Projekt Zespołowy

Etap projektu – projektowanie rozwiązania na zadaną architekturę

Autorzy:
Biernacka Kamila
Kania Dominik
Leśniak Mateusz
Maziarz Wojciech

kwiecień 2021

Streszczenie

Poniższe sprawozdanie jest wynikiem naszej pracy na drugim etapie projektu zespołowego z implementacji metody indeksu w architekturach GPU. Przedstawimy w nim przygotowane przez nas projekty i rysunki koncepcyjne wymaganych do zaimplementowania algorytmów.

Spis treści

1 Mnożenie modularne dużych liczb

2 Poszukiwanie relacji i faktoryzacja w bazie

2.1 Szybkie potęgowanie modularne

Metoda indeksu wymaga obliczenia wartości typu $a^b \ mod \ n$. Szybkie potęgowanie modularne jest prostym algorytmem pozwalającym zredukować liczbę mnożeń i dzieleń modulo z b do $O(log\ b)$.

Algorithm 1: `szybkie potęgowanie`

Input : podstawa potęgi a, wykładnik potęgi b, modulnik n
Output: $a^b \ mod \ n$

```
1  bits = to_bin(b)
2  nbits = length(bits)
3  a = a%n
4  result = 1
5  x = a
6  for i=0 to nbits do
7      if bits[i]==1 then
8          result = result * x
9          result = result%n
10     x = x * x
11     x = x%n
12 return result
```

2.2 Fakoryzacja w bazie

2.3 Budowa relacji

3 Eliminacja Gaussa w pierścieniu $\mathbb{Z}_{p-1}$

3.1 Algorytm Euklidesa

3.2 Rozszerzony algorytm Euklidesa