



Sito Eratostenesa

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



Sito Eratostenesa jest algorytmem wyznaczającym liczby pierwsze z danego przedziału $<2, n>$. Liczby pierwsze znajdują zastosowanie między innymi w kryptografii, o czym przeczytasz m.in. w e-materiałach:

- [Zastosowanie liczb pierwszych](#),
- [Szyfr RSA](#).

Implementacje omawianego algorytmu przedstawiamy w e-materiałach:

- [Programowanie sita Eratostenesa w języku C++](#),
- [Programowanie sita Eratostenesa w języku Java](#),
- [Programowanie sita Eratostenesa w języku Python](#).

Więcej zadań? Sięgnij do: [Sito Eratostenesa w zadaniach](#).

W e-materiale [Algorytmy liczbowe](#) znajdziesz informacje na temat algorytmu sprawdzającego, czy dana liczba należy do liczb pierwszych.

Twoje cele

- Wymienisz własności liczb pierwszych oraz ich zastosowanie.
- Przeanalizujesz działanie algorytmu sita Eratostenesa.

- Stworzysz program wyznaczający liczby pierwsze z zadanego zakresu.

Przeczytaj

Sito [Eratostenesa](#) jest algorytmem znajdującym w danym przedziale $< 2, n >$ wszystkie liczby pierwsze. Liczby pierwsze znajdują zastosowanie w [kryptografii](#), m.in. w szyfrze RSA. Z powodu trudności w rozkładzie dużych liczb na czynniki pierwsze, algorytm RSA jest bezpieczny, a co za tym idzie – często stosowany w szyfrowaniu, a także przy tworzeniu [podpisów cyfrowych](#). Więcej na ten temat dowiesz się z e-materiału [Szyfr RSA](#).

Ideą algorytmu sita Eratostenesa jest wykrycie i usunięcie (wykreślenie) z zadanego przedziału liczb złożonych, zaczynając od wielokrotności liczby 2. Liczby złożone są wielokrotnościami liczb pierwszych. Jeżeli ze zbioru liczb naturalnych wykreślimy liczby złożone, pozostaną wyłącznie liczby pierwsze.

Problem 1

Dany jest przedział liczb naturalnych $< 2, n >$. Znajdź wszystkie liczby pierwsze zawarte w tym przedziale. Problem rozważmy dla $n = 30$.

Specyfikacja problemu:

Dane:

- Zbiór liczb naturalnych z przedziału $< 2, n >$
- n – liczba naturalna

Wyniki:

- liczby pierwsze z przedziału $< 2, n >$

Przeanalizujemy działanie algorytmu dla $n = 30$. Wybieramy liczbę najmniejszą (2). Następnie wykreślamy wszystkie liczby będące jej wielokrotnościami (4, 6, 8, 10, 12..., 30).

Otrzymujemy następujący zbiór:

2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29

Z pozostałych liczb wybieramy najmniejszą niewykreśloną liczbę (3). Usuwamy jej wszystkie wielokrotności (6, 9, 12, 15, 18, 21, 24, 27, 30). Oczywiście część z tych wielokrotności została już usunięta.

Otrzymujemy następujący zbiór:

2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29

Czynność powtarzamy, dopóki liczba, której wielokrotności wykreślamy, jest nie większa niż pierwiastek z liczby n . W naszym przypadku $n = 30$, więc właściwy pierwiastek to $\sqrt{30}$.

Po wykreśleniu wielokrotności liczby 5 otrzymamy zbiór:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

W tym momencie zakończymy algorytm. Nie będziemy usuwać wielokrotności liczby 7, ponieważ jak wiemy $7 > \sqrt{30}$. Zbiór zawiera wszystkie liczby pierwsze z zakresu od 2 do 30.

Algorytm zapisany za pomocą pseudokodu

Napiszmy teraz algorytm sita Eratostenesa za pomocą pseudokodu.

Zaczynamy od zadeklarowania zmiennej n oraz n -elementowej tablicy. Przyjmujemy, że indeksy tablicy odpowiadają kolejnym liczbom naturalnym z analizowanego przedziału. Na początku zakładamy, że wszystkie liczby są pierwsze i dlatego każdemu z elementów przypiszemy wartość `prawda`. Wykreślanie będzie polegało na zmianie wartości wykreślanego elementu z wartości `prawda` na `fałsz`. Indeksy tablicy odpowiadające elementom o wartości `prawda` to poszukiwane liczby pierwsze.

```
1 n = wprowadź liczbę naturalną
2
3 T[n] = tablica wartości logicznych
4
5 dla s = 2, 3, ... n wykonuj:
6     T[s] = prawda
```

Następnie tworzymy pętlę `dla`, w której będziemy sprawdzać czy element kryjący się w tablicy pod indeksem i ma wartość `true`. Jeżeli tak, wówczas w wewnętrznej pętli będziemy wykreślać wielokrotności indeksu tego elementu.

Iterator zewnętrznej pętli (i) będzie przyjmował wartości $< 2, \sqrt{n} >$. Deklarujemy zmienną j . Tak jak wspomnieliśmy, jej zadaniem będzie wskazanie indeksu wykreślanego elementu, czyli kolejnych wielokrotności liczby i . Inicjalizujemy ją kwadratem liczby i . Zostanie przez nas wykorzystana w wewnętrznej pętli dopóki i . Wewnątrz pętli wyznaczamy kolejne wielokrotności liczby i , dodając jej wartość do zmiennej j . Wewnętrzną pętlę przerywamy, kiedy wielokrotność i , zapisana w zmiennej j , będzie większa od ustalonego rozmiaru sita.

```
1 n = wprowadź liczbę naturalną
2
3 T[n] = tablica wartości logicznych
```

```

4
5 dla s = 2, 3, ... n wykonuj:
6     T[s] = prawda
7
8 dla i = 2, 3, ... <= pierwiastek(n) wykonuj:
9     jeżeli T[i] == prawda wykonaj:
10        j = i * i
11        dopóki j <= n wykonuj:
12            T[j] = fałsz
13            j = j + i

```

Ostatnim krokiem jest wypisanie liczb pierwszych.

Kompletny algorytm sita Eratostenesa zapisany za pomocą pseudokodu:

```

1 n = wprowadź liczbę naturalną
2
3 T[n] = tablica wartości logicznych
4
5 dla s = 2, 3, ... n wykonuj:
6     T[s] = prawda
7
8 dla i = 2, 3, ... <= pierwiastek(n) wykonuj:
9     jeżeli T[i] == prawda wykonaj:
10        j = i * i
11        dopóki j <= n wykonuj:
12            T[j] = fałsz
13            j = j + i
14
15 dla a = 2, 3, ... n wykonuj:
16     jeżeli T[a] == prawda:
17         wypisz a

```

Ważne!

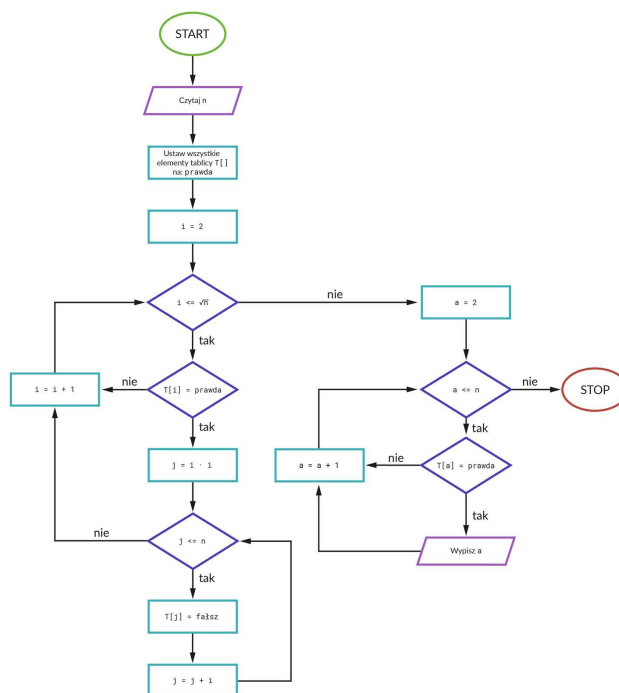
W przedstawionym algorytmie Sita Eratostenesa w pętli dla... wykonuj zastosowaliśmy warunek $i \leq \text{pierwiastek}(n)$. Gdy obie strony nierówności $i \leq \text{pierwiastek}(n)$ podniesiemy do kwadratu, otrzymamy $i * i \leq n$. Tego warunku możesz używać w swoich implementacjach sita Eratostenesa: $i * i \leq n$.

```

1  n = wprowadź liczbę naturalną
2
3  T[n] = tablica wartości logicznych
4
5  dla s = 2, 3, ... n wykonuj:
6      T[s] = prawda
7
8  i = 2
9
10 dopóki i * i <= n wykonuj:
11     jeżeli T[i] == prawda wykonaj:
12         j = i * i
13         dopóki j <= n wykonuj:
14             T[j] = fałsz
15             j = j + i
16     i = i + 1
17
18 dla a = 2, 3, ... n wykonuj:
19     jeżeli T[a] == prawda:
20         wypisz a

```

Schemat blokowy algorytmu



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Słownik

Eratostenes

grecki matematyk, filozof i astronom; wyznaczył obwód Ziemi oraz oszacował odległość Ziemi od Słońca

kryptografia

gałąź wiedzy, która zajmuje się zabezpieczaniem informacji przed niepowołanym dostępem

liczba pierwsza

liczba naturalna większa od 1, która dzieli się tylko przez jeden i przez samą siebie

podpis cyfrowy

matematyczny sposób sprawdzenia autentyczności dokumentów i wiadomości elektronicznych

sito Eratostenesa

algorytm wyznaczania liczb pierwszych z zadanego przedziału $<2, n>$ – jego autorstwo jest przypisywane greckiemu matematykowi Eratostenesowi z Cyreny, który żył w III w. p.n.e.

Schemat interaktywny

Polecenie 1

Zapisz algorytm, który wypisze wszystkie liczby pierwsze z przedziału $<2, n>$ oraz wyświetli ich liczbę. Wykorzystaj do tego schemat blokowy (jeśli chcesz powtórzyć wiadomości ze szkoły podstawowej) lub język programowania.

Przetestuj jego działanie dla zakresu $<2, 100>$.

Specyfikacja problemu:

Dane:

n – liczba naturalna dodatnia, $n > 2$

Wynik:

Na standardowym wyjściu program wyświetla liczby pierwsze z zakresu $<2, n>$ oraz podaje ich liczbę.

1

1



Polecenie 2

Dodaj do swojego programu komentarze tak, żeby był zrozumiały dla osoby, która nie potrafi programować.

Sprawdź się

Pokaż ćwiczenia:   

Ćwiczenie 1



Zaznacz wszystkie liczby, których wielokrotnościom przyporządkowane zostaną wartości fałsz w algorytmie sita Eratostenesa dla zbioru $\langle 2, 120 \rangle$. Analizy dokonaj na podstawie algorytmu zapisanego za pomocą pseudokodu w sekcji „Przeczytaj”.

☐ 7

☐ 11

☐ 3

☐ 6

☐ 4

☐ 5

☐ 2

Ćwiczenie 2



Wskaż, do jakiego momentu następuje wykreślanie liczb ze zbioru $\langle 2, \dots, n \rangle$ w algorytmie sita Eratostenesa.

☐ Do momentu, gdy liczba, której wielokrotności usuwamy, będzie większa niż n .

☐ Do momentu, gdy liczba, której wielokrotności usuwamy, będzie większa niż $\sqrt{n}$.

☐ Do momentu, gdy wartości wszystkich elementów tablicy będą wynosiły fałsz.

☐ Do momentu, gdy usuwana wielokrotność liczby będzie większa niż $\sqrt{n}$.

Ćwiczenie 3



Wskaż, jaką metodę należy zastosować, aby po użyciu algorytmu sita Eratostenesa, wypisać na ekranie liczby pierwsze z przedziału $\langle 2, 154 \rangle$.

- ☐ Wypisanie wartości indeksów tablicy z zakresu $\langle 2, 154 \rangle$.
- ☐ Wypisanie wartości elementów tablicy o indeksach z zakresu $\langle 2, 154 \rangle$.
- ☐ Wypisanie wartości indeksów elementów tablicy, których zawartość wynosi fałsz.
- ☐ Wypisanie wartości indeksów elementów tablicy, których zawartość wynosi prawda.

Ćwiczenie 4



Odpowiedz na pytanie.

Ile razy elementowi tablicy o indeksie 51 została przypisana wartość fałsz w algorytmie Sita Eratostenesa dla zbioru $\langle 2, 70 \rangle$? Analizy dokonaj na podstawie algorytmu zapisanego za pomocą pseudokodu w sekcji „Przeczytaj”.

Ćwiczenie 5



Dana jest n-elementowa tablica A wypełniona wartościami 1. Korzystając z algorytmu sita Eratostenesa, zmień zawartość tablicy tak, aby wartość 1 miały tylko te elementy tablicy, których indeksy są liczbami pierwszymi, pozostałe elementy powinny mieć wartość 0. W przeciwieństwie do algorytmu zapisanego za pomocą pseudokodu przedstawionego w sekcji „Przeczytaj”, zrealizuj własny, używając jedynie pętli dopóki.

Specyfikacja problemu:

Dane:

- n – liczba elementów tablicy
- A – tablica liczb wypełniona wartościami 1

Wynik:

Zmodyfikowana tablica A; wartość 1 przechowują wyłącznie komórki, których indeksy są liczbami pierwszymi; wartość 0 przechowują komórki, których indeksy są liczbami złożonymi.

1



Ćwiczenie 6



Podobnie jak w **Ćwiczeniu 5**, napisz za pomocą pseudokodu algorytm sita Eratostenesa, tym razem jednak przynajmniej raz użyj pętli wykonuj . . . dopóki.

Dana jest n-elementowa tablica A wypełniona wartościami 1. Korzystając z algorytmu sita Eratostenesa, zmień zawartość tablicy tak, aby wartość 1 miały tylko te elementy tablicy, których indeksy są liczbami pierwszymi, pozostałe elementy powinny mieć wartość 0.

Specyfikacja problemu:

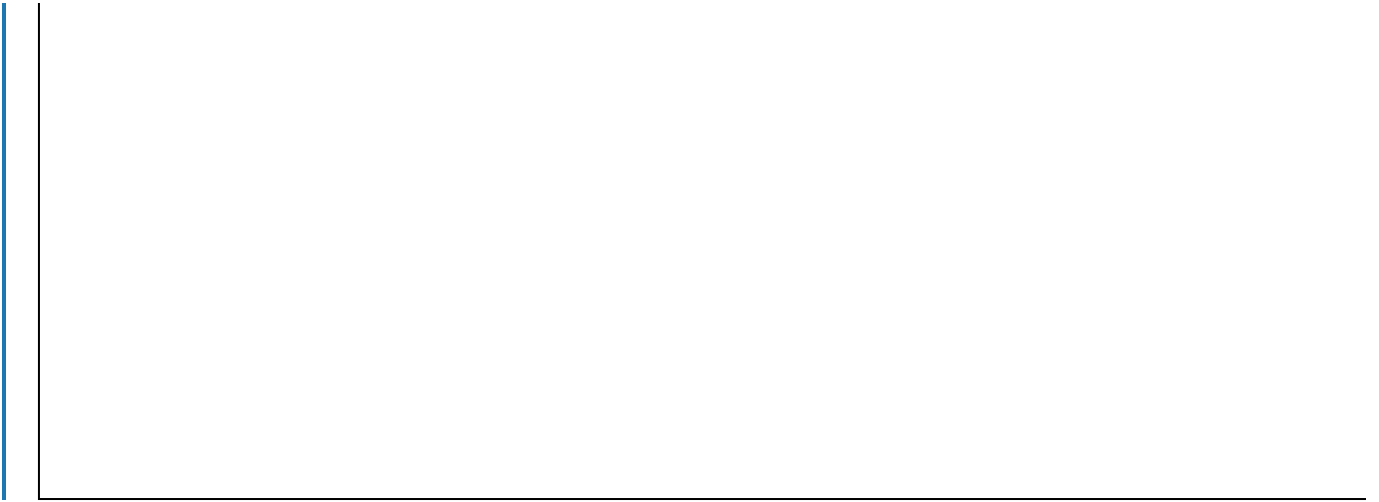
Dane:

- n – liczba elementów tablicy
- A – tablica liczb wypełniona wartościami 1

Wynik:

Zmodyfikowana tablica A; wartość 1 przechowują wyłącznie komórki, których indeksy są liczbami pierwszymi; wartość 0 przechowują komórki, których indeksy są liczbami złożonymi.

1



Ćwiczenie 7



Dokończ algorytm zapisany za pomocą pseudokodu tak, aby wypisywał wszystkie liczby złożone ze zbioru $\langle 2, n \rangle$.

```
1 dla s = 2, 3, ... n wykonuj:
2     T[s] = prawda
3
4 i = 2
5 dopóki i <= pierwiastek(n) wykonuj:
6     jeżeli T[i] == prawda wykonaj:
7         j = i * i
8         dopóki j <= n wykonuj:
9             T[j] = fałsz
10        j = j + i
11    i = i + 1
```

Ćwiczenie 8



Zmodyfikuj algorytm sita Eratostenesa tak, aby wartością elementu tablicy była liczba dzielników właściwych, które są liczbami pierwszymi (dzielniki będące liczbami pierwszymi, oprócz dzielników o wartości danego indeksu).

Specyfikacja problemu:

Dane:

- n – liczba elementów tablicy
- A – tablica liczb wypełniona wartościami 0

Wynik:

Zmodyfikowana tablica A ; wartość kryjąca się pod indeksem i przechowuje liczbę dzielników właściwych, które są liczbami pierwszymi.

Przykład:

Liczba 7 będzie miała 0 dzielników, ponieważ nie bierzemy pod uwagę dzielnika 7.

1



Dla nauczyciela

Autor: Maurycy Gast

Przedmiot: Informatyka

Temat: Sito Eratostenesa

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

1) zapisuje za pomocą listy kroków, schematu blokowego lub pseudokodu, i implementuje w wybranym języku programowania, algorytmy poznane na wcześniejszych etapach oraz algorytmy:

c) generowania liczb pierwszych metodą sita Eratostenesa,

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):

- Wymienisz własności liczb pierwszych oraz ich zastosowanie.

- Przeanalizujesz działanie algorytmu sita Eratostenesa.
- Stworzysz program wyznaczający liczby pierwsze z zadanego zakresu.

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. Uczniowie przypominają sobie najważniejsze informacje dotyczące własności liczb pierwszych oraz ich zastosowań. W razie potrzeby przypominają sobie również algorytm testowania, czy dana liczba należy do liczb pierwszych.

Faza wstępna:

1. Chętna lub wybrana osoba referuje najważniejsze informacje dotyczące właściwości oraz zastosowań liczb pierwszych.
2. Nauczyciel wyświetla temat oraz cele zajęć, omawiając lub ustalając razem z uczniami kryteria sukcesu.

Faza realizacyjna:

1. Uczniowie analizują przykład z sekcji „Przeczytaj” i powtarzają zaprezentowane rozwiązanie na swoim komputerze.

2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Schemat interaktywny”, czyta treść polecenia nr 1 „Zapisz algorytm, który wypisze wszystkie liczby pierwsze z przedziału $<2, n>$ oraz wyświetli ich liczbę. Wykorzystaj do tego schemat blokowy (jeśli chcesz powtórzyć wiadomości ze szkoły podstawowej) lub język programowania” i omawia kolejne kroki rozwiązania.
3. **Ćwiczenie umiejętności.** Liga zadaniowa – uczniowie realizują indywidualnie ćwiczenia nr 1–7 z sekcji „Sprawdź się”. Po ich wykonaniu nauczyciel omawia najlepsze rozwiązania problemów postawionych w zadaniach.

Faza podsumowująca:

1. Nauczyciel zadaje pytania podsumowujące, np.
 - jakie liczby nazywamy liczbami pierwszymi?
 - czym jest kryptografia?
 - podaj sposób wyznaczania liczb pierwszych z zadanego zbioru,
 - na czym polega algorytm Sito Eratostenesa?

Praca domowa:

1. Uczniowie wykonują ćwiczenie 8 z sekcji „Sprawdź się”.
2. Uczniowie wykonują polecenie 2 z sekcji „Schemat interaktywny”.

Wskazówki metodyczne:

- Multimedia w sekcji „Schemat interaktywny” można potraktować jako zadanie domowe dotyczące analizy problemu zawartego w temacie „Sito Eratostenesa”.