Разложение чисел на множители

Тагиев Б. А.

23 ноября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Изучение задачи разложения на множители, изучение p-алгоритма Полларда.

p-алгоритм Полларда

- Вход. Число n, начальное значение c, функция f, обладающая сжимающими свойствами.
- Выход. Нетривиальный делитель числа n.

1. Положить $a = c, b = c$
2. Вычислить $a = f(a)(mod n), b = f(b)(mod n)$
3. Найти $d = GCD(a - b, n)$
4. Если $1 < d < n$, то положить $p = d$ и результат: p. При $d = n$ результат: ДЕЛИТЕЛЬ НЕ НАЙДЕН. При $d = 1$ вернуться на шаг 2.

Пример

```
6       41      1
41      123939  1
1686    391594  1
123939  438157  1
435426  582738  1
391594  1144026 1
1090062 885749  1181

result:  1181
```