МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «СГУ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

АЛГОРИТМЫ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

ЛАБОРАТОРНАЯ РАБОТА №18

студента 4 курса 431 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Никитина Арсения Владимировича

Проверил
доцент _____ А. С. Гераськин

Саратов 2022

СОДЕРЖАНИЕ

1 Задание лабораторной работы

Разложение на мнодители полиномов над конечными полями:

— Алгоритм Бэрликемпа.

2 Теоретическая часть

Разложение полиномов на свободные от квадратов мно- множители (Polynomial Squarefree Factorization)

Вход: Нормированный свободный от квадратов полином $p(x)$ над $GF(p)$, $\deg[p(x)] = n$.

Выход: Неприводимые сомножители полинома $p(x)$ над $GF(p)$.

1. Построить матрицу Q размерности $n \times n$.
2. Триангулировать матрицу $Q - I$, вычислив ее ранг $n - r$ и найдя нульпространство матрицы $Q - I$, то есть найти r линейно независимых векторов $b_1, \ldots, b_r$, таких, что $b_j[Q - I] = 0, j = \overline{1, r}$. Первый вектор всегда может быть выбран в виде $(1, 0, \ldots, 0)$, что представляет тривиальное решение $b_1(x) = 1$ уравнения.
3. Вычисление сомножителей. Пусть $b_2(x)$ — полином, соответствующий вектору b_2. Вычислим $\gcd(p(x), b_2(x) - s)\ \forall s \in GF(p)$. В результате данной операции будет получено нетриваиельное разложение полинома $p(x)$. Если с использованием $b_2(x)$ получено менее r сомножителей, вычислим $\gcd(w(x), b_k(x) - s)\ \forall s \in GF(p)$ и для всех сомножителей $w(x)$, найденных к данному времений для $k = \overline{3, r}$, пока не будет найдено r сомножителей. Таким образом гарантируется, что будут найдены все сомножители полинома $p(x)$. Если p достаточно мало, то вычисления на данном шаге можно считать эффективными. Считается, что если $p > 25$, следует использовать более эффективные алгоритмы.

3 Практическая часть

3.1 Пример работы алгоритма

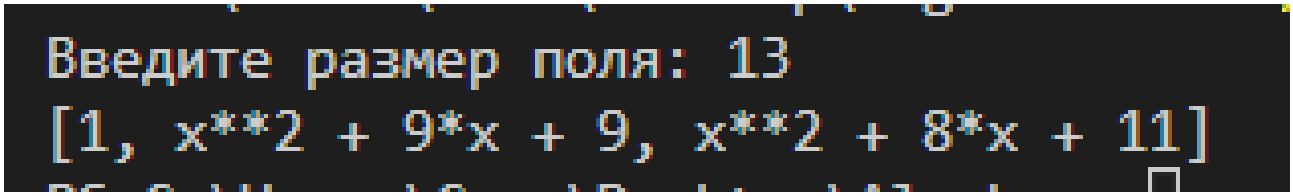

Рисунок 1

3.2 Код программы, реализующей рассмотренный алгоритм

```
import random
cnt = 30
ls = []
while cnt:
    a = random.randrange(5, 10)
    b = random.randrange(10, 20)
    c = random.randrange(20, 41)
    d = random.randrange(2, 6)
    if a + b + c + d > 55:
        ls.append((a, b, c, d))
        print(cnt)
        cnt -= 1
print(*ls, sep='\n')
```