Liczby Mersenne'a i Algorytm Lucas-Lehmer

Paweł Gliwny

26/04/2024

Liczby Mersenne'a

- Liczby Mersenne'a to specjalny rodzaj liczb, które sa definiowane jako liczby o jednostkach mniejszych o 1 od potegi liczby 2.
- Zapisywane sa jako $M_n = 2^n - 1$, gdzie n jest dodatnia liczba całkowita.
- Przykładowo, dla $n = 3$, $M_3 = 2^3 - 1 = 7$, co jest liczba Mersenne'a.

Liczby Mersenne'a (cd.)

- Nie wszystkie liczby Mersenne'a sa pierwsze.
- Aby liczba Mersenne'a była pierwsza, jej eksponent n musi być również liczba pierwsza, choć nawet to nie gwarantuje pierwszości M_n.

Algorytm Lucas-Lehmer

- Algorytm Lucas-Lehmer jest specyficzna metoda służaca do testowania, czy dana liczba Mersenne'a jest liczba pierwsza.
- Został on opracowany przez Édouarda Lucasa i później ulepszony przez D.H. Lehmera.

Algorytm Lucas-Lehmer (cd.)

- Algorytm Lucas-Lehmer dla liczby Mersenne'a M_p (gdzie p jest liczba pierwsza wieksza niż 2) działa nastepujaco:
  - Inicjalizacja: Ustal $S_0 = 4$.
  - Iteracja: Dla każdego k od 1 do $p-2$ oblicz $S_k = S_{k-1}^2 - 2$ modulo M_p.
  - Test: Jeśli S_{p-2} jest równy 0 modulo M_p, to M_p jest liczba pierwsza. W przeciwnym razie nie jest to liczba pierwsza.

Przykład działania algorytmu

Aby sprawdzić, czy $M_3 = 7$ jest liczba pierwsza, wykonujemy nastepujace kroki:

1. Obliczamy $S_1 = 4^2 - 2 \mod 7 = 14 \mod 7 = 0$.
2. Ponieważ $S_1 = 0$, możemy stwierdzić, że $M_3 = 7$ jest liczba pierwsza.

Wydajność algorytmu

- Algorytm Lucas-Lehmer jest stosunkowo prosty w implementacji.
- Jego wydajność zależy od wartości n: czas działania rośnie eksponencjalnie z wiekszymi wartościami n.