



Liczby pseudolosowe

- [Wprowadzenie](#)
- [Przeczytaj](#)
- [Schemat interaktywny](#)
- [Sprawdź się](#)
- [Dla nauczyciela](#)



Liczby pseudolosowe

Źródło: Riho Kroll, domena publiczna.

Najstarsze znane nam kości do gry są datowane na XXIV w. p.n.e., co świadczy o tym, że liczby losowe używane są już od dawna. Jednak dopiero niecałe sto lat temu nastąpiła prawdziwa rewolucja. W latach 40. ubiegłego wieku rzuty kostką czy monetą stały się przeżytkiem. Firma RAND Corporation stworzyła wtedy maszynę, która wytwarzała losowe liczby, używając generatora sygnałów. Wyniki działania tego urządzenia opisano w książce *A Million Random Digits with 100,000 Normal Deviates*. Pomysł zapisania miliona przypadkowych liczb w książce może się wydawać absurdalny, był jednak prawdziwym przełomem dla naukowców i pasjonatów, którzy uzyskali dostęp do dużej sekwencji liczb losowych.

W tym e-materiale wyjaśnimy, czym są liczby losowe i pseudolosowe, a także jakie jest ich zastosowanie.

Jak wygenerować liczby pseudolosowe w poszczególnych językach programowania dowiesz się z e-materiałów:

- [Generowanie liczb pseudolosowych w języku C++](#),
- [Generowanie liczb pseudolosowych w języku Java](#),
- [Generowanie liczb pseudolosowych w języku Python](#).

Więcej zadań? Sięgnij do [Generowanie liczb pseudolosowych – zadania maturalne](#).

Twoje cele

- Poznasz różnicę pomiędzy liczbami prawdziwie losowymi a pseudolosowymi.
- Dowiesz się, jakie jest zastosowanie liczb losowych w różnych dziedzinach.

Przeczytaj

Liczba losowa to liczba otrzymana jako efekt losowania z określonego zbioru. Takim losowaniem może być na przykład rzut kostką czy wyciąganie kul z urny. Możemy je także generować za pomocą programu komputerowego, jednak czy rzeczywiście są one w pełni losowe?

Liczby pseudolosowe

Niestety, otrzymywanie liczb prawdziwie losowych jest skomplikowane. Na przykład rzucając kostką, musielibyśmy mieć pewność, że jest ona idealnie wyważona – a więc każda ścianka musiałaby mieć taką samą masę, by nie zaburzać wyniku losowania. W przypadku programu komputerowego wynik jest często rezultatem kilku działań matematycznych. Liczby wytworzone w ten sposób wyglądają na losowe, choć nimi nie są. Takie liczby nazywamy pseudolosowymi, a program – generatorem liczb pseudolosowych.

Generatory liczb pseudolosowych

Algorytmy służące do generowania liczb pseudolosowych to w rzeczywistości seria obliczeń bazujących na liczbie, którą nazywamy ziarnem (ang. *seed*). Popularną praktyką jest pobieranie czasu systemowego i używanie go jako ziarna dla generatorów. Taka liczba poddana serii działań matematycznych stanowi podstawę do wytwarzania liczb przypominających losowe. W praktyce oznacza to, że ustawiając to samo ziarno, jesteśmy w stanie generować dokładnie ten sam zestaw liczb, stąd brak przydatności tego algorytmu w kryptografii.

Ciekawostka

W niektórych grach komputerowych opartych na liczbach pseudolosowych twórcy pozostawiają możliwość ustawienia ziarna. Jest ona szczególnie przydatna, gdy chcemy rozpocząć grę dokładnie w tych samych warunkach, co inne osoby.

Ogromną zaletą generatorów pseudolosowych jest prędkość ich działania przy jednoczesnym braku utraty właściwości statystycznych. Trzeba jednak pamiętać, że znając dane wejściowe i algorytm jesteśmy w stanie obliczyć wynik działania generatora.

Ciekawostka

Istnieją urządzenia, które generują liczby losowe nie na podstawie algorytmu, a na podstawie procesów fizycznych, takich jak na przykład szum elektryczny. Taki generator produkuje stan, który można interpretować jako liczbę. Nazywamy je generatorami sprzętowymi lub generatorami zdarzeń losowych.

Zastosowanie

Symulacje

Liczby losowe znajdują szerokie zastosowanie, między innymi do przeprowadzania symulacji, na podstawie których można wyciągnąć określone wnioski. Przykładowo możemy przeprowadzić serię symulacji możliwych ruchów chmur, żeby zbadać, jakie jest prawdopodobieństwo, że w najbliższą sobotę będzie padać deszcz.

Statystyka

Kolejną dziedziną, w której liczby losowe znalazły zastosowanie, jest statystyka. Na przykład chcąc zbadać popularność radiostacji w Polsce, trudno byłoby przepytąć każdego radiosłuchacza w Polsce. W takim przypadku losowo wybiera się określoną liczbę osób. Warto pamiętać, że im większa będzie to grupa, tym badanie będzie dokładniejsze. Wynik takiego badania może zaburzyć nieodpowiednio przygotowana baza [respondentów](#). Jeśli do jego przeprowadzenia wybierzemy np. połowę uczniów z danej klasy, wynik nie będzie odzwierciedlał preferencji całej populacji Polaków. Dlatego zawsze warto sprawdzać, w jakich warunkach interesujące nas badania zostały przeprowadzone, zanim ukształtujemy na ich podstawie swoją opinię.

Gry komputerowe

Nie możemy zapomnieć o grach komputerowych. Te wykorzystują liczby losowe do tworzenia realistycznie wyglądającego świata, w którym, przykładowo, postacie poruszają się w losowy sposób, a nie tylko pomiędzy kilkoma punktami w określonej kolejności. Nagrody otrzymywane w grach również mogą być losowe lub posiadać losowe właściwości. W efekcie mamy do czynienia z ciekawszym lub bardziej realistycznym światem.

Ciekawostka

Wśród graczy popularny jest zwrot RNG, który pochodzi od angielskiej nazwy generatora liczb losowych, *random number generator* i określa się w ten sposób losowe zdarzenia w grach.

Gry losowe

Oczywiście liczby losowe znajdują zastosowanie także w grach losowych, loteriach czy w kasynach. Jako przykład tych pierwszych możemy podać chociażby gry karciane czy planszowe, których wynik zależy od rzutów kostką czy wylosowanej karty. W przypadku gier [hazardowych](#) wykorzystywanych w loteriach i kasynach liczby losowe mają kluczowe znaczenie. Niestety, reguły tych gier ustawiają gracza na straconej pozycji. Rachunek prawdopodobieństwa jasno wskazuje, że wylosowanie jednej lub kilku konkretnych figur

czy liczb ze sporej puli jest mało prawdopodobne. Warto zaznaczyć, że niektórzy producenci gier hazardowych próbowali dodatkowo się wzbogacić, manipulując generatorami liczb losowych w swoich grach, dlatego są one w wielu krajach kontrolowane przez rząd, a w innych uznano je nawet za nielegalne.

Kryptografia

Liczb losowe są także używane w [kryptografii](#) do szyfrowania danych. Tego procesu zazwyczaj nie dostrzegamy – wiadomości, które wysyłamy przy pomocy poczty elektronicznej czy ulubionego portalu społecznościowego zazwyczaj są przynajmniej w minimalnym stopniu szyfrowane tak, by osoby nieuprawnione nie były ich w stanie odczytać. Jeśli jednak osoba postronna zna algorytm oraz klucz, według którego wiadomość została zaszyfrowana, będzie w stanie ją odczytać.

Ciekawostka

Wciąż rozwijane komputery kwantowe ze względu na swoją szybkość stanowią spory problem dla kryptografii, ponieważ są w stanie złamać wiele obecnie używanych szyfrów metodą siłową – czyli próbując wszystkich możliwych rozwiązań.

Słownik

respondent

osoba przekazująca swoje dane dla celów statystycznych

hazard

gry pieniężne, w których wygrana zależy od wyniku losowania

kryptografia

dziedzina nauki zajmująca się sposobami utajniania przekazywanych wiadomości

Schemat interaktywny

Polecenie 1

Wykorzystaj poniższą aplikację do stworzenia imitacji loterii, w której losujemy bez powtórzeń x razy ze zbioru liczb $[1, n]$. Wybierz przykładowy zestaw liczb i sprawdź, ile razy musisz wykonać losowanie, aby wygrać. Następnie wykonaj polecenie 2.

Działanie programu przetestuj dla $x = 3$ oraz $n = 15$. Załóż, że wylosować masz liczbę 2.

Specyfikacja problemu:

Dane:

- x – liczba losowanych liczb; liczba naturalna dodatnia; $x < n$
- n – liczba dostępnych liczb; liczba naturalna dodatnia

Wynik:

- x wylosowanych liczb ze zbioru liczb $[1, n]$ bez powtórzeń

Polecenie 2

Przygotuj notatkę ze swoimi spostrzeżeniami dotyczącymi schematu interaktywnego.

Polecenie 3

Zastanów się, w jakich sytuacjach w życiu spotykasz się z liczbami pseudolosowymi. Zapisz swoje propozycje.

Sprawdź się

Pokaż ćwiczenia:   

Ćwiczenie 1



Zaznacz, w którym wieku stworzono maszynę generującą liczby losowe.

☐ XIX w.

☐ XVII w.

☐ XX w.

☐ XVIII w.

Ćwiczenie 2



Przyporządkuj pojęcia do ich definicji.

wariacja

To dowolny ciąg utworzony ze wszystkich elementów zbioru.

permutacja

Pozwala policzyć, na ile sposobów można wybrać elementy ze zbioru.

kombinacja

Pozwala na utworzenie ciągu z elementów zbioru.

Ćwiczenie 3



Zaznacz wartości, które mogą być prawdopodobieństwem pewnego wydarzenia.

☐ 33%

☐ $\frac{3}{2}$

☐ 121%

☐ $\frac{5}{6}$

☐ $\frac{1}{2}$

Ćwiczenie 4



Wskaż, jakie jest prawdopodobieństwo, że wybierając losową odpowiedź z poniższych, wybierzesz prawidłową.

☐ 50%

☐ 25%

☐ 60%

☐ 75‰

Ćwiczenie 5



Dokończ zdanie.

Rzucamy trzy razy symetryczną monetą. Prawdopodobieństwo otrzymania co najmniej jednej reszki jest równe...

☐ $\frac{1}{2}$

☐ $\frac{1}{4}$

☐ $\frac{1}{8}$

☐ $\frac{7}{8}$

Ćwiczenie 6



Wskaż, jakie jest prawdopodobieństwo, że dziś jest wtorek.

☐ $\frac{4}{20}$

☐ $\frac{1}{7}$

☐ $\frac{5}{7}$

☐ $\frac{6}{7}$

Ćwiczenie 7



W jednej z popularnych loterii losujemy 6 liczb z 49 (bez powtórzeń). Wskaż, jakie jest prawdopodobieństwo, że mając tylko jedną szansę, odgadniemy wynik losowania.

☐ Jest równe 0,13983816%.

☐ Jest w przybliżeniu równe 0,0081667%.

☐ Jest w przybliżeniu równe 0,0000072%.

☐ Jest w przybliżeniu równe 0,1224490%.

Ćwiczenie 8



Zaznacz, co musimy zrobić, chcąc mieć pewność, że na pewno wygramy powyższą loterię.

- ☐ Wydać mniej niż 35 milionów złotych, gdyby los kosztował 2,50 zł.
- ☐ Wydać ponad 25 milionów złotych, gdyby los kosztował 2,00 zł.
- ☐ Wydać ponad 45 milionów złotych, gdyby los kosztował 2,25 zł.
- ☐ Zakupić los z każdą możliwą kombinacją liczb, ignorując ich pozycję.
- ☐ Zakupić los z każdą możliwą kombinacją liczb na każdej możliwej pozycji.

Dla nauczyciela

Autor: Adam Żółtowski

Przedmiot: Informatyka

Temat: Liczby pseudolosowe

Grupa docelowa:

Liceum ogólnokształcące i technikum, liceum ogólnokształcące, technikum, zakres rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

- I. Rozumienie, analizowanie i rozwiązywanie problemów na bazie logicznego i abstrakcyjnego myślenia, myślenia algorytmicznego i sposobów reprezentowania informacji.
- II. Programowanie i rozwiązywanie problemów z wykorzystaniem komputera oraz innych urządzeń cyfrowych: układanie i programowanie algorytmów, organizowanie, wyszukiwanie i udostępnianie informacji, posługiwanie się aplikacjami komputerowymi.

Treści nauczania – wymagania szczegółowe

- I. Rozumienie, analizowanie i rozwiązywanie problemów.

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

- 1) w zależności od problemu rozwiązuje go, stosując metodę wstępującą lub zstępującą;

- II. Programowanie i rozwiązywanie problemów z wykorzystaniem komputera i innych urządzeń cyfrowych.

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

- 1) projektuje i tworzy rozbudowane programy w procesie rozwiązywania problemów, wykorzystuje w programach dobrane do algorytmów struktury danych, w tym struktury dynamiczne i korzysta z dostępnych bibliotek dla tych struktur;

3) sprawnie posługuje się zintegrowanym środowiskiem programistycznym przy pisaniu, uruchamianiu i testowaniu programów;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Poznasz różnicę pomiędzy liczbami prawdziwie losowymi a pseudolosowymi.
- Dowiesz się, jakie jest zastosowanie liczb losowych w różnych dziedzinach.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimediu i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Liczby pseudolosowe”. Nauczyciel prosi uczniów o zapoznanie się z multimediu w sekcji „Schemat interaktywny”.

Faza wstępna:

1. **Rozpoznanie wiedzy uczniów.** Nauczyciel prosi wybranego ucznia lub uczniów o przedstawienie sytuacji problemowej związanej z tematem lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu e-materiału. Indywidualnie zapoznają się z treścią w sekcji „Przeczytaj”.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Schemat interaktywny”. Uczniowie wspólnie zapoznają się z treścią zawartego w niej multimedium. Następnie wykorzystują aplikację do stworzenia imitacji loterii, w której losują 3 z 15 liczb bez powtórzeń. Wybierają przykładowy zestaw liczb i sprawdzają, ile razy muszą wykonać losowanie, aby wygrać.
3. W kolejnym etapie uczniowie dobierają się w pary i wykonują ćwiczenia nr 1-5. Następnie konsultują swoje rozwiązania z inną parą uczniów i ustalają jedną wersję odpowiedzi.

Faza podsumowująca:

1. Na koniec zajęć nauczyciel prosi uczniów o rozwinięcie zdania: „Na dzisiejszych zajęciach nauczyłam/łem się jak...”.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 6-7 z sekcji „Sprawdź się”.
2. Uczniowie wykonują polecenie 2 z sekcji „Schemat interaktywny”.

Wskazówki metodyczne:

- Treści w sekcji „Schemat interaktywny” można wykorzystać na lekcji jako podsumowanie i utrwalenie wiedzy uczniów.