РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Презентация ПО

ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Хиссен Али Уэддей
Группа: НПМмд-02-20
Ст. билет № 1032209306

Цель работы

Изучие алгоритм разложение чисел на множители..

Теоретические часть

Алгоритм, реализующий p-метод 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 ← НОД(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.

Например : найти p-методом Полларда нетривиальный делитель числа n=1359331. Положим c = 1 и f(x) = x^2^ + 5 (mod n).

Метод кеадратов. (Теорема Ферма о разложении)

Для любого положительного нечетного числа n существует взаимно однозначное соответствие между множеством делителей числа n, не меньших, чем $\sqrt{n}$, и множеством пар {s,t} таких неотрицательных целых чисел, что n = s^2^ - t^2^. Например . У числа 15 два делителя, не меньших, чем $\sqrt{15}$, — это числа 5 и 15. Тогда получаем два представления:

1. 15 = pq =3.5, откуда s = 4, откуда t= 1 и 15 = 4^2^ — 1^2^;
2. 15 = pq = 1.15, откуда s =8, откуда t = 7 и 15 = 8^2^ — 7^2^ .

програмная часть

Альгоритм, реализующий p-метод Полларда

результата вызова функцию, реализующая p-метод Полларда

Тогда пр n =1359331, его нетривиальный детитель равно 1181

```
1 AlgorithmPollard()
```

```
Введите n: 1359331
Введите c: 1
НОД(a,b) = 1
a=  6 b=  41 d=  1
НОД(a,b) = 1
a=  41 b=  123939 d=  1
НОД(a,b) = 1
a=  1686 b=  391594 d=  1
НОД(a,b) = 1
a=  123939 b=  438157 d=  1
НОД(a,b) = 1
a=  435426 b=  582738 d=  1
НОД(a,b) = 1
a=  391594 b=  1144026 d=  1
НОД(a,b) = 1181
a=  1090062 b=  885749 d=  1181
Нетривиальный делитель равно
 1181
```

Альгоритм, реализующий метод Квадратов

резултат работы метода

```
33
34                print("{} можно преставит в виде {} -{}".format(n,s**2,t**2))
35
```

```
Введите нечетное число n: 75
тогда получаем 3 представление
75 можно преставит в виде 100 -25
75 можно преставит в виде 196 -121
75 можно преставит в виде 1444 -1369
```

вывод Мы изучали алгоритм для разложния чисел на множители..