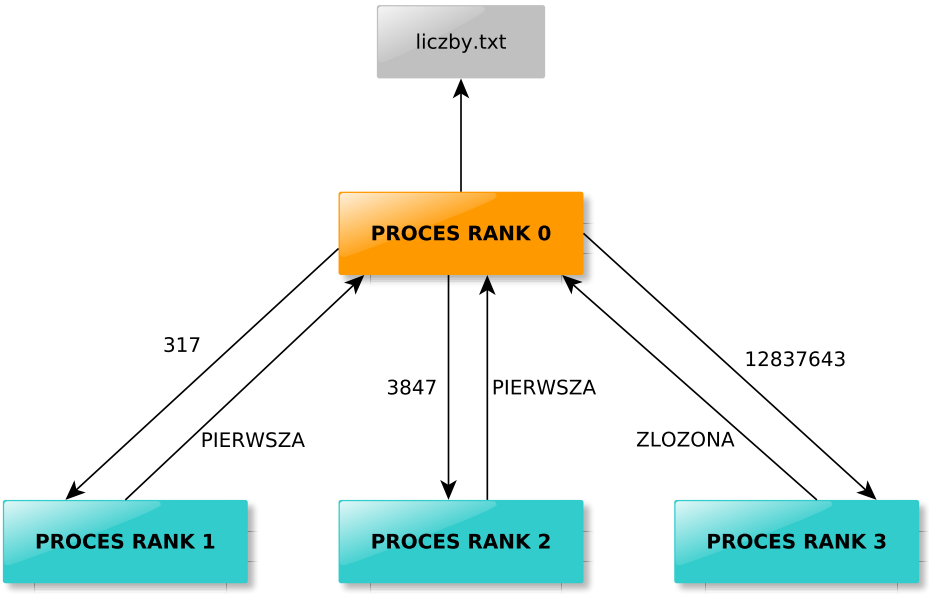
Cel zadania

Celem zadania jest zapoznanie z działaniem środowiska do obliczeń rozproszonym MPI.

Zadanie 7 - Test Millera-Rabina - MPI

Napisz program sprawdzający czy zadane liczby są liczbami pierwszymi za pomocą testu Millera-Rabina. Testowane liczby znajdują sie w pliku tekstowym, którego ściezka podana jest jako argument wykonania programu.

Program powinien mieć jeden proces, który odczytuje liczby z pliku *.txt i rozsyła je pomiędzy inne procesy, które testują te liczby i odsyłają informację czy liczba jest pierwsza czy złożona.



Rysunek 1: Rysunek poglądowy

Wskazówki

Algorytm działania testu Millera-Rabina:

1. przedstaw $n-1$ jako $2^s \cdot d$, gdzie s jest maksymalne,
2. wylosuj a ze zbioru $\{1, 2, ..., n-1\}$,
3. jeśli $a^d \equiv 1 \bmod n$ oraz $a^{2^r \cdot d} \equiv -1 \bmod n$, dla wszystkich r ze zbioru $\{0, 1, 2, ..., s-1\}$, to n jest złożona,
4. powtórz kroki 2 i 3 k razy,
5. jeśli w powyższych krokach liczba nie została wykryta jako złożona to przyjmujemy, że jest pierwsza.

Do potęgowania $a^{2^r \cdot d}$ możemy użyć algorytmu szybkiego potęgowania. Jest to algotym bazujący na przesunięciu bitowym.

Formaty

Przykładowy format pliku z liczbami:

```
317
287
12837643
3847
34568781
89737629
```

Przykładowe wyjście programu:

```
317: pierwsza
287: zlozona
12837643: zlozona
3847: pierwsza
34568781: zlozona
89737629: zlozona
Czas: 7.337s
```

Wymagania

Program powinien:

- wypisać informację czy podana liczba jest pierwsza czy złożona,
- mierzyć sumaryczny czas przetwarzania całego pliku liczb,
- wypisać czas obliczeń podany w ms.

Dokumentacja

Dokumentacja oprócz standardowych elementów powinna jeszcze zawierać wykresy zależności czasu obliczeń od ilości procesów oraz wykres przyśpieszenia. Mierzony czas powinien być nie mniejszy niż 3 s.

Położenie plików

- Program: `./zad7/miller_rabin`
- Dokumentacja LaTeX: `./zad7/dok.tex`
- Dokumentacja PDF: `./zad7/dok.pdf`

Uruchamianie

```
mpirun -n <count> ./miller_rabin <path> <k>
```

- `count` - liczba procesów,
- `path` - ścieżka do pliku z liczbami
- `k` - liczba powtórzeń dla testu Millera-Rabina

