1 Projekt "*biblioteka algebry dużych liczb*"

1.1 Wymagania wstępne

- opracowanie dynamicznej reprezentacji dowolnej liczby $a \in \mathbb{N}$ w systemie o podstawie 10 oraz 2^i, gdzie $i \in \mathbb{N} \setminus \{0\}$;
- zaimplementowanie algorytmów wymienionych w punkcie 2.2;
- realizacja prostego zadania badawczego opisanego w punkcie 2.3;
- stworzenie dokumnetacji biblioteki w formacie HTML wraz z opisem i oszacowaniem złożoności pamieciowej oraz czasowej użytych algorytmów a także przedstawienie rozwiązania problemu badawczego;

1.2 Algorytmy

- podstawowe operacje arytmetyczne na liczbach naturalnych
  - dodawanie liczb;
  - odejmowanie liczb;
  - mnożenie liczb metodą klasyczną oraz za pomocą algorytmu Karatsuby (zobacz [3]);
  - dzielenie liczb bez reszty;
  - odwrotność całkowitoliczbowa (zobacz [2]);
  - dzielenie modulo liczb;
- algorytm Euklidesa (zobacz [1]);
- algorytm potęgowania modulo przez wielkorotne podnoszenie do kwadratu (zobacz [1]);
- niedeterministyczny test Millera-Rabina pierwszości liczby naturalnej (zobacz [1]);

1.3 Problem badawczy

Zaimplementowanie systemu kryptograficznego RSA przy użyciu algorytmów z projektowaniej biblioteki. Przeprowadzić eksperymenty badające wydajność systemu dla różnych algorytmów (np. mnożenie metodą klasyczną kontra algorytm Karatsuby).

2 Szczegółowy opis problemu badawczego

(pojawi się w połowie marca 2003)

Literatura

[1] T. H. Cormen, C. E. Leiserson, R. L. Rivest "*Wprowadzenie do algorytmów*", WNT, Warszawa 1997.

[2] A. V. Aho, J. E. Hopcroft, J. D. Ullman "*Projektowanie i analiza algorytmów komputerowych*", PWN, Warszawa 1983.

[3] P. Wróblewski "*Algorytmy struktury danych i techniki programowania*", HELION, Gliwice 1997.