Adam Karczewski, 235039
Michał Skrzęta, 235004

Prowadzący: Mgr inż. Dominik Żelazny

ARCHITEKTURA KOMPUTERÓW 2- PROJEKT

PLAN PRACY

Testowanie pierwszości

1. Plan pracy

   1.1 Etap pierwszy:

   - planowanie pracy
   - implementacja sita Eratostenesa,
   - implementacja testu pierwszości Fermata wraz z funkcją szybkiego potęgowania modularnego.

   1.2 Etap drugi:

   - naiwny test pierwszości na podstawie sita Eratostenesa,
   - implementacja testu Millera - Rabina,
   - test Solovaya - Strassena.

   1.3 Etap trzeci:

   - generacja liczb pierwszych sitem Atkina - Bernsteina,
   - chiński test pierwszości,
   - porównanie zaimplementowanych sit i testów oraz przykłady ich użycia.

2. Założenia projektu

   Projekt ma na celu zaimplementowanie podstawowych probabilistycznych testów pierwszości oraz deterministycznych sit wraz z naiwnym testem pierwszości. Projekt zostanie napisany w języku assembler składania AT&T, wersja 64- bitowa. W kodzie zostaną użyte funkcje z podstawowej biblioteki języka C – głównie funkcje związane z losowaniem.