Магистры 2 КУРС
весна 2021

СЕМЕСТРОВОЕ ЗАДАНИЕ
ПО КУРСУ Доп. главы фундаментальной математики

Каждый студент выбирает себе один из вариантов

У всех разные.

И оформляет решение в виде семестрового задания.

Образцы решений приведены в практиках.

С которыми нужно ознакомиться и применить их для решения своего варианта.

ЗАДАЧА № 1

1. Для многочлена f(x) над полем P проверить неприводимость.
2. Построить поле Q разложения многочлена f(x).
3. Найти примитивный элемент g поля Q.
4. Составить таблицу степеней примитивного элемента g.
5. Составить таблицу логарифмов Якоби элемента g.
6. Используя таблицы степеней и логарифмов Якоби решить

а) систему линейных уравнений над полем Q

$$\begin{cases} x+(\alpha+1)\,\mathrm{y}-\mathrm{z}=2 \\ (3\alpha+1)\,\mathrm{x}+2\,\mathrm{y}+\mathrm{z}=3 \\ x+2y+3\mathrm{z}=\alpha^2+5 \end{cases},$$

б) квадратное уравнение $(\alpha+1)\,\mathrm{x}^2+(\alpha^2+\alpha+1)\,\mathrm{x}+\alpha^2+1.$

ВАРИАНТЫ

1. $f(\mathrm{x})=\mathrm{x}^4+x^3+1, P=GF(2)$
2. $f(\mathrm{x})=\mathrm{x}^4+x+1, P=GF(2)$
3. $f(\mathrm{x})=\mathrm{x}^4+x^3+x^2+x+1, P=GF(2)$
4. $f(\mathrm{x})=x^3+x-1, P=GF(3)$
5. $f(\mathrm{x})=x^3+x^2-1, P=GF(3)$

6. $f(\mathrm{x}) = x^3 - x^2 + 1, P = GF(3)$
7. $f(\mathrm{x}) = x^3 - x + 1, P = GF(3)$
8. $f(\mathrm{x}) = x^2 + 2, P = GF(5)$
9. $f(\mathrm{x}) = x^2 + 3, P = GF(5)$
10. $f(\mathrm{x}) = x^2 + x + 1, P = GF(5)$
11. $f(\mathrm{x}) = x^2 + x + 2, P = GF(5)$
12. $f(\mathrm{x}) = x^2 + 2x + 3, P = GF(5)$
13. $f(\mathrm{x}) = x^2 + 2x + 4, P = GF(5)$
14. $f(\mathrm{x}) = x^2 + 3x + 3, P = GF(5)$
15. $f(\mathrm{x}) = x^2 + 3x + 4, P = GF(5)$
16. $f(\mathrm{x}) = x^2 + 4x + 1, P = GF(5)$
17. $f(\mathrm{x}) = x^2 + 4x + 2, P = GF(5)$

ЗАДАЧА № 2

1. Эллиптическую кривую f(x,y) над полем P привести к каноническому виду g(x,y)

$$\mathrm{f}(\mathrm{x}, \mathrm{y}) = \mathrm{y}^2 + axy + 5y = x^3 + bx^2 + 8x + 9$$

2. Вычислить количество точек на кривой g(x,y)
3. Найти элемент наибольшего порядка кривой g(x,y)

ВАРИАНТЫ

1. $a = 3, b = 3, P = GF(5)$
2. $a = 3, b = 7, P = GF(5)$
3. $a = -1, b = 4, P = GF(5)$
4. $a = 2, b = 2, P = GF(5)$
5. $a = 3, b = 6, P = GF(7)$
6. $a = 3, b = 5, P = GF(7)$
7. $a = 4, b = 6, P = GF(7)$
8. $a = 4, b = 2, P = GF(7)$
9. $a = 4, b = 2, P = GF(11)$

10. $a=4, b=6, P=GF(11)$
11. $a=1, b=3, P=GF(11)$
12. $a=6, b=10, P=GF(11)$
13. $a=6, b=10, P=GF(13)$
14. $a=6, b=1, P=GF(13)$
15. $a=3, b=5, P=GF(13)$
16. $a=2, b=12, P=GF(13)$
17. $a=10, b=5, P=GF(13)$

ЗАДАЧА № 3

Используя язык программирования Julia и его пакеты Primes и Nemo.

1. Построить систему RSA с простыми числами p и q, имеющими 10 знаков в десятичной записи, т.е. $n=pq$ двадцатизначное число.

2. Зашифровать число $x=abc$,

где a – количество букв в фамилии,

b – имени,

c – отчестве студента.

Пусть получилось число y.

3. Расшифровать число y.

Д.ф.-м.н., профессор,
Профессор кафедры ФАА Рожков А.В.
05.02.2021