

Вычисления в полях Галуа

Задание 1

Для многочлена $f(x) = x^2 + ax + b$ над полем $GF(p)$ решить несколько задач.

1. Проверить неприводимость многочлена $f(x)$ над полем $GF(p)$
2. Построить поле разложения многочлена $f(x)$.
3. Найти примитивный элемент α поля $GF(p^2)$, заданного как поле разложения многочлена $f(x)$

Составить таблицу степеней примитивного элемента α

Построить таблицу сложения и умножения многочленов. $a=7, b=N_9$ в журнале. Если многочлен приводим, то изменить a .

Задание 2

Для многочлена $f(x) = x^3 + ax^2 + bx + c$ над полем $GF(p)$ решить несколько задач.

1. Проверить неприводимость многочлена $f(x)$ над полем $GF(p)$
2. Построить поле разложения многочлена $f(x)$.
3. Найти примитивный элемент α поля $GF(p^3)$, заданного как поле разложения многочлена $f(x)$

Составить таблицу степеней примитивного элемента α

$P \sim n \cdot 1000$, где n – номер в журнале.

$a=2, b=10, c=171$. Если многочлен приводим, то изменить a .