Кодирование с помощью порождающего полинома

- Разрешенное кодовое слово:

$$W(x) = V(x)\, g(x) = (x^3 + x^2 + x + 1)(x^3 + x + 1) =$$
$$= x^6 + x^5 + x^4 + x^3 + x^2 + x + x^3 + x^2 + x + 1 =$$
$$= x^6 + x^5 + x^4 + 1$$

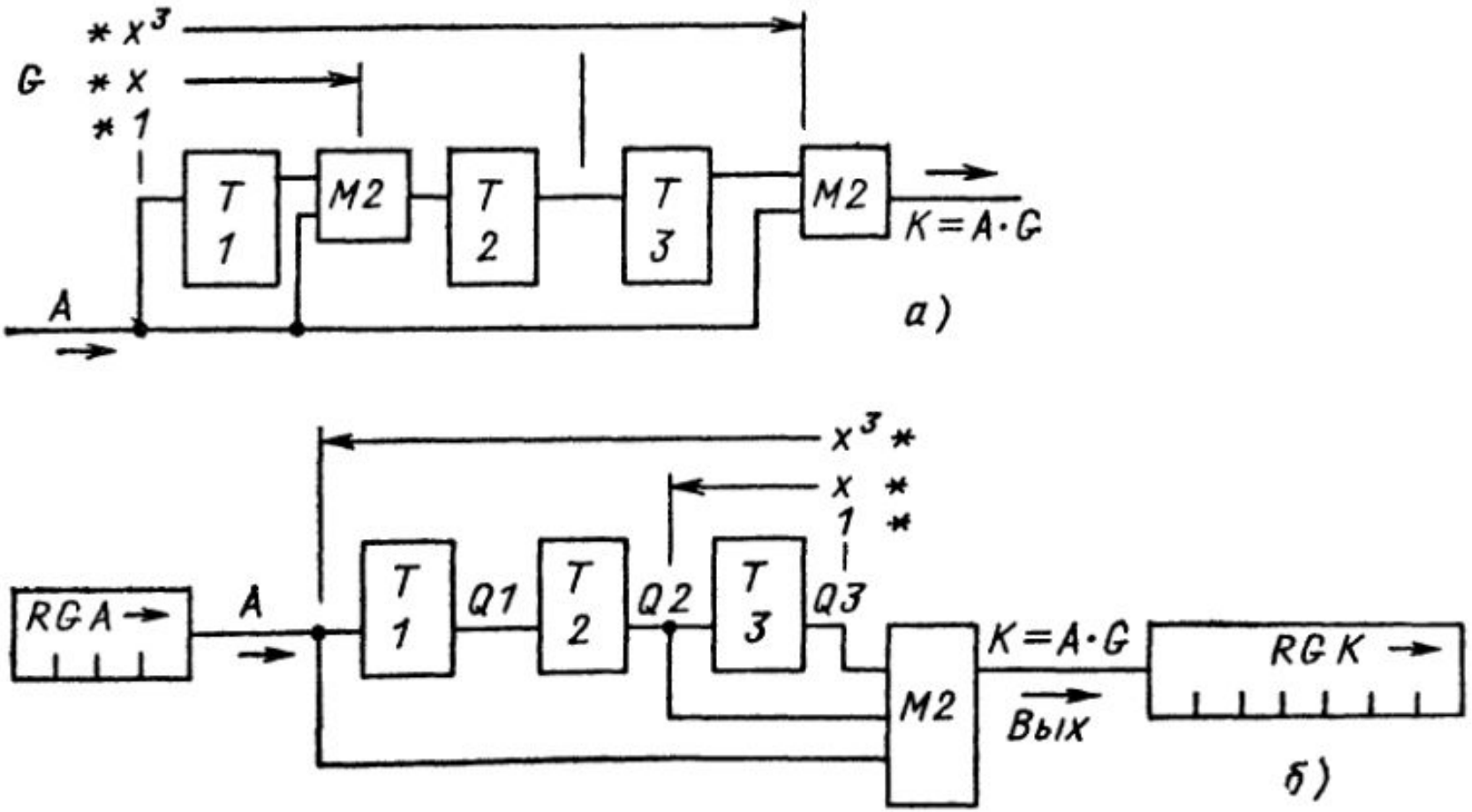
Пример умножения полиномов

- Пример. Перемножить два полинома A и G.
  - $K = A \cdot G = (1 + x^3)(1 + x + x^3)$.

```
A     1 0 0 1
    x
G     1 1 0 1
  ---------------
      1 0 0 1
        1 0 0 1
  ⊕     0 0 0 0
            1 0 0 1
  ---------------
      1 1 0 0 1 0 1
```

Ответ: $A \cdot G = 1 + x + x^4 + x^6$.

Узел умножения полиномов



- $K = A \cdot G = (1 + x^3)(1 + x + x^3)$.

Пример деления полиномов

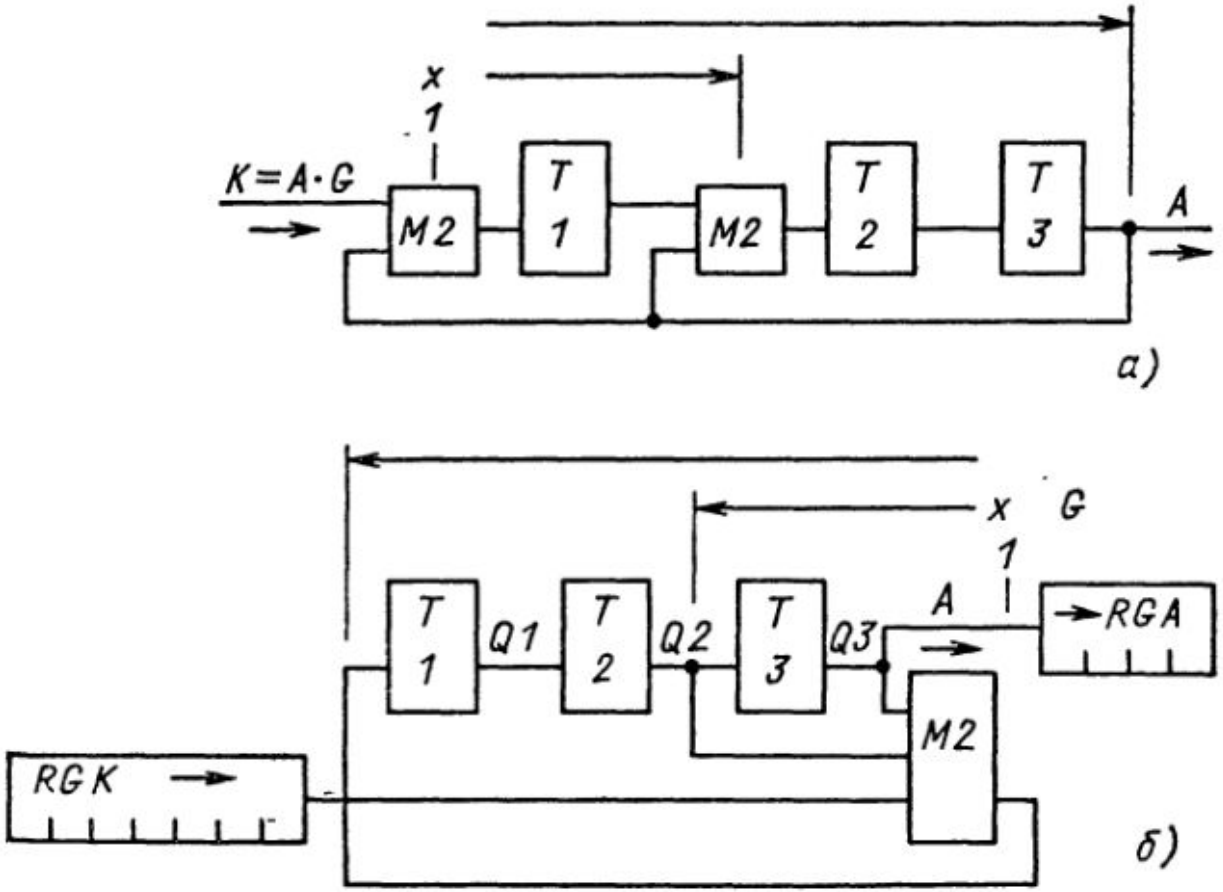
- В результате получен код полинома К = 1101 и нулевой остаток.

```
1 1 0 0 1 0 1 | 1 0 0 1
      1 0 0 1 | 1 1 0 1
    0 1 1 0 0 |
⊕     0 0 0 0
    1 0 1 1
    1 0 0 1
  -------------
  1 0 0 1
  1 0 0 1
  -------
  0 0 0 0  – остаток.
```

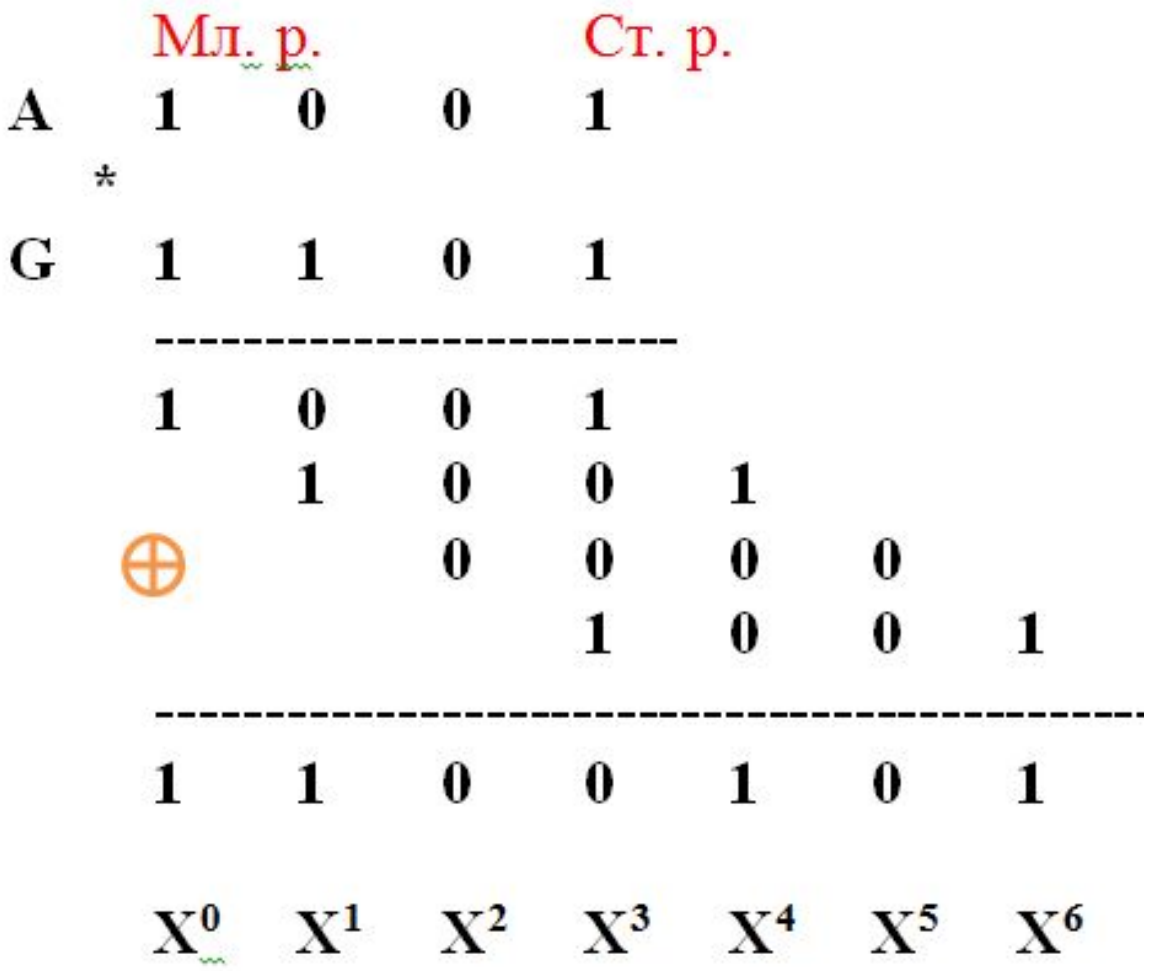
Ответ: К = 1101.

Узел деления полиномов

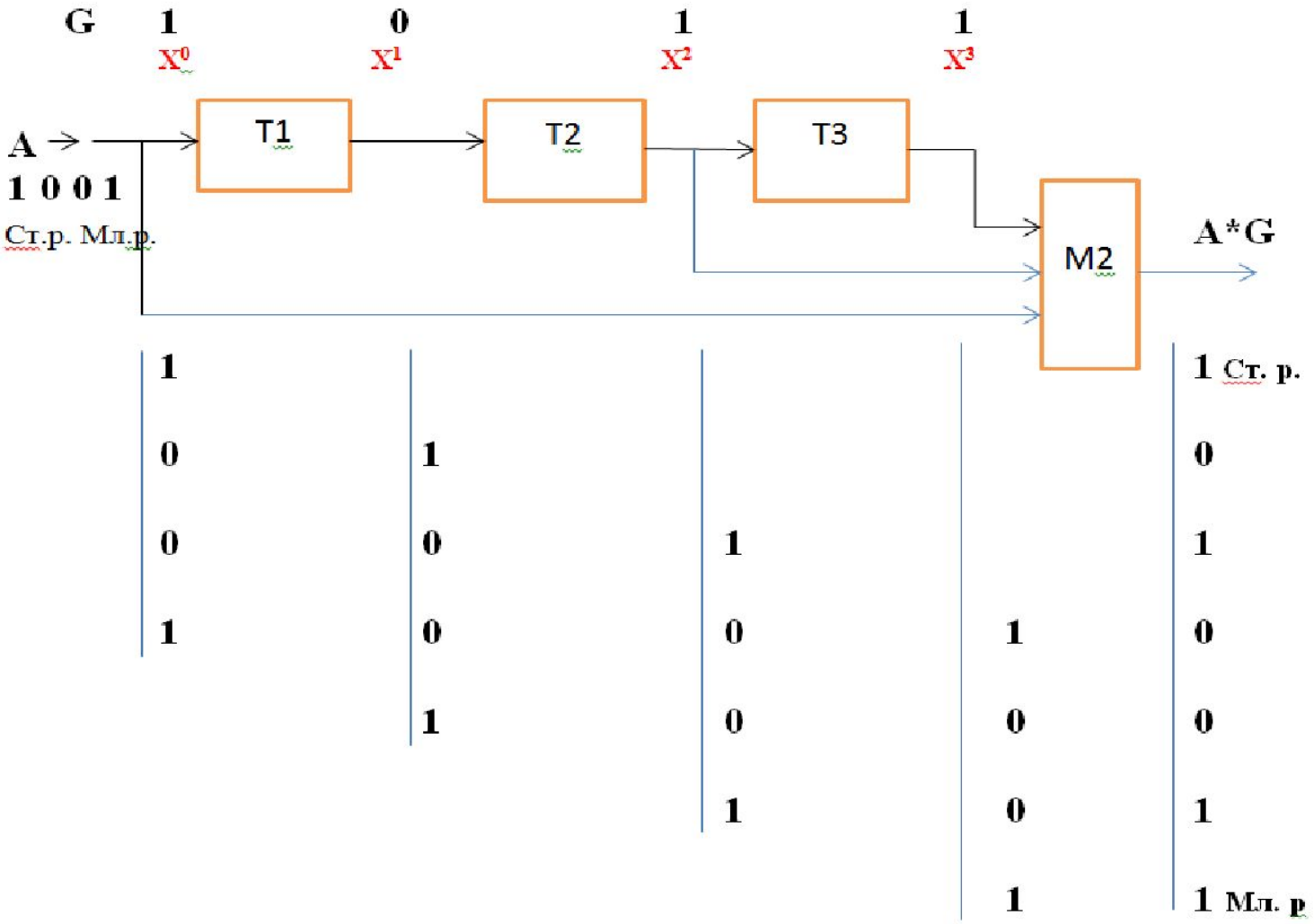
- Узел деления полиномов K = AG. A = K/G



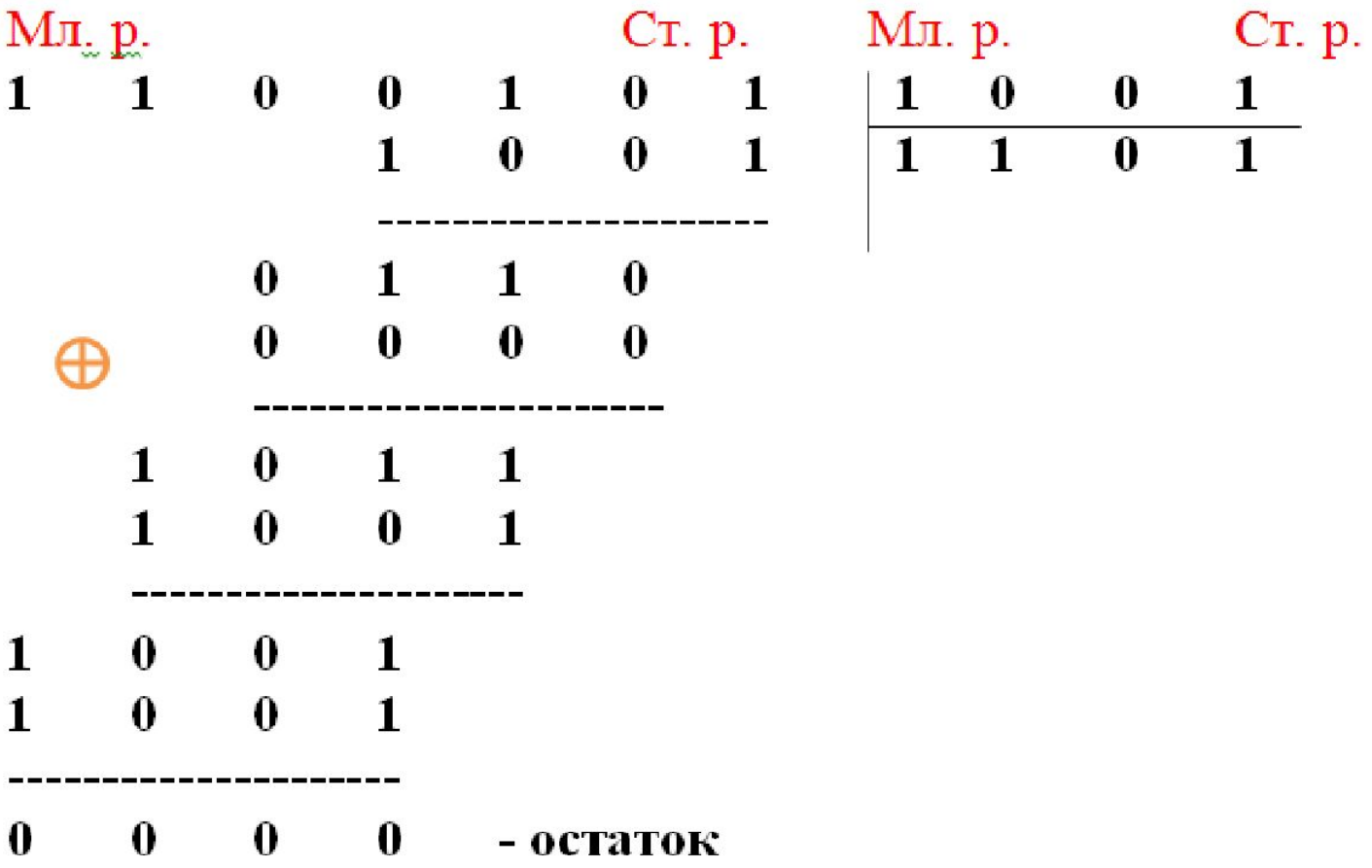
Пример умножения полиномов



Пример умножения полиномов



Пример деления полиномов



Поля Галуа.
Выполнение арифметических операций

- б) перемножим полиномы:

$$5 \cdot 7 = (x^2 + 1)(x^2 + x + 1) =$$

$$= x^4 + x^3 + x^2 + x^2 + x + 1 =$$

$$= x^4 + x^3 + x + 1 =$$

$$= 11011_2 = 27_{10}.$$

Поля Галуа. Порождающий полином

- Продолжим вычисление произведения 5 и 7, добавив слагаемые $x^2 + x + x^2 + x$, не меняющее уравнение:

$$5 \cdot 7 =$$

$$= x^4 + x^3 + x + 1 =$$

$$= (x^4 + x^2 + x) + (x^3 + x + 1) + x^2 + x =$$

$$= x(x^3 + x + 1) + (x^3 + x + 1) + x^2 + x =$$

$$= x^2 + x = 110_2 = 6_{10}.$$

- Таким образом, результат умножения 5 · 7 = 6 принадлежит полю $GF(2^3)$.

Поля Галуа. Порождающий полином

- Такой же результат можно получить, вычислив остаток от деления полинома, полученного при умножении, на порождающий полином
- $(x^3 + x + 1)$:

$$
\begin{array}{l|l}
x^4 + x^3 + \quad + x + 1 & x^3 + x + 1 \\
\oplus & \\
\cline{1-1}
x^4 + \quad x^2 + x & x + 1 \\
\cline{1-1}
\quad x^3 + x^2 \quad + 1 & \\
\oplus & \\
\cline{1-1}
\quad x^3 \quad + x + 1 & \\
\cline{1-1}
\quad x^2 + x = 110_2 = 6_{10}. &
\end{array}
$$

Вывод: полученное значение произведения двух чисел 5 и 7 также принадлежит полю $GF(2^3)$.

Поля Галуа. Таблица умножения

- Таблица умножения чисел от 1 до 7 (табл. 1).

Полиномиальное представление		1	2	3	4	5	6	7
1	1	1	2	3	4	5	6	7
x	2	2	4	6	3	1	7	5
x + 1	3	3	6	5	7	4	1	2
x^2	4	4	3	7	6	2	5	1
$x^2+ 1$	5	5	1	4	2	7	3	6
$x^2+ x$	6	6	7	1	5	3	2	4
$x^2+ x+ 1$	7	7	5	2	1	6	4	3

Поля Галуа. Таблица степеней

- Таблица степеней обладает цикличностью, т.е. «7» степень соответствует «0», «8» – «1» и т.д. (табл. 2).

Полиномиальное представление		Степени							
		0	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1	1	1
x	2	1	2	4	3	6	7	5	1
x + 1	3	1	3	5	4	7	2	6	1
x^2	4	1	4	6	5	2	3	7	1
$x^2+ 1$	5	1	5	7	6	3	4	2	1
$x^2+ x$	6	1	6	2	7	4	5	3	1
$x^2+ x+ 1$	7	1	7	3	2	5	6	4	1

Поля Галуа.

- Пример 2. Вычислить значение 5^2 в полиноминальной форме.
-

$$5^2 = (x^2 + 1)^2 = x^4 + x^2 + x^2 + 1 = x^4 + x^2 + x + x^2 + x + 1 =$$

- $= x(x^3 + x + 1) + x^2 + x + 1 = x^2 + x + 1 = 111_2 = 7_{10}$.
-
- При вычислении были добавлены значения **x+x**, а согласно определению $x^3 + x + 1 = 0$.

Поля Галуа

- Любой элемент поля можно выразить через степень примитивного полинома, например: **$5 = 2^6$, $7 = 2^5$.** Рассмотрим примеры выполнения арифметических операций по таблице степеней.

- Пример 3. Вычислить значение произведения двух чисел.

- **$5 \cdot 7 = 2^6 \cdot 2^5 = 2^{(6+5)} = 2^{11} = 2^{(11 \bmod 7)} = 2^4 = 6.$**

Поля Галуа

- Пример 4. Выполнение операции деления чисел.
- $\frac{6}{5} = 2^4 / 2^6 = 2^{(4-6)} = 2^{-2} = 2^{((-2) \bmod 7)} = 2^5 = 7.$
- Пример 5. Вычислить значение 5^2.
- $5^2 = (2^6)^2 = 2^{6 \cdot 2} = 2^{12} = 2^{(12 \bmod 7)} = 2^5 = 7.$

Поля Галуа $GF(2^8)$

- Согласно теории, i-й элемент поля Галуа – это результат возведения в i-ю степень некоторого примитивного элемента, в качестве которого обычно берется простое число 2, где $i = 0 \ldots 2^8 - 1$.

- Начиная $i = 8$, мы получим результат ,который уже выходит за пределы $[0, 2^8 - 1]$ и здесь используется особый подход.

Поля Галуа. $GF(2^8)$

- Правило первоначальной генерации поля:

$$\begin{cases} GF[0]=1, GF[1]=2, GF[255]=0, \\ i=2...254 \\ GF[i]=\begin{cases} (GF[i-1]<<1), GF[i-1]<128 \\ (GF[i-1])<<1)\oplus 285, GF[i-1]\geq 128 \end{cases} \end{cases}$$

Поля Галуа. GF(2^8)

- Правило построения поля:
- 0-й элемент поля это 1,
- 1-й элемент – 2,
- а, начиная со 2-го элемента по 254-й элемент, элемент вычисляется как удвоенное значение предыдущего элемента, и если удвоение привело к числу, вышедшему границы 8-разрядов, то на него делается XOR с числом **285_{10}** (11D16), наконец, последний 255-й элемент поля – 0.
- Число 285 – это десятичное представление (11D в
- 16 – ричном представлении) так называемого неприводимого полинома $x^8+x^4+x^3+x^2+1$, с помощью которого и порождается первоначальное поле.

Поля Галуа. $GF(2^8)$

- Символом обозначается операция XOR – побитовое сложение по модулю 2, а символом << обозначается логический сдвиг влево двоичного представления числа на указанное количество разрядов.

- При этом биты, «вылезшие слева» из 8-разрядного байта, пропадают, а разряды, «освобождающиеся справа», заполняются нулями.

- Сдвиг числа в двоичном представлении на один разряд влево– это эквивалентно удвоению числа.

Поля Галуа. $GF(2^8)$

- Сгенерированное поле $GF(2^8)$, содержит результаты возведения примитивного элемента «2» во все степени, начиная с 0, заканчивая 255.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	4	8	16	32	64	128	29	58	116	232	205	135	19	38
16	76	152	45	90	180	117	234	201	143	3	6	12	24	48	96	192
32	157	39	78	156	37	74	148	53	106	212	181	119	238	193	159	35
48	70	140	5	10	20	40	80	160	93	186	105	210	185	111	222	161
64	95	190	97	194	153	47	94	188	101	202	137	15	30	60	120	240
80	253	231	211	187	107	214	177	127	254	225	223	163	91	182	113	226
96	217	175	67	134	17	34	68	136	13	26	52	104	208	189	103	206
112	129	31	62	124	248	237	199	147	59	118	236	197	151	51	102	204
128	133	23	46	92	184	109	218	169	79	158	33	66	132	21	42	84
144	168	77	154	41	82	164	85	170	73	146	57	114	228	213	183	115
160	230	209	191	99	198	145	63	126	252	229	215	179	123	246	241	255
176	227	219	171	75	150	49	98	196	149	55	110	220	165	87	174	65
192	130	25	50	100	200	141	7	14	28	56	112	224	221	167	83	166
208	81	162	89	178	121	242	249	239	195	155	43	86	172	69	138	9
224	18	36	72	144	61	122	244	245	247	243	251	235	203	139	11	22
240	44	88	176	125	250	233	207	131	27	54	108	216	173	71	142	0

Поля Галуа. GF(2^8)

- Вычисление значения 29
- 1 2 4 6 16 32 64 128 29 58…
- ----------
- 128 64 32 16 8 4 2 1
- 1 0 0 0 0 0 0 0 = 128
- 1 0 0 0 0 0 0 0 0 - сдвиг
- 1 0 0 0 1 1 1 0 1 = 285
- ----------
- 1 1 1 0 1 = 29

Поля Галуа. $GF(2^8)$

- Помимо основного поля в технологии кодирования важно также иметь и так называемое обратное поле, позволяющее по заданному значению 2^k выяснить степень k, в которое был возведен примитивный элемент 2, иными словами иметь таблицу логарифмов пооснованию2.
- Обратное поле вычисляется следующим образом:

$$\begin{cases} i = 0...255 \\ GF^{-1}[GF[i]] = i \end{cases}$$

Поля Галуа $GF(2^8)$

- Сгенерированное обратное поле $GF^{-1}(2^8)$, содержит логарифмы всех элементов, начиная с 0, заканчивая 255, по основанию примитивного элемента 2.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	255	0	1	25	2	50	26	198	3	223	51	238	27	104	199	75
16	4	100	224	14	52	141	239	129	28	193	105	248	200	8	76	113
32	5	138	101	47	225	36	15	33	53	147	142	218	240	18	130	69
48	29	181	194	125	106	39	249	185	201	154	9	120	77	228	114	166
64	6	191	139	98	102	221	48	253	226	152	37	179	16	145	34	136
80	54	208	148	206	143	150	219	189	241	210	19	92	131	56	70	64
96	30	66	182	163	195	72	126	110	107	58	40	84	250	133	186	61
112	202	94	155	159	10	21	121	43	78	212	229	172	115	243	167	87
128	7	112	192	247	140	128	99	13	103	74	222	237	49	197	254	24
144	227	165	153	119	38	184	180	124	17	68	146	217	35	32	137	46
160	55	63	209	91	149	188	207	205	144	135	151	178	220	252	190	97
176	242	86	211	171	20	42	93	158	132	60	57	83	71	109	65	162
192	31	45	67	216	183	123	164	118	196	23	73	236	127	12	111	246
208	108	161	59	82	41	157	85	170	251	96	134	177	187	204	62	90
224	203	89	95	176	156	169	160	81	11	245	22	235	122	117	44	215
240	79	174	213	233	230	231	173	232	116	214	244	234	168	80	88	175

Поля Галуа. Выполнение арифметических операций

- Определим четыре арифметические операции:

$$a + b = a \oplus b$$

$$a - b = a \oplus b$$

$$a \cdot b = \begin{cases} a = 0 \,|\, b = 0 \Rightarrow 0 \\ a \neq 0 \,\&\, b \neq 0 \Rightarrow \begin{cases} \log_2 a + \log_2 b < 255 \Rightarrow 2^{\left(\log_2 a + \log_2 b\right)} \\ \log_2 a + \log_2 b \geq 255 \Rightarrow 2^{\left(\log_2 a + \log_2 b - 255\right)} \end{cases} \end{cases}$$

Поля Галуа.
Выполнение арифметических операций

- Операция деления:

$$a/b=\begin{cases} a=0\ \&\ b\neq 0\Rightarrow 0 \\ a\neq 0\ \&\ b\neq 0\Rightarrow \begin{cases} \log_2 a-\log_2 b\geq 0\Rightarrow 2^{\left(\log_2 a-\log_2 b\right)} \\ \log_2 a-\log_2 b<0\Rightarrow 2^{\left(\log_2 a-\log_2 b+255\right)} \end{cases} \\ b=0\Rightarrow \textit{Ошибка} \end{cases}$$

Поля Галуа. Выполнение арифметических операций

- Возведение в степень:

$$2^x = GF[x]$$

$$\log_2 x = GF^{-1}[x]$$

$$a, b, x \in GF(2^8)$$

- Особенности выполнения арифметических операций.
- Сложение и вычитание для поля $GF(2^8)$ заменяется побитовым сложением по mod2.

Так как $\log(a \cdot b) = \log a + \log b$ и $\log (a/b) = \log a - \log b$, то умножение (деление) сводится к вычислению $\log_2$ от операндов (по обратному полю Галуа), сложению (вычитанию) значений логарифмов и возведению в степень числа 2 суммы (разности) (по основному полю Галуа).

Поля Галуа.
Выполнение арифметических операций

- Примечания:
- Если сумма степеней больше или равна 255, то из нее вычитается 255.
- Если сумма степеней меньше 0, к ней прибавляется 255.
- При вычислении произведения степеней за результат берется остаток произведения по mod2.

Поля Галуа.
Выполнение арифметических операций

- Пример 2. Выполнение условия a = (a/в) · в,
- например при a = 7 и в = 3.
-
- **$7 \cdot 3 = 2^{(\log_2 7 + \log_2 3)} = 2^{(198 + 25)} = 2^{(223)} = 9.$**
-
- **$9/3 = 2^{(\log_2 9 - \log_2 3)} = 2^{(223 - 25)} - 2^{(198)} = 7.$**

- Используем GF^{-1}.
-

Поля Галуа.
Пример деления полиномов

- **Пример 2.** Разделить полином A(x) на полином g(x).
- **Делимое** $A(x) = 4x^4 \oplus 2\,x^3 \oplus x^2$
- **Делитель** $g(x) = x^2 \oplus 2\,x \oplus 2$
- **Результат** $Q(x)$
- **Остаток от деления** $R(x)$

Поля Галуа.
Пример деления полиномов

- Первый шаг

$$\begin{array}{l} 4x^4 \oplus 2x^3 \oplus x^2 \\ \oplus \\ 4x^4 \oplus 8x^3 \oplus 8x^2 \\ \hline 10x^3 \oplus 9x^2 \end{array} \qquad \begin{array}{|l} g(x) = x^2 \oplus 2x \oplus 2 \\ \hline Q(x) = 4x^2 \end{array}$$

$$\begin{array}{l} 2 \rightarrow 0010 \\ \oplus \\ 8 \rightarrow 1000 \\ \hline 10 \rightarrow 1010 \end{array}$$

Поля Галуа.
Пример деления полиномов

- Второй шаг

$$10x^3 \oplus 9x^2 \qquad \big| \quad g(x) = x^2 \oplus 2x \oplus 2$$

$$\oplus$$

$$10x^3 \oplus 20x^2 \oplus 20x \qquad \big| \quad Q(x) = 4x^2 \oplus 10x$$

$$29x^2 \oplus 20x$$

Поля Галуа.
Пример деления полиномов

- Третий шаг

$$
\begin{array}{l|l}
29x^2 \oplus 20x & g(x) = x^2 \oplus 2x \oplus 2 \\
\oplus & \\
\underline{29x^2 \oplus 58x \oplus 58} & \\
46x \oplus 58 = R(x) & Q(x) = 4x^2 \oplus 10x \oplus 29
\end{array}
$$

Поля Галуа.
Пример деления полиномов

- Проверка:

$$A(x) = g(x) \cdot Q(x) \oplus R(x) = (x^2 \oplus 2x \oplus 2) \cdot (4x^2 \oplus 10x \oplus 29) \oplus (46x \oplus 58) =$$

$$= (4x^4 \oplus (10 \oplus 8)x^3 \oplus (29 \oplus 20 \oplus 8)x^2 \oplus (2 \cdot 29 \oplus 2 \cdot 10)x \oplus 58) \oplus (46x \oplus 58).$$

$$\begin{array}{r} 4x^4 \oplus 2x^3 \oplus x^2 \oplus 46x \oplus 58 \\ \oplus \\ 46x \oplus 58 \\ \hline \end{array}$$

$$A(x) = 4x^4 \oplus 2x^3 \oplus x^2$$

Контрольные вопросы

Номер варианта	Степень делимого	Коэффициенты делимого	Степень делителя	Коэффициенты делителя
1	4	4; 3; 2; 1; 1	3	1; 3; 4; 2
2	4	5; 2; 6; 4; 2	3	1; 2; 3; 1
3	3	3; 2; 1; 3	2	1; 4; 2
4	3	6; 2; 4; 4	2	1; 2; 1
5	4	4; 2; 3; 2; 5	3	1; 5; 3; 7
6	4	6; 5; 6; 8; 6	3	1; 2; 9; 4
7	4	5; 4; 3; 2; 7	3	1; 4; 3; 1
8	5	5; 2; 6; 1;2; 8	3	1; 2; 8; 2
9	5	3; 7; 8; 1; 4; 3	4	1; 2; 5; 7; 3
10	6	3; 2; 1; 4; 2; 1; 2	5	1; 5; 6; 4; 9; 4
11	6	1; 2; 3; 4; 3; 2; 1	4	1; 2; 8; 5; 5
12	4	5; 4; 3; 4; 5	3	1; 8; 6; 6
13	4	4; 7; 9; 6	3	1; 6; 5; 7
14	4	8; 5; 4; 6	3	1; 4; 3; 8
15	4	5; 2; 1; 3	3	1; 2;2; 6
16	4	2; 6; 8; 7	4	1; 1; 2; 6; 5
17	3	4; 5; 6; 2	2	1; 9; 4
18	5	3; 4; 6; 1	4	1; 2; 2; 1; 3
19	6	1; 6; 4; 7; 9; 8;4	4	1; 5; 1; 6; 2
20	4	4; 8; 7; 6; 2	2	1; 7; 1

Список использованных источников и литературы

1. Рахман П.А. Основы защиты данных от разрушения. Коды Рида-Соломона.- М.:МЭИ, 2007.
2. Потемкин И.С Функциональные узлы цифровой автоматики. – М.: Энергоатомиздат, 1988. – 320 с.
3. Открытые источники Internet.