Лабораторная работа №6 Разложение чисел на множители

ВОЛКОВА ДАРЬЯ АЛЕКСАНДРОВНА НПММД-02-21

Цель работы

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

Задачи

Программная реализация p-алгоритма Полларда.

Теоретические сведения

Разложение на множители — предмет непрерывного исследования в прошлом; и такие же исследования, вероятно, продолжатся в будущем. Разложение на множители играет очень важную роль в безопасности некоторых криптосистем с открытым ключом.

Результаты

```
: # p-метод Полларда
```

```
: from math import gcd
```

```
: ag = 1
  bg = 1
```

```
: def f(x, n):
      return (x*x+5)%n
```

```
: def method(n, a, b, d):
      a = f(a, n)%n
      b = f(f(b,n), n)%n
      d = gcd(a-b, n)
      if 1 < d < n:
          p = d
          print(p)
          exit()
      if d == n:
          print("Делитель не найден")
      if d == 1:
          global ag
          ag = b
          method(n, a, b, d)
```

```
: def main():
      n = 1359331
      c = 1
      a = c
      b = c
      a = f(a, n)%n
      b = f(a, n)%n
      d = gcd(a-b, n)
      if 1 < d < n:
          p = d
          print(p)
          exit()
      if d == n:
          pass
      if d == 1:
          method(n, a, b, d)
```

```
: main()
```

```
1181
```

Пример работы p-алгоритма Полларда

Выводы

В ходе выполнения работы удалось изучить задачу разложения на множители и p-алгоритм Полларда, а также реализовать данный алгоритм программно на языке Python.