**Wyznaczanie liczb pierwszych**

Aby znaleźć wszystkie liczby pierwsze w zadanym przedziale liczbowym można posłużyć się algorytmem zwanym [**sitem Eratostenesa**](http://pl.wikipedia.org/wiki/Sito_Eratostenesa)**:** jeśli liczba naturalna *N* większa od 1 nie jest podzielna przez żadną z liczb pierwszych nie większych od pierwiastka z *N*, to *N* jest liczbą pierwszą.

Metoda, która daje odpowiedź na pytanie czy dana liczba naturalna jest pierwsza, czy nie – nosi nazwę [**testu pierwszości**](http://pl.wikipedia.org/wiki/Test_pierwszo%C5%9Bci)**.**

**Test pierwszości** to [algorytm](http://pl.wikipedia.org/wiki/Algorytm) określający czy dana liczba jest [pierwsza](http://pl.wikipedia.org/wiki/Liczba_pierwsza) czy złożona. Nie jest to równoważne znalezieniu jej rozkładu na czynniki pierwsze. W obecnej chwili ([2011](http://pl.wikipedia.org/wiki/2011) rok) nie są znane [efektywne algorytmy](http://pl.wikipedia.org/wiki/Algorytm_wielomianowy) rozkładu na czynniki pierwsze, natomiast testy pierwszości można przeprowadzać bardzo szybko.

|  |
| --- |
| **Metoda naiwna** |

Najprostszy test pierwszości wygląda następująco: dla danej liczby *n* sprawdzamy czy [**dzieli**](http://pl.wikipedia.org/wiki/Dzielnik)się ona kolejno przez 2, 3, aż do *n-1*. Jeśli przez żadną z nich się nie dzieli, oznacza to, że jest pierwsza.

Zamiast testować wszystkie liczby do *n-1*, wystarczy sprawdzać podzielność *n* przez liczby mniejsze lub równe \sqrt n.

Kolejne udoskonalenie polega na sprawdzaniu podzielności *n* jedynie przez liczby pierwsze mniejsze lub równe \sqrt n. Ich listę łatwo możemy uzyskać metodą [**sita Eratostenesa**](http://pl.wikipedia.org/wiki/Sito_Eratostenesa)**.**

Metoda ta niestety wciąż wymaga wykonania dużej ilości (\sqrt n/\log n) dzieleń, co oznacza, że już dla 50-cyfrowych liczb pierwszych jest niewykonalna na współczesnych komputerach.

Obecnie najbardziej efektywne i najczęściej stosowane są [testy probabilistyczne](http://pl.wikipedia.org/wiki/Algorytm_probabilistyczny). Korzysta się w nich z losowo wygenerowanych liczb z ustalonego przedziału – pewien dobór tych wartości może dać błędny wynik testu, ale przy wybraniu wystarczająco wielu z nich [prawdopodobieństwo](http://pl.wikipedia.org/wiki/Prawdopodobie%C5%84stwo) takiego zdarzenia jest znikome.

Przebieg testu probabilistycznego wygląda następująco:

1. Wybierz losowo liczbę *a*
2. Sprawdź pewne równanie zawierające *a* oraz zadaną liczbę *n*. Jeśli okaże się fałszywe, zwróć wynik ***n* jest złożona**. Wartość *a* jest wtedy *świadkiem* złożoności i test można zakończyć.
3. Powtarzaj całą procedurę aż uzyskasz wystarczającą pewność.

Jeśli w wystarczająco wielu próbach nie uda się stwierdzić złożoności *n*, test zwraca odpowiedź: *n* jest prawdopodobnie pierwsza.

Najbardziej znanymi testami pierwszości są:

* [Test pierwszości Fermata](http://pl.wikipedia.org/wiki/Test_pierwszo%C5%9Bci_Fermata) – prosty do przeprowadzenia, ale niepewny: istnieją liczby złożone ([Liczby Carmichaela](http://pl.wikipedia.org/wiki/Liczby_Carmichaela)), które przez ten test zawsze zostaną uznane za pierwsze.
* [Test pierwszości Solovay-Strassena](http://pl.wikipedia.org/wiki/Test_pierwszo%C5%9Bci_Solovay-Strassena) – dający przy każdej próbie 1/2 szans na wylosowanie świadka złożoności.
* [Test Millera-Rabina](http://pl.wikipedia.org/wiki/Test_Millera-Rabina) – dający przy każdej próbie 3/4 szans na wylosowanie świadka złożoności. Ten test jest najczęściej stosowany w [kryptografii](http://pl.wikipedia.org/wiki/Kryptologia), gdy wymagana jest szybka weryfikacja pierwszości dużych liczb. Już sprawdzenie dwudziestu losowych świadków gwarantuje, że prawdopodobieństwo błędnego rozpoznania liczby jako pierwszej jest mniejsze niż jeden do [biliona](http://pl.wikipedia.org/wiki/Bilion).

**Sito Eratostenesa** to [algorytm](http://pl.wikipedia.org/wiki/Algorytm) wyznaczania [liczb pierwszych](http://pl.wikipedia.org/wiki/Liczba_pierwsza) z zadanego przedziału [2,n]\;.

Ze zbioru liczb naturalnych z przedziału [2,n]\;, tj. \{2, 3, 4, \dots, n\},wybieramy najmniejszą, czyli 2 i wykreślamy wszystkie jej wielokrotności większe od niej samej, to jest 4, 6, 8, \dots

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 3 | ~~-4-~~ | 5 | ~~6~~ | 7 | ~~8~~ | 9 | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | 15 | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| 21 | ~~22~~ | 23 | ~~24~~ | 25 | ~~26~~ | 27 | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | 33 | ~~34~~ | 35 | ~~36~~ | 37 | ~~38~~ | 39 | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~-44-~~ | 45 | ~~46~~ | 47 | ~~48~~ | 49 | ~~50~~ |
| 51 | ~~52~~ | 53 | ~~54~~ | 55 | ~~56~~ | 57 | ~~58~~ | 59 | ~~60~~ |

Z pozostałych liczb wybieramy najmniejszą niewykreśloną liczbę (3) i usuwamy wszystkie jej wielokrotności większe od niej samej: 6, 9, 12, \dots, przy czym nie przejmujemy się tym, że niektóre liczby (na przykład 6 czy 12) będą skreślane więcej niż raz.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 3 | ~~-4-~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | 25 | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | 35 | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~-44-~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | 49 | ~~50~~ |
| ~~51~~ | ~~52~~ | 53 | ~~54~~ | 55 | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |

Według tej samej procedury postępujemy dla liczby 5.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 3 | ~~-4-~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~-44-~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | 49 | ~~50~~ |
| ~~51~~ | ~~52~~ | 53 | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |

Następnie dla 7, 11, 13; aż do sprawdzenia wszystkich niewykreślonych wcześniej liczb.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 3 | ~~-4-~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~-44-~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | ~~49~~ | ~~50~~ |
| ~~51~~ | ~~52~~ | 53 | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |

Wykreślanie powtarzamy do momentu, gdy liczba i\;, której wielokrotność wykreślamy nie jest większa niż \sqrt{n}.

Dla danej liczby n\;wszystkie niewykreślone liczby mniejsze od n\; są liczbami pierwszymi.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **2** | **3** | ~~-4-~~ | **5** | ~~6~~ | **7** | ~~8~~ | ~~9~~ | ~~10~~ |
| **11** | ~~12~~ | **13** | ~~14~~ | ~~15~~ | ~~16~~ | **17** | ~~18~~ | **19** | ~~20~~ |
| ~~21~~ | ~~22~~ | **23** | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | **29** | ~~30~~ |
| **31** | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | **37** | ~~38~~ | ~~39~~ | ~~40~~ |
| **41** | ~~42~~ | **43** | ~~-44-~~ | ~~45~~ | ~~46~~ | **47** | ~~48~~ | ~~49~~ | ~~50~~ |
| ~~51~~ | ~~52~~ | **53** | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | **59** | ~~60~~ |