Домашние задние от Иванова

Дано поле Голуа GF(7^4), для каждой группы свое (образованно при помощи разных полиномов). Поле GF(7^4) содержит $7^4=2401$ элемент. Заданное поле имеет подполе 7^2. «Учитывая свойства поля, считаем, что аддитивная группа подполя (всех элементы подполя относительно операции сложения) являются подгруппой аддитивной группы всего поля. Более того, аддитивная группа подполя является нормальным делителем в аддитивной группе поля. Основной задачей является нахождение смежных классов при разложении относительно операции сложения».

Теперь для тех, кто не понял. Поле GF(7^1) — поле натуральных чисел от 0 до 6, где определена операция сложения по модулю 7. Результатом такого сложения является остаток от деления на 7 обычного сложения. Например, $6+1=0$, $6+2=1$. Соответственно отрицательные числа определяются как $x+(-x)=0$, т.е. для 6 отрицательным числом является 1. В таком поле чисел не любой многочлен имеет корни, например x^2+5x+3 не имеет корней в поле GF(7^1). С помощью таких многочленов, можно расширить поле — получить новое поле, в котором многочлен будет иметь корни. Расширение поля с помощью указанного полинома было разобрано на первом семинаре. В случае домашнего задания за основу был взят многочлен 4-ой степени, поэтому поле расширили до 7^4.

И так нам дано поле GF(7^4) — две таблицы (ivanov_field_7-4.pdf) из 2400 элементом, в первой таблице элементы расположены по возрастанию степени полинома, во второй — по возрастанию коэффициентов полинома. Для получения поля необходимо еще учитывать нулевой элемент. Далее дано само задание (ivanov_task.pdf): на первой странице таблица с полиномами для 24 вариантов, на второй — то самое подполе 7^2 из 48 элементов плюс нулевой. Это подполе является *нормальным делителем* исходного поля. При помощи нормального делителя можно все поле разбить на непересекающиеся классы. В домашнем задании нужно найти 3 таких класса.

Для нахождения первого из них нужно все элементы подполя (49 многочленов) сложить с многочленом «элемент N 1» из таблицы в файле ivanov_task.pdf, в соответствии с номером варианта. При сложении многочленов следует помнить, что операции сложения проводятся по модулю 7, т.е. $4x+5x=2x$. Это очень просто — сначала складываем многочлены как обычно, приводим подобные слагаемы, а затем все числовые коэффициенты заменяем остатками от их деления на 7. Таким образом, находим первый *смежный класс*. Получив 49 многочленом нужно определить их номера в основном поле, использую вторую таблицу из файл а ivanov_field_7-4.pdf. Если к номеру многочлена прибавить 1 то получиться *модифицированный логарифм* этого элемента (многочлена). Теперь распечатываем карту поля (ivanov_map.pdf) и закрашиваем номера модифицированных логарифмов элементов полученного смежного класса. Другим цветом можно закрасить и элементы подполя, в задании (ivanov_task.pdf) указаны модифицированные логарифмы элементов (1 прибавлять не нужно). Аналогично находим и закрашиваем элементы второго смежного класса для «элемента N 2». Подполе и 2 смежных класса не должны пересекаться.

Для нахождения третьего смежного класса берем по одному любому элементу из первого и второго класса и складываем их — это «элемент N 3». Строим аналогично для него третий смежный класс. Подполе и все три класса должны не пересекаться. Что интересно третий класс не зависит от выбора элементов, это можно проверить, сложив еще 2 произвольных элемента из первого и второго классов — результат должен оказаться в третьем классе. В этом и есть суть нормального делителя, и вообще такое разбиение называется *правильным*.

Теперь надо найти *следы* нескольких произвольных элементов (2-3 из каждого класса). След элемента — это число (элемент поля GF(7^1)), и находится по формуле $T_{r^m/_q}(a) = a + a^q + a^{2q} + ... + a^{(m-1)q}$, где a — элемент поля. В нашем случае $q = 7$, а $m = 4$. След элемента для нашего поля находится как $T_r(a) = a + a^7 + a^{49} + a^{343}$.

Сахаров К.В. 30.10.2007, Версия 0.2