ВТОРАЯ КОНТРОЛЬНАЯ

Определения вспомогательные

- **Неприводимый многочлен** — это многочлен, который не может быть разложен на произведение многочленов более низкой степени с коэффициентами из того же поля. Он играет роль, похожую на простые числа в теории чисел: неприводимые многочлены — это «основные блоки» в алгебраических структурах, из которых можно составить другие многочлены.
- **Поле Галуа** - это особый вид поля, который содержит конечное количество элементов. Такие поля обозначаются как F_{p^n}, где:
  - p - простое число
  - n - степень расширения поля
- Основные свойства поля Галуа.
  i. Конечное число элементов
  ii. Циклическая мультипликативная группа (любой элемент группы может быть выражен как степень другого ($g, g^2, ...g^{p^n-1}$)
  iii. Простота алгебраической структуры. В поле выполняются все правила, что и в рациональном поле (деления на ноль тоже нету)
- **Мультипликативная группа** $F^*_{3^3}$ Это все ненулевые элементы поля F_{3^3}, то есть $27 - 1 = 26$ элементов
- **Порядок элемента** - наименьшее число k, для которого $a^k = 1$.

Первая задачка

1. **Найти порядок элемента x^2, принадлежашего к мультипликативной группе поля Галуа $F^*_{3^3}$, построенного относительно неприводимого многочлена $x^3 + 2x^2 + 1$**

   i. Находим порядок группы $F^*_{3^3}$: поскольку это группа ненулевых элементов конечного поля F_{3^3}, то порядок равен $27 - 1 = 26$

   ii. Находим порядок x^2. Поскольку группа циклическая, то порядок любого элемента должен быть делителем порядка группы, то есть одно из чисел $(1, 2, 13, 26)$.

   iii. Проверим возведение x^2 в степень

   - Если $(x^2)^{13} = 1$, то порядок равен 13
   - Если $(x^2)^{13} \neq 1$, то порядок равен 26

   iv. Рассчитаем $(x^2)^{13}$

Вычислим (x^4):

Сначала выразим (x^3) через (x^2) и (x) с помощью многочлена (f(x)):

$$f(x) = x^3 + 2x^2 + 1 = 0 \implies x^3 = -2x^2 - 1$$

В поле F_3 (где арифметика по модулю 3):

$$-2x^2 - 1 \equiv x^2 + 2 \pmod 3$$

Таким образом, имеем:

$$x^3 \equiv x^2 + 2$$

Пусть $y = x^2$, тогда

$$y^2 = x^4 = x^3 * x = (x^2 + 2)x = x^3 + 2x = x^2 + 2x + 2$$

Значит, $0(x^2) \neq 2$

$$y^3 = y^2 * y = (x^2 + 2x + 2)x^2 = x^4 + 2x^3 + 2x^2 =$$

$$= x^2 + 2x + 2 + 2x^2 + 4 + 2x^2 = 5x^2 + 2x + 6 = 2x^2 + 2x$$

$$y^6 = (y^3)^2 = (2x^2 + 2x)^2 = (-x^2 - x)^2 = x^4 + 2x^3 + x^2 = x^2 + 2x$$

$$y^7 = y^6 * y = (x^2 - x) * x^2 = x^4 - x^3 = x^2 + 2x + 2 - x^2 - 2 = 2x$$

$$y^{14} = (y^7)^2 = 4x^2 = x^2 \Rightarrow y^{14} = y \Rightarrow y^{13} = 1$$

Значит порядок $y = x^2$ равен 13.

Ответ: 13

Определения

- **Эллептическая кривая** - эллиптическая кривая над полем F_p, где p - простое число, задается уравнением

$$y^2 = x^3 + ax + b$$

  где a и b - коэффиценты, принадлежащие полю F_p. Кривая должна удовлетворять условию, что её дискриминант не равен нулю.
- **Группа точек эллиптической кривой -** удовлетворяют свойствам:
  - Сумма двух точек на кривой также лежит на кривой
  - Для точки (x, y) ее обратной является $(x, -y)$, где $-y$ берется по модулю 13
  - Точка на бесконечности O, где для любой P выполняется $O + P = P$
- **Исследовать группу точек эллиптической кривой**
  - Найти все точки (x, y) на кривой над полем F_{13}

- Определить порядок группы, то есть количество точек над кривой, включая точку на бесконечности
- Изучить свойства группы, такие как наличие подгрупп.

Вторая задачка

https://edu.hse.ru/pluginfile.php/3851506/mod_resource/content/1/Семинар 06.pdf

2. Построить и исследовать группу точек эллиптической кривой $E_{2,2}(F_{13})$

   Уравнение элиптической кривой $E_{a,b}$:

   $$y^2 = x^3 + ax + b$$

   Для начала я проверю, что параметры удовлетворяю условию гладкости.

   $$\Delta = -16(4a^3 + 27b^2) \neq 0$$

   Не забывать, что все могу брать по модулю поля (13), что упрощает нахождение и дискриминанта и просто проживания в этом мире.

   Само решение:

   i. Сначала расписать все элементы поля и рассчитать “удобное” извлечение корня из них (все еще учитывать модуль 13)

   ii. Затем для каждого x посчитать y (расписать на всю страницу). Как раз в этом шаге помогает нам предыдущий.

   iii. Выписать все в ряд и посчитать количество: $E_{2,2}(F_{13}) = \{0, (-5, -6)....(6, 3)\} = 15$

   iv. Выписать все делители для числа общего количества

   v. Проверка на цикличность группы.

   - **Запомнить формулу для $P + P$**

     $$x' = (\frac{3x^2 + a}{2y})^2 - 2x$$

     $$y' = (\frac{3x^2 + a}{2y})(x - x') - y$$

   - **Запомнить формулу для $P + Q$**

     $$x' = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$$

     $$y' = (\frac{y_2 - y_1}{x_2 - x_1})(x - x') - y_1$$