Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчёт**

**по лабораторной работе №3**

**Дисциплина: КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ**

**Тема: «Кольцо многочленов»**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ К. А. Корнилов

Направление подготовки 02.03.02 Фундаментальная информатика и

информационные технологии

Направленность (профиль) Математическое и программное обеспечение

компьютерных технологий

Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. А. Крамаренко

**Тема:** Кольцо многочленов.

**Цель:** Изучение операций и свойств кольца многочленов.

**Ход работы:**

1. Умножить и разделить с остатком многочлен на многочлен в поле GF(2)
   1. F = x^3+x+1 G = x + 1
      1. F \* G = x^4 + x^3 +x^2 + x + x + 1 = x^4 + x^3 + x^2 + 1
      2. F/G = (x+1) \* (x^2 + x) + 1
   2. F = x^2+1 G = x + 1
      1. F \* G = x^3 + x^2 + x + 1
      2. F/G = (x+1) \* (x + 1)
   3. F = x^3+x^2+1 G = x^2 + 1
      1. F \* G = x^5 + x^3 +x^4 +x^2 + x^2 + 1= x^5 + x^4 + x^3 + 1
      2. F/G = (x^2+1) \* (x + 1) + x + 1
   4. F = x^4+x^2+1 G = x^2 + x + 1
      1. F \* G = x^6 + x^5 + x^4 +x^4 + x^3 + x^2 + x^2 + x + 1= x^6 + x^5 + x^3 + x + 1
      2. F/G = (x^2 + x+1) \* (x^2 + x + 1)
   5. F = x^4+x^2 + x+1 G = x + 1
      1. F \* G = x^5 + x^4 + x^3 + x^2 + x + x + 1= x^5 + x^4 + x^3 + 1
      2. F/G = (x+1) \* (x^3 + x^2 + 1)
   6. F = x^5 + x^3+x^2+1 G = x^2 + x + 1
      1. F \* G = x^7 + x^6 + x^5 +x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^2 + x + 1 = x^7 + x^6 + x + 1
      2. F/G = (x^2 + x + 1) \* (x^3 + x^2 + x + 1)
2. Найти нод указанных многочленов над полем GF
   1. R1 = X^5 +1 R2 = X^3 + X^2 + X +1

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| X^2+X | X^5+1 | X^3+X^2+X+1 | X+1 |
| X^2+1 | X^3+X^2+X+1 | X+1 | 0 |
| 0 | **X+1** | 0 | 0 |

* 1. R1 = X^5 + X^4 + 1 R2 = X^4 + X^3 + X + 1

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| X | X^5 + X^4 + 1 | X^4 + X^3 + X + 1 | X^2 + X + 1 |
| X^2+1 | X^4 + X^3 + X + 1 | X^2 + X + 1 | 0 |
| 0 | **X^2 + X + 1** | 0 | 0 |

* 1. R1 = X^5 + X^4 + 1 R2 = X^4 + X^3 + X + 1

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| X | X^5 + X^3 + X^2 + 1 | X^4 + 1 | X^3 + X^2 + X + 1 |
| X+1 | X^4 + 1 | X^3 + X^2 + X + 1 | 0 |
| 0 | **X^3 + X^2 + X + 1** | 0 | 0 |

* 1. R1 = X^5 + X^4 + X^3 + X R2 = X^5 + X^3 + X^2 + X

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 1 | X^5 + X^4 + X^3 + X | X^5 + X^3 + X^2 + X | X^4 + X^2 |
| X | X^5 + X^3 + X^2 + X | X^4 + X^2 | X^2 + X |
| X^2 + X | X^4 + X^ 2 | X^2 + X | 0 |
| 0 | **X^2 + X** | 0 | 0 |

1. Выяснить является ли данный многочлен неприводимым и примитивным над полем GF(2)
   1. Для проверки на неприводимость нужно проверить делится ли данный многочлен на любой многочлен степени <=deg(f)/2, где f – рассматриваемый многочлен.  
      Если многочлен является неприводимым, то тогда будем проверяться на примитивность. Для этого нужно показать, что есть такой корень многочлена, что его порядок будет 2^deg(f) – 1.
      1. F(X) = x^2+1  
         Делится на x+1 по признаку деления => приводим => не может быть примитивным
   2. F(x) = x^3 + 1  
      Делится на x+1 по признаку деления => приводим => не может быть примитивным
   3. F(X) = X^2 + X +1 – неприводим => может быть примитивным.  
      Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
      ф(4) = 2  
      g^2 = x^2 mod x^2 + x + 1 = x + 1 <> 1  
      g^3 = x^3 mod x^2 + x + 1 = x^2 + x mod x^2 + x + 1 = x + x + 1 = 1 =>  
      Покажем, что элементы все есть: x,x^2=x+1,x^3 = 1 => многочлен примитивный
   4. F(x) = x^3 + x  
      Делится на x+1 по признаку деления => приводим => не может быть примитивным
   5. F(X) = X^3+ X +1 – неприводим => может быть примитивным.  
      Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
      ф(8) = 4  
      g^2 = x^2 mod x^3 + x + 1 = x^2 <> 1  
      g^7 = x^7 mod x^3 + x + 1 = x \* (x+1) \* (x+1) = x\*(x^2+1) = x^3 + x = x + 1 + x = 1 => многочлен примитивный
   6. F(x) = x^3 + x^2  
      Делится на x+1 по признаку деления => приводим => не может быть примитивным
   7. F(X) = X^3+ X^2 +1 – неприводим => может быть примитивным.  
      Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
      ф(8) = 4  
      g^2 = x^2 mod x^3 + x^2 + 1 = x^2 <> 1  
      g^7 = x^7 = x\*(x^4+1) = x\* ( x^3 + x + 1) = x \* ( x^2 + 1 + x + 1) = x^3 + x^2 = x^2 + 1 + x^2 = 1 => примитивный
   8. F(x) = x^3 + x^2 + x  
      Делится на x по признаку деления => приводим => не может быть примитивным
   9. F(x) = x^3 + x^2 + x + 1  
      Делится на x+1 по признаку деления => приводим => не может быть примитивным
   10. F(x) = x^4 + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   11. F(X) = X^4+ X +1 – неприводим => может быть примитивным.  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(16) = 8  
       g^4 = x^4 mod x^4 + x + 1 = x+1 <> 1  
       g^15 = x^15 = (x+1)^3 \* x^3 = (x^2+1) \* (x+1) \* x^3 = (x^2+1) \* (x^3 + x + 1) = x^5 + x^3 + x^2 + x^3 +x + 1 = x^2 +x + x^2 + x + 1 = 1=> примитивный
   12. F(x) = x^4 + x^2  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   13. F(x) = x^4 + x^2 + 1  
       Делится на x^+x + 1 => приводим => не может быть примитивным
   14. F(x) = x^3 + x^2 + x + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   15. F(X) = X^4+ X^3 +1 – неприводим => может быть примитивным.  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(16) = 8  
       g^4 = x^2 mod x^4 + x^3 + 1 = x^3+1 <> 1  
       g^15 = x^15 = x^4+x^3 = 1=> примитивный
   16. F(x) = x^4 + x^3 + x^2 + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   17. F(X) = X^4+ X^3 + X^2 + X + 1 – неприводим => может быть примитивным.  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(16) = 8  
       g^4 = x^4 mod x^4 + x^3 + x^2 + x + 1 = x^3 + x^2 + x + 1 <> 1  
       g^15 = x^15 = (x^3+x^2+x+1)^3 \* x^3 = 1=> Покажем,что есть все элементы: x, x^2, x^3, x^4 = x^3 + x^2 + x + 1, x^5 = 1 =>условие выполнено, но у нас есть циклическая подгруппа внутри => раз для произвольного корня нет выполнено наличие всех элементов => не примитивный
   18. F(x) = x^5 + x^3 + x + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   19. F(x) = x^5 + x^3 + x^2 + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   20. F(x) = x^5 + x^4 + x^3 + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   21. F(x) = x^5 + x^4 + x^2 + 1  
       Делится на x+1 по признаку деления => приводим => не может быть примитивным
   22. F(x) = x^5 + x^4 + x^3 + x^2 + 1 = >неприводим  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(32) = 16  
       g^8 = x^8 mod x^5 + x^4 + x^3 + x^2 + 1 = x^4 + x^3 + x^2 <> 1  
       g^31 = x^31 = (x^5+x^4+x^3+x^2) = 1=> Покажем,что есть все элементы: x, x^2, x^3, x^4, x^5 = x^4+x^3+x^2+1, x^6 = x^2+x+1, x^7 = x^3 +x^2+x, x^8 = x^4+x^3+x^2, x^9=x^2+1, x^10 = x^3+x, x^11=x^4+x^2, x^12 = x^4+x^2+1, x^13 = x^4+x^2+x+1, x^14 = x^4+x+1, x^15 = x^4+x^3+x+1, x^16 = x^3+x+1, x^17 = x^4+x^2+x, x^18 = x^4+1, … x^31 = 1 => примитивный
   23. F(x) = x^5 + x^4 + x^3 + x + 1 = >неприводим  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(32) = 16  
       g^8 = x^8 mod x^5 + x^4 + x^3 + x + 1 = x^4 + x^3 + x <> 1  
       g^31 = x^31 = (x^5+x^4+x^3+x) = 1=> Покажем,что есть все элементы: x, x^2, x^3, x^4, x^5 = x^4+x^3+x+1, … x^31 = 1 => примитивный
   24. F(x) = x^5 + x^3 + 1 = >неприводим  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(32) = 16  
       g^8 = x^8 mod x^5 + x^3 + 1 = x^4 + x^3 + 1 <> 1  
       g^31 = x^31 = 1=> Покажем,что есть все элементы: x, x^2, x^3, x^4, x^5 = x^3+1, … x^31 = 1 => примитивный
   25. F(x) = x^5 + x^3 + 1 = >неприводим  
       Пусть g = x – корень. Тогда проведем проверку аналогично первообразным элементам в обычном поле по числовому модулю.  
       ф(32) = 16  
       g^8 = x^8 mod x^5 + x^3 + 1 = <> 1  
       g^31 = x^31 = (x^5+x^3+1) = 1=> Покажем,что есть все элементы: x, x^2, x^3, x^4, x^5 = x^3 + 1, … x^31 = 1 => примитивный
2. Построить таблицу умножения в поле Галуа GF(8) c образующим многочленом 1101

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 000 | 000 | 000 | 000 | 000 | 000 | 000 | 000 | 000 |
| 001 | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 010 | 000 | 010 | 100 | 110 | 101 | 111 | 001 | 0111 |
| 011 | 000 | 011 | 110 | 101 | 001 | 010 | 111 | 100 |
| 100 | 000 | 100 | 101 | 001 | 111 | 011 | 010 | 110 |
| 101 | 000 | 101 | 111 | 010 | 011 | 110 | 100 | 001 |
| 110 | 000 | 110 | 001 | 111 | 010 | 100 | 011 | 101 |
| 111 | 000 | 111 | 011 | 100 | 110 | 001 | 101 | 010 |

1. Построить таблицу умножения в поле Галуа GF(8) c образующим многочленом 1011

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 000 | 000 | 000 | 000 | 000 | 000 | 000 | 000 | 000 |
| 001 | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 010 | 000 | 010 | 100 | 110 | 001 | 011 | 101 | 111 |
| 011 | 000 | 011 | 110 | 010 | 111 | 001 | 100 | 101 |
| 100 | 000 | 100 | 001 | 111 | 101 | 010 | 011 | 110 |
| 101 | 000 | 101 | 011 | 001 | 010 | 110 | 111 | 100 |
| 110 | 000 | 110 | 101 | 100 | 011 | 111 | 010 | 001 |
| 111 | 000 | 111 | 111 | 101 | 110 | 100 | 001 | 011 |

1. Найти примитивные элементы для поля из задачи 4  
   Пусть g = x  
   Проверим наличие всех элементов: x,x^2,x^2+1,x^2+x+1,x+1,x^2+x,1 => g=x – образующий элемент

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2,x^4=x^2+x+1

1. Найти примитивные элементы для поля из задачи 5  
   Пусть g = x  
   Проверим наличие всех элементов: x,x^2,x+1,x^2+x,x^2+x+1,x^2+1,1 => g=x – образующий элемент

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2,x^4=x^2+x

1. Найти примитивные элементы для поля GF(16) и полинома из x^4+x^3+1  
   Пусть g = x – корень. Образующий полином является примитивным (раннее проверяли)

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2,x^4, x^8=(x^3+1)\*(x^3+1) = x^3+x^2+x

1. Найти примитивные элементы для поля GF(16) и полинома из x^4+x+1  
   Пусть g = x – корень. Образующий полином является примитивным (раннее проверяли)

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2,x^4=x+1, x^8= x^2+1

1. Найти примитивные элементы для поля GF(64) и полинома из x^6+x+1  
   Пусть g = x – корень. Образующий полином является примитивным (раннее проверяли)

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2,x^4, x^8=x^3+x^2,x^16=x^4+x+1,x^32=x^3+1

1. Найти примитивные элементы для поля GF(64) и полинома из x^6+x^3+1  
   Пусть g = x – корень. Образующий полином является примитивным (раннее проверяли)

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2, x^4, x^8=x^5+x^2, x^16=x^4+x, x^32=x^5 + x^2 +1

1. Найти примитивные элементы для поля GF(64) и полинома из x^6+x^4+x^2+x+1  
   Пусть g = x – корень. Образующий полином является примитивным (раннее проверяли)

Тогда g^(2^i) – также будет образующим элементом и корнем образующего полинома=> Корни: x, x^2, x^4, x^8=x^6+x^4+x^3+x^2, x^16=x^4+x, x^32=x^3+x^2+x+1

1. Умножить 2-битовые слова, используя полиномы:
   1. (11)x(10) = (x+1)\*x = x^2+x
   2. (1010)x(1000) = 1010000 = x^6+x^4
   3. (11100)x(10000) = x^8+x^7+x^6
2. Найти мультипликативную инверсию следующих полиномов в GF(2^2):
   1. 1 = (x^3) => a = 1^-1 = x^-3 = x^0 = 1
   2. x = g^1  
      a = x^-1 = g^-1 = g^2=x^2 = x+1
   3. x+1 = g^2  
      a = (x+1)^-1 = g^-2 = g^(3-2) = g = x
3. Используя расширенный евклидов алгоритм найти инверсию x^4+x^3+1 в GF(2^5) по модулю x^5+x^2+1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | R1 | R2 | R | T1 | T2 | T |
| X+1 | X^5+x^2+1 | X^4+x^3+1 | X^3+x^2+x | 0 | 1 | X+1 |
| X | X^4+x^3+1 | X^3+x^2+x | X^2+1 | 1 | X+1 | X^2+x+1 |
| X+1 | X^3+x^2+x | X^2+1 | 1 | X+1 | X^2+x+1 | X^3+x |
| X^2+1 | X^2+1 | 1 | 0 | X^2+x+1 | X^3+x |  |
| 0 | 1 | 0 | 0 | **X^3+x** |  |  |

(X^4+x^3+1)^-1 = x^3+x

1. Создайте таблицу сложения и умножения GF(2^4), используя x^4+x^3+1 как модуль

import numpy as np

# Определяем элементы GF(2^4) как многочлены

# Представляем элементы как числа от 0 до 15 (0000 - 1111 в двоичном виде)

gf2\_4\_elements = list(range(16))

# Модульный многочлен: x^4 + x^3 + 1 -> 0b10011 (19 в десятичной системе)

modulus = 0b10011

# Функция для сложения в GF(2^4) (покомпонентный XOR)

def gf2\_4\_add(a, b):

return a ^ b

# Функция для умножения в GF(2^4) с приведением по модулю

def gf2\_4\_multiply(a, b, mod=modulus):

result = 0

while b:

if b & 1: # Если младший бит b установлен, прибавляем (XOR)

result ^= a

b >>= 1 # Сдвигаем b вправо (деление на x)

a <<= 1 # Умножаем a на x (сдвиг влево)

if a & 0b10000: # Если степень x^4 появляется, приводим по модулю

a ^= mod

return result

# Создаем таблицы сложения и умножения

addition\_table = np.zeros((16, 16), dtype=int)

multiplication\_table = np.zeros((16, 16), dtype=int)

for i in range(16):

for j in range(16):

addition\_table[i][j] = gf2\_4\_add(i, j)

multiplication\_table[i][j] = gf2\_4\_multiply(i, j)

# Выводим таблицы

addition\_table, multiplication\_table

1. Выполнить операцию: (100)/(010) = 100 \* 010^-1=100\*110=010=x
2. Реализовать проверку многочлена на неприводимость и примитивность, сложение и умножение.

Для этого был написан класс, принимающий на вход строку с полиномом модулем. Данная строка внутри парсится в векторное двоичное представление полинома

Для сложения полиномов был реализован внутренний метод, которые обеспечивает сложению по модулю 2 коэффициентов полиномов и срез незначащих нулей.

Для того,чтобы полиномы оставались в поле по нужному полю была реализована функция, выполняющая деление полиномов в столбик. Для этого в цикле каждый раз создается новый полином равный делитель \* 10^i. Затем происходит сложение текущего значения делимого и полученного полинома и выполняется проверка на размер делимого. Если его длина меньше делителя,то процесс заканчивается.

Для реализации умножения была написана функция, осуществляющая умножения полиномов в столбик. На каждом шаге производится умножения на 10 результата и сложение по модулю 2 с произведением текущей цифры первого множителя и второго множителя.

В конце операций сложения и умножения производится перевод из вектора в полином с помощью отдельной функции.

Для проверки на неприводимость необходимо проверить делится ли полином f на полиномы r со степенью deg(r)<=deg(f)//2. Для этого сначала создается словарь примитивных полиномов до степени def(f)//2. Для этого проверяемый полином с помощью функции деления делится на все уже известные примитивные полиномы. После получения всех примитивных полиномов, удовлетворяющих условию по степени, производится их поочередное деление на полином f. Если нет нигде деления без остатка, то полином f – неприводимый.

Для проверки на примитивность осуществляется сначала проверка на неприводимость. Затем производится возведения в степени 1..2^deg(f)-1 произвольного корня полинома f, записанного как [1,0]. Если порядок корня равен 2^deg(f) – 1, то полином примитивный.

**Вывод:** Были изучены операции в полях Галуа.