МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕШЕНИЕ ЗАДАЧИ КИРКМАНА О ШКОЛЬНИЦАХ С ПОМОЩЬЮ ЛОГАРИФМА ЗЕХА – ЯКОБИ

Е. Ю. Бегунков, Е. А. Малыгин
(Екатеринбург, УрГУПС)

Цель работы: найти способ составления перестановок для логарифма Зеха – Якоби с помощью решения задачи Киркмана о школьницах.

Логарифм Зеха – Якоби и его применение

Логарифм Зеха – Якоби является одним из видов перестановок, который используется для шифрования сообщений. Для кодирования сообщения используется свойство логарифма Зеха – Якоби, заключающееся в перестановке, которая при любом циклическом сдвиге имела только одну общую точку.

Формула логарифма Зеха – Якоби: $x^{L(m)} = 1 + x^m$.

Для того чтобы построить таблицу логарифма Зеха – Якоби, существует следующий алгоритм:

1. Выбрать примитивный многочлен, например, $x^4 + x + 1$ (порядок многочлена – 15).

2. Составить таблицу степеней многочлена:

n	x^{0*}	x^1	x^2	x^3
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	1	0	0
5	0	1	1	0
6	0	0	1	1
7	1	1	0	1
8	1	0	1	0
9	0	1	0	1
10	1	1	1	0
11	0	1	1	1
12	1	1	1	1
13	1	0	1	1
14	1	0	0	1
15	1	0	0	0

* x^{15} повторяется с x^0

3. Составить таблицу логарифма Зеха – Якоби, соответствующую этому примитивному многочлену:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(m)$	0	4	8	14	1	10	13	9	2	7	5	12	11	6	3

Задача Киркмана о школьницах

Построение таблицы логарифма Зеха – Якоби связано с задачей Киркмана о школьницах.

З а д а ч а. Школьницы должны были гулять ежедневно пятью группами по три в каждой группе. При этом необходимо было так составить расписание для их прогулок, чтобы каждая школьница в течение семи дней смогла точно один раз попасть в одну группу с каждой из остальных.

Для решения задачи берется один из примитивных многочленов с периодом 15.

Берем многочлен $x^4 + x + 1$.

Далее составляется таблица степеней многочлена.

Затем 2 степени многочлена, которые будут 2 из элементов тройки, складываются, а получившийся результат укажет на третий элемент тройки.

Также можно составить таблицу Кэли. На пересечении 2 элементов тройки находится недостающий элемент:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	4	8	14	1	10	13	9	2	7	5	12	11	6	3
1	4	1	5	9	0	2	11	14	10	3	8	6	13	12	7
2	8	5	2	6	10	1	3	12	0	11	4	9	7	14	13
3	14	9	6	3	7	11	2	4	13	1	12	5	10	8	0
4	1	0	10	7	4	8	12	3	5	14	2	13	6	11	9
5	10	2	1	11	8	5	9	13	4	6	0	3	14	7	12
6	13	11	3	2	12	9	6	10	14	5	7	1	4	0	8
7	9	14	12	4	3	13	10	7	11	0	6	8	2	5	1
8	2	10	0	13	5	4	14	11	8	12	1	7	9	3	6
9	7	3	11	1	14	6	5	0	12	9	13	2	8	10	4
10	5	8	4	12	2	0	7	6	1	13	10	14	3	9	11
11	12	6	9	5	13	3	1	8	7	2	14	11	0	4	10
12	11	13	7	10	6	14	4	2	9	8	3	0	12	1	5
13	6	12	14	8	11	7	0	5	3	10	9	4	1	13	2
14	3	7	13	0	9	12	8	1	6	4	11	10	5	2	14

По тройкам с элементом 0 (первая строка в таблице Кэли) можно составить таблицу перестановок логарифма Зеха – Якоби:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(m)$	0	4	8	14	1	10	13	9	2	7	5	12	11	6	3

Взяв другой простейший многочлен с порядком 15, например $x^4 + x^3 + 1$, можно решить задачу другим способом.

Таблица степеней многочлена и таблица Кэли:

n	x^0	x^1	x^2	x^3
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	0	1
5	1	1	0	1
6	1	1	1	1
7	1	1	1	0
8	0	1	1	1
9	1	0	1	0
10	0	1	0	1
11	1	0	1	1
12	1	1	0	0
13	0	1	1	0
14	0	0	1	1
15	1	0	0	0

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	12	9	11	12	10	8	13	6	2	5	14	1	7	11
1	12	1	13	10	12	13	11	9	14	7	3	6	0	2	8
2	9	13	2	14	11	13	14	12	10	0	8	4	7	1	3
3	11	10	14	3	0	12	14	0	13	11	1	9	5	8	2
4	12	12	11	0	4	1	13	0	1	14	12	2	10	6	9
5	10	13	13	12	1	5	2	14	1	2	0	13	3	11	7
6	8	11	14	14	13	2	6	3	0	2	3	1	14	4	12
7	13	9	12	0	0	14	3	7	4	1	3	4	2	0	5
8	6	14	10	13	1	1	0	4	8	5	2	4	5	3	1
9	2	7	0	11	14	2	2	1	5	9	6	3	5	6	4
10	5	3	8	1	12	0	3	3	2	6	10	7	4	6	7
11	14	6	4	9	2	13	1	4	4	3	7	11	8	5	7
12	1	0	7	5	10	3	14	2	5	5	4	8	12	9	6
13	7	2	1	8	6	11	4	0	3	6	6	5	9	13	10
14	11	8	3	2	9	7	12	5	1	4	7	7	6	10	14

Таблица перестановок логарифма Зеха – Якоби:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(m)$	0	12	9	11	12	10	8	13	6	2	5	14	1	7	11

Используя другой простейший многочлен той же степени, получаем другую таблицу перестановок логарифма Зеха – Якоби.

Найдя перестановки логарифма Зеха – Якоби для многочлена более высокой степени, можно решить задачу Киркмана для большего числа школьниц.

Например, составим таблицу перестановок логарифма Зеха – Якоби для многочлена $x^6 + x^5 + 1$, имеющего порядок 63:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$L(m)$	0	58	53	34	43	6	5	44	23	27	12	49	10	41	25	55

m	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$L(m)$	46	33	54	26	24	42	35	8	20	14	19	9	50	32	47	60

m	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$L(m)$	29	17	3	22	45	56	52	59	48	13	21	4	7	36	16	30

m	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
$L(m)$	40	11	28	61	38	2	18	15	37	62	1	39	31	51	57

При помощи этой таблицы можно решить задачу Киркмана для 63 школьниц, так как в таблице содержатся тройки с нулевым элементом, а добавляя 1, можно получить все тройки, которых будет $(63/3) \times ((63 - 1)/2) = 651$.

Вывод

Таким образом, можно сделать вывод, что удобно использовать логарифм Зеха – Якоби для нахождения троек Штейнера и последующего решения задачи Киркмана о школьницах. Сначала составляется таблица степеней простейшего многочлена, затем по этой таблице можно составить таблицу перестановок логарифма Зеха – Якоби, из нее получить тройки Штейнера и, соответственно, решение задачи Киркмана. Данный метод значительно упрощает нахождение троек Штейнера, которые используются в совершенных шифрах.

АВТОМАТИЗАЦИЯ МАТЕМАТИЧЕСКОГО АЛГОРИТМА РАСШИРЕНИЯ БИНАРНЫХ ПОЛЕЙ

Е. А. Букина, О. О. Ванцева, М. Ю. Филиппов, Кр. Л. Геут
(Екатеринбург, УрГУПС, prosto-bukina@mail.ru)

Научно-исследовательский проект посвящен автоматизации математического алгоритма расширения бинарных полей и построения неприводимых многочленов больших степеней вида 2^n, используемых для работы регистров сдвига, реализации криптографических алгоритмов и решения других задач кодирования и защиты информации.

В последние годы повсеместно и с большой интенсивностью ведутся работы по созданию и применению различных автоматичес-