwie kule w tej samej urnie) występują szybciej, niż mogłoby się wydawać. Intuicja z **birthday paradox** pozwala zrozumieć mechanikę pojawiania się dwóch kul w urnie.

Coupon collector's problem:

- W problemie kolekcjonera kuponów celem jest zebranie co najmniej jednego egzemplarza każdego kuponu z określonej puli. W naszym przypadku chodzi o umieszczenie co najmniej jednej kuli w każdej urnie.
- Zastosowanie w zadaniu: rozkład rzutów kul do urn przypomina zbieranie różnych kuponów, gdzie potrzeba określonej liczby rzutów, aby każda urna miała przynajmniej jedną kulę (analogicznie do zebrania wszystkich unikalnych kuponów).

Wniosek:

- **Birthday paradox** pomaga zrozumieć, kiedy dwie kule pojawią się w jednej urnie.
- **Coupon collector's problem** wyjaśnia, ile prób jest potrzebnych, aby każda urna miała przynajmniej jedną kulę.

Znaczenie **birthday paradox** w funkcjach hashujących i kryptograficznych

- W funkcjach hashujących celem jest przypisanie unikalnej wartości (hasza) do każdego możliwego wejścia. Jednak w praktyce przestrzeń hashów jest skończona, co oznacza, że dla wystarczająco dużej liczby różnych wejść mogą wystąpić **kolizje** (dwa różne wejścia generują ten sam hash).
- Funkcje kryptograficzne powinny minimalizować możliwość kolizji, aby zapewnić bezpieczeństwo (np. w podpisach cyfrowych czy kluczach).

Birthday paradox może pomóc w obliczeniu prawdopodobieństwa kolizji w funkcjach hashujących i kryptograficznych