Построить расширенное поле Галуа из p^m *элементов* $GF(p^m)$ по модулю неприводимого многочлена, указанного в таблице:

N задачи	Порядок поля *p*	Длина последовательности *m*	*Неприводимый многочлен p(x)*
1	**2**	**2**	$x^2 + x + 1$
2	**2**	**3**	$x^3 + x + 1$
3	**2**	**3**	$x^3 + x^2 + 1$
4	**2**	**4**	$x^4 + x + 1$
5	**2**	**4**	$x^4 + x^3 + 1$

Задача 1 (*Пример решения*):

Последовательность длины 2	Многочлен	Степень	Логарифм
00	0	0	$-\infty$
10	1	1	0
01	α	α	1
11	$1+\alpha$	α^2	2

Правила сложения и умножения в этом поле приведены на рис. П.1.5.

а)

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

б)

·	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Рис. П.1.5

Формирование первой строки, первого столбца и диагональных элементов таблицы сложени двух первых строк и двух первых столбцов таблицы умножения не вызывает затруднения формирование других элементов:

$$1+\alpha = \alpha^2,\ 1+\alpha^2 = \alpha,\ \alpha+\alpha^2 = 1;$$

$$\alpha \cdot \alpha^2 = \alpha^3 = \alpha \cdot (1+\alpha) = \alpha+\alpha^2 = 1$$

на основе соотношения для примитивного элемента $\alpha^2+\alpha+1 = 0$.