

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

<b>1</b>	<b>Mnożenie modularne dużych liczb</b>	<b>3</b>
<b>2</b>	<b>Poszukiwanie relacji i faktoryzacja w bazie</b>	<b>3</b>
2.1	Szybkie potęgowanie modularne . . . . .	3
2.2	Fakoryzacja w bazie . . . . .	3
2.3	Budowa relacji . . . . .	3
<b>3</b>	<b>Eliminacja Gaussa w pierścieniu <math>\mathbb{Z}_{p-1}</math></b>	<b>3</b>
<b>4</b>	<b>Rozszerzony algorytm Euklidesa</b>	<b>3</b>

- 1 Mnożenie modularne dużych liczb
- 2 Poszukiwanie relacji i faktoryzacja w bazie
  - 2.1 Szybkie potęgowanie modularne
  - 2.2 Faktoryzacja w bazie
  - 2.3 Budowa relacji
- 3 Eliminacja Gaussa w pierścieniu  $\mathbb{Z}_{p-1}$ 
  - 3.1 Algorytm Euklidesa
  - 3.2 Rozszerzony algorytm Euklidesa