«Методика прикладных вычислений в конечных полях»

- **Цель работы:**

на основе изученной учебно-методической и научной литературы по теме исследования разработать элективный курс по теме «Вычисление в конечных полях » для учащихся 10-11 класса профильного уровня подготовки.

- **задачи:**

Изучить, обобщить и систематизировать теоретический материал в учебно-методической и научной литературе по теме исследования.

Разработать содержание занятий элективного курса и наглядный демонстрационный материал для их проведения.

№ п/п	Наименование темы	Общее кол-во часов
1	Конечные поля. Аксиомы поля.	1
2	Поля из четырех элементов.	1
3	Алгоритмы вычислений в конечных полях(сложение, разность, произведение)	2
4	Алгоритмы вычислений в конечных полях(деление). Вычисление обратного элемента	2
5	Бинарный алгоритм возведения в степень. Проверка элемента на примитивность	2
6	Вычисление степеней	3
	Итого:	11

«Алгоритмы вычислений в конечных полях.»

- Цель урока:

научить находить произведение сумму и разность элементов конечного поля.

- Задачи:

Закрепить вычисление операций в конечном поле.

Закрепить лекционный материал на практике.

Для вычисления $\gamma_1 \mp \gamma_2$ достаточно в выражении $q_1(\beta) \mp q_2(\beta)$ привести подобные члены

Пусть $f(x) = x^3 + 2x + 1 \in F_3[x]$. Он неприводим в F_3. Вычислить сумму, разность элементов $\gamma 1 = \beta + 1$ и

$\gamma 2 = \beta^2 + \beta + 2.$

Ясно что

$$\gamma_1 + \gamma_2 = (\beta + 1) + (\beta^2 + \beta + 2) = \beta^2 + 2\beta;$$

$$\gamma_1 - \gamma_2 = (\beta + 1) - (\beta^2 + \beta + 2) = -\beta^2 - 1 = 2\beta^2 + 2;$$

Чтобы найти каноническое представление произведения $\gamma_1 \gamma_2 = q_1(\beta)q_2(\beta)$ нужно многочлен $q_1(\beta)q_2(\beta)$ разделить в кольце $P[x]$ на многочлен $f(x)$ с остатком:

$$q_1(x)q_2(x) = f(x)h(x) + r(x)$$