Алгебраические основы криптографии в задачах и упражнениях.

22 марта 2019 г.

Оглавление

Введение

Учебное пособие является практическим введением в математические методы криптологии. Сборник задач и упражнений предназначен для бакалавров и магистров, обучающихся по направлению, связанному с информационной безопасностью компьютерных систем. В основе пособия положен опыт проведения авторами практических занятий по курсам математические основы криптологии и криптографические протоколы, читаемых авторами на факультете ВМК МГУ имени М.В.Ломоносова и Московском Авиационном Институте. Первый цикл задач и упражнений относится к теоретико-числовым моделям криптографии. В качестве приложений предлагается задачи и упражнения, связанные с построением криптографических протоколов, в частности схем ЭЦП на основе модульной арифметики. В разделе конечные поля особое внимание уделяется задачам построения линейных реккурентных последовательностей и применения их к шифрам гаммирования. В разделе теория групп содержатся задачи и упражнения, связанные со строением конечных групп подстановок. Последний раздел задач связан с современными криптографическими алгоритмами, построенными на основе эллиптических кривых над конечными полями. Даются задачи и упражнения построения моделей современных схем ЭЦП на основе группы точек эллиптических кривых.

Список обозначений

$\mathbb{N}$ — множество натуральных чисел;
$\mathbb{Z}$ — множество целых чисел;
$\mathbb{Z}_n$ — кольцо вычетов по модулю n;
$\mathbb{Z}_n^*$ — мультипликативная группа обратимых по умножению элементов кольца $\mathbb{Z}_n$;
$\varphi(n) = |\mathbb{Z}_n^*| = |\{x \in \mathbb{Z}_n : \text{НОД}(x, n) = 1\}|$ — функция Эйлера;
$|G|$ — мощность множества G (порядок группы G);
$A \simeq B$ — структура A изоморфна структуре B;
$H < G$ — H является подгрупой группы G;

$H \lhd G$ — H является нормальной подгруппой группы G ($ghg^{-1} \in H$ для всех $g \in G$ и $h \in H$);

$\mathrm{ord}(a)$ — порядок элемента a (в какой-либо группе);

G/H — фактор группа группы G по подгруппе H;

$[G : H]$ — индекс группы G по подгруппе H;

$\langle a \rangle$ — группа, порождённая элементом a;

S^{Ω} — группа перестановок (подстановок) на множестве Ω (симметрическая группа);

S_n — группа перестановок на множестве $\{1, \ldots, n\}$;

A_n — знакопеременная подгруппа группы S_n (группа чётных подстановок);

$N_G(S)$ — нормализатор группы G по множеству $S \subset G$:

$$N_G(S) = \{x \in G : x^{-1}Sx = S\};$$

$Z_G(S)$ — централизатор группы G по множеству $S \subset G$:

$$Z_G(S) = \{x \in G : sx = xs,\ \forall s \in S\};$$

$Z(G) = \{x \in G | xg = gx, \forall g \in G\}$ — центр группы;

$\mathbb{K}[x]$ — кольцо многочленов от одной переменной над кольцом $\mathbb{K}$;

$GF(q), F_q$ — поле Галуа с q элементами;

$\mathbb{F}_q^*$ — группа обратимых элементов поля F_q;

$\mathbb{P}$ — множество всех простых чисел;

$a|b$ — a является делителем b;

$gcd(a, b)$, НОД(a, b) — наибольший общий делитель чисел a и b;

$SIG(x)$ — подпись сообщения x.

1. Теоретико-числовые методы и алгоритмы

Теорема 1 (Эйлера). *Для любого a такого, что НОД$(a, n) = 1$*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Теорема 2 (Ферма). *Для любого простого p и любого $a \in \mathbb{Z}$*

$$a^p \equiv a \pmod{n}$$

Определение 1. *Число $a \in \mathbb{Z}$ обратимо по модулю n, если существует $b \in \mathbb{Z}$ такое, что $a \cdot b \equiv 1 \pmod{n}$*

Теорема 3. *Число $a \in \mathbb{Z}$ обратимо по модулю n тогда и только тогда, когда НОД$(a, n) = 1$.*

Алгоритм вычисления обратного элемента в $\mathbb{Z}_n$

Вычислим обратный элемент к $\boldsymbol{a}$ по модулю $\boldsymbol{n}$.

Полагаем $r_0 = n,\ r_1 = a$ и применяем алгоритм Евклида вычисления НОД(r_0, r_1) :

$$\begin{array}{ll} r_0 = r_1 q_1 + r_2, & r_2 < r_1 \\ r_1 = r_2 q_2 + r_3, & r_3 < r_2 \\ \quad \vdots & \quad \vdots \\ r_{k-2} = r_{k-1} q_{k-1} + r_k, & 1 \leqslant r_k < r_{k-1} \\ r_{k-1} = r_k q_k, & \textbf{НОД} = (\mathbf{r_0 = n},\ \mathbf{r_1 = a}) = \mathbf{r_k} \end{array}$$

Если $r_k \neq 1$, то $a^{-1} \pmod{n}$ — не существует. Если $r_k = 1$, то полагаем $P_0 = 1,\ P_1 = q_1$ и вычисляем $P_i,\ i = \overline{2, k}$ по рекуррентной формуле:

$$P_i = q_i P_{i-1} + P_{i-2}, \quad P_k = r_0 = n. \tag{1}$$

Обратный к a элемент $a^{-1} = (-1)^{k+1} P_{k-1}$. При этом $P_k = n$. При вычислениях удобно использовать таблицу из $k+1$ клеток, клетки которой последовательно заполняем, используя формулу (1).

Пример. Вычислить НОД для $n = 181,\ a = 27$.

Решение. Вычисляем НОД$(181, 27)$ по алгоритму Евклида:

$$181 = 27 \cdot 6 + 19$$
$$27 = 19 \cdot 1 + 8$$
$$19 = 8 \cdot 2 + 3$$
$$8 = 3 \cdot 2 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2$$

Составляем таблицу и заполняем её по формуле (1):

	q_1	q_2	q_3	q_4	q_5	q_6
	6	1	2	2	1	2
1	6	7	20	47	67	181

Так как $k = 6$, то $27^{-1} = (-1)^7 \cdot 67 = -67 = 181 - 67 = 114 \pmod{181}$

Определение 2. *Порядок элемента a группы G это минимальное натуральное число n такое, что $a^n = e$, (e — единица группы G).*

Теорема 4. *Порядок элемента $a \in G$ равен n тогда и только тогда, когда $a^n = e$ и для любого простого $q \mid n$ выполняется условие*

$$a^{\frac{n}{q}} \neq e. \tag{2}$$

Пример. Проверить, что порядок элемента $a = 7$ по модулю $p = 71$ равен 70.

Решение. Так как порядок мультипликативной группы $\mathbb{Z}_{71}^*$ равен $70 = 2 \cdot 5 \cdot 7$, то нужно убедиться, что

$$7^{\frac{70}{7}} = 7^{10} \not\equiv 1 \pmod{71};$$
$$7^{\frac{70}{5}} = 7^{14} \not\equiv 1 \pmod{71};$$
$$7^{\frac{70}{2}} = 7^{35} \not\equiv 1 \pmod{71}.$$

Предварительно вычисляем

$$7^2 = 49, \qquad 7^4 \equiv 58 \pmod{71}, \qquad 7^8 \equiv 27 \pmod{71},$$
$$7^{16} \equiv 19 \pmod{71}, \qquad 7^{32} \equiv 6 \pmod{71}.$$

Следовательно,

$7^{10} = 7^8 \cdot 7^2 \equiv 49 \cdot 27 \equiv 45 \pmod{71} \not\equiv 1 \pmod{71}$,
$7^{14} = 7^{10} \cdot 7^4 \equiv 45 \cdot 58 \equiv 54 \pmod{71} \not\equiv 1 \pmod{71}$,
$7^{35} = 7^{32} \cdot 7^2 \cdot 7 = 42 \cdot 49 \cdot 7 \equiv 70 \equiv -1 \pmod{71} \not\equiv 1 \pmod{71}$.

Таким образом, $\mathrm{ord}(7) = 70$.

Теорема 5 (Китайская теорема об остатках). *Система сравнений*

$$\{x = a_i \pmod{n_i},\ i = \overline{1,k},$$

где НОД$(n_i, n_j) = 1$ *при* $i \neq j$ *имеет единственное решение по модулю* $N = n_1 \cdot \ldots n_k$*, и это решение имеет вид:*

$$X = \sum_{i=1}^{k} a_i N_i M_i \pmod{N}, \tag{3}$$

где $N_i = \dfrac{N}{n_i},\ M_i = N_i^{-1} \pmod{n_i},\ i = \overline{1,k}$

Следствие. *Сравнение*

$$\{f(x) \equiv 0 \pmod{N = \prod_{i=1}^{k} n_i}, \qquad \text{НОД}(n_i, n_j) = 1 \text{ при } i \neq j \tag{4}$$

равносильно системе

$$\{f(x) \equiv 0 \pmod{n_i},\ i = \overline{1,k}. \tag{5}$$

Если T_i *— число решений* i*-ого сравнения системы (5), то число решений сравнения (4) равно* $T = \prod_{i=1}^{k} T_i$*.*
Общее решение сравнения (4) вычисляется по формуле (3):

$$X = \sum_{i=1}^{k} x_i N_i M_i \pmod{N}, \tag{6}$$

где x_i *— решение* i*-ого сравнения системы (5),* $N_i = \dfrac{N}{n_i},\ M_i = N_i^{-1} \pmod{n_i}, i = \overline{1,k}$*.*

Пример. Решить сравнение

$$x^3 \equiv 1 \pmod{504} \tag{7}$$

Решение. Так как $504 = 7 \cdot 9 \cdot 8$, то сравнение (7) равносильно системе

$$\begin{cases} x^3 \equiv 1 \pmod{7} \\ x^3 \equiv 1 \pmod{8} \\ x^3 \equiv 1 \pmod{9} \end{cases}$$

Первое сравнение имеет три решения: $x_1 = 1, 2, 4$. Второе сравнение имеет одно решение: $x_2 = 1$. Третье — три решения: $x_3 = 1, 4, 7$.

Общее решение сравнения (7), согласно (6) имеет вид:

$$X = \big(x_1 \cdot 72 \cdot (72^{-1} \pmod 7) + \\ + x_2 \cdot 63 \cdot (63^{-1} \pmod 8) + \\ + x_3 \cdot 56 \cdot (56^{-1} \pmod 9)\big) \pmod{504}.$$

Вычислив обратные, получим общее решение:

$$X = (x_1 \cdot 288 - x_2 \cdot 63 + x_3 \cdot 280) \pmod{504}$$

Если $x_1 = x_2 = x_3 = 1$, то $X = 1$. При $x_1 = 2,\ x_2 = 1,\ x_3 = 4$. $X = 121$.

Теорема 6. *Пусть НОД$(a, n) = d$. Тогда*

если $d \mid b$, то сравнение

$$ax \equiv b \pmod n \tag{8}$$

имеет d решений;

если $d \nmid b$, то сравнение (8) не имеет решений.

Алгоритм решения сравнения (8) при $d \mid b$

Пусть $n = n_1 d,\ a = a_1 d,\ b = b_1 d,$ НОД$(a_1, n_1) = 1$.
Решаем сравнение:

$$a_1 x \equiv b_1 \pmod{n_1}$$

Находим его решение $x_0 = a_1^{-1} \pmod{n_1} \cdot b_1$ Остальные решения сравнения (8) имеют вид:

$$x_i = x_0 + in_1,\ i = \overline{1, d-1}$$

Пример. Решить сравнение

$$63 \cdot x \equiv 87 \pmod{303} \tag{9}$$

Решение. Находим НОД$(63, 303) = 3$. Так как $3 \mid 87$, то сравнение (9) имеет 3 решения. Решаем сравнение:

$$21 \cdot x \equiv 27 \pmod{101}$$

Находим его решение $x_0 = 21^{-1} \pmod{101} \cdot 29 = 77 \cdot 29 \equiv 11 \pmod{101}$.
Остальные 2 решения:
$x_1 = 11 + 101 = 112$,
$x_2 = 11 + 202 = 213$.

1.1. Упражнения

Упражнение 1.1. Найти обратный к элементу a по модулю n.

N	1	2	3	4	5	6	7	8	9	10
p	601	701	910	620	599	650	810	840	920	640
a	58	37	47	53	29	61	77	79	89	401

N	11	12	13	14	15	16	17	18	19	20
p	740	840	602	881	700	800	770	870	923	661
a	103	79	97	227	341	109	113	103	109	257

Упражнение 1.2. Убедиться, что a является первообразным корнем по модулю p. (Проверить что a есть примитивный элемент $\mathbb{Z}_p^*$)

N	1	2	3	4	5	6	7	8
p	101	103	107	109	113	127	131	137
a	2	5	2	6	3	3	2	3

N	9	10	11	12	13	14	15	16
p	139	149	151	157	163	167	173	179
a	2	2	6	5	2	5	2	2

Упражнение 1.3. Используя теорему Ферма, доказать, что $p \mid 2^{2^{an+b}} + c$ при $n \geqslant 0$.

N	1	2	3	4	5	6	7	8	9	10
p	11	37	67	97	29	13	73	23	43	89
a	4	6	10	6	6	4	6	10	6	10
b	1	2	1	6	2	2	2	1	1	1
c	7	21	63	36	13	10	57	19	39	85

N	11	12	13	14	15	16	17	18	19	20
p	61	43	47	53	19	31	71	41	79	83
a	4	6	11	12	6	4	12	4	12	20
b	4	2	1	2	2	1	1	3	2	2
c	39	27	43	39	3	27	67	31	63	67

Указание: Нужно вычислить 2^{an+b} по модулю $p-1$. Например, рассмотрим вариант 5. Заметим, что $(2^{6n}) = (2^6)^n \equiv 1 \pmod 7$. Следовательно, $7 \mid 2^{6n} - 1$. Поэтому $28 \mid 2^{6n+2} - 4 = 4(2^{6n} - 1)$ и $2^{6n+2} = 28k + 4$, т.е. $2^{2^{6n+2}} \equiv 16 \pmod{29}$. Это означает, что $29 \mid 2^{2^{6n+2}} + 13$.

Упражнение 1.4. Решить сравнение $ax \equiv b \pmod{p}$.

N	1	2	3	4	5	6	7	8	9	10
p	211	223	227	229	233	239	241	251	257	263
a	79	87	96	90	91	92	93	94	95	101
b	51	52	53	54	55	56	57	58	59	60

N	11	12	13	14	15	16	17	18	19	20
p	269	271	277	281	283	293	307	311	313	317
a	102	103	104	120	121	122	123	124	125	126
b	61	62	63	64	65	66	67	68	69	70

Упражнение 1.5. Решить сравнение $ax \equiv b \pmod{M}$.

N	1	2	3	4	5	6	7	8	9	10
M	159	148	177	164	183	172	201	188	219	212
a	60	16	63	20	42	24	81	28	87	32
b	51	68	75	76	69	80	54	56	57	52

N	11	12	13	14	15	16	17	18	19	20
M	237	236	249	244	267	268	284	292	291	303
a	102	36	57	40	117	44	56	88	123	144
b	60	60	63	80	60	84	92	64	90	99

N	21	22	23	24	25	26	27	28	29	30
M	305	311	324	343	426	312	348	338	374	339
a	23	29	31	37	41	43	47	53	59	61
b	50	60	51	61	71	81	70	80	91	90

N	31	32	33	34	35
M	359	375	385	378	352
a	67	71	73	79	83
b	54	55	64	65	75

N	1	2	3	4	5	6	7
M	7820	9860	6460	7140	9660	7980	12180
a	79	83	89	97	101	103	109
b	1000	1001	1002	1003	1004	1005	1006

N	8	9	10	11	12	13	14
M	12075	9177	14007	10626	8602	12650	15850
a	113	127	131	223	211	229	71
b	1007	1008	1009	1010	1011	1012	1013

N	15	16	17	18	19	20	
M	10925	16675	14614	7854	9350	12122	
a	73	137	149	151	157	163	
b	1014	1015	1016	1017	1018	1019	

Упражнение 1.6. Найти минимальный первообразный в $\mathbb{Z}_p$.

N	1	2	3	4	5	6	7	8	9	10
p	97	103	113	127	137	157	167	193	199	223
N	11	12	13	14	15	16	17	18	19	20
p	233	257	263	277	281	283	307	331	353	383

Упражнение 1.7. На основе К.Т.О. найти все решения сравнения $x^2 \equiv a \pmod{p \cdot q}$.

N	1	2	3	4	5	6	7	8	9	10	11	12
a	9	4	16	25	49	9	16	4	25	49	64	49
p	17	13	23	31	43	19	23	47	53	61	71	53
q	19	23	29	37	41	37	41	19	17	29	19	17

2. Квадратичные вычеты, сравнения, символ Лежандра

Пусть p — простое. Число $a \in \mathbb{Z}$ называется квадратичным вычетом по модулю p, если существует $x_0 \in \mathbb{Z}$ такое, что $x_0^2 \equiv a \pmod{p}$.

Символ Лежандра $\left(\frac{a}{b}\right) = \begin{cases} 1, \text{если } a \text{ — квадратичный вычет,} \\ -1, \text{в противном случае.} \end{cases}$

Свойства символа Лежандра

1) $\left(\frac{1}{p}\right) = 1$,

2) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

3) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$,

4) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, если $a \equiv b \pmod{p}$,

5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,

6) $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$, где $p,\ q$ — различные простые $\neq 2$.

Используя эти свойства можно эффективно вычислять символ Лежандра.

Пример. Определить является ли $a = 401$ квадратичным вычетом по модулю 853.
Вычислим символ Лежандра с учетом его свойств:
$\left(\frac{401}{853}\right) \overset{(6)}{=} (-1)^{\frac{853-1}{2}\cdot\frac{401-1}{2}}\left(\frac{853}{401}\right) \overset{(4)}{=} \left(\frac{51}{401}\right) \overset{(3)}{=} \left(\frac{3}{401}\right)\cdot\left(\frac{17}{401}\right) \overset{(6)}{=}$
$\overset{(6)}{=} (-1)^{\frac{3-1}{2}\cdot\frac{401-1}{2}}\left(\frac{401}{3}\right)\cdot(-1)^{\frac{17-1}{2}\cdot\frac{401-1}{2}}\left(\frac{401}{17}\right) \overset{(4)}{=} \left(\frac{2}{3}\right)\cdot\left(\frac{10}{17}\right) =$
$= -\left(\frac{2}{17}\right)\cdot\left(\frac{5}{17}\right) \overset{(5),(6)}{=} -(-1)^{\frac{17^2-1}{8}}(-1)^{\frac{17-1}{2}\cdot\frac{17-1}{2}} = (-1)(+1)(+1) = -1.$
Таким образом, 401 — квадратичный невычет по модулю 853, т.е. сравнение $x^2 \equiv 401 \pmod{853}$ не имеет решений.

Алгоритм решения сравнения по модулю $x^2 \equiv a \pmod{n}$

1) $n = p = 4m + 3,\ p$ — простое.
   Вычисляем символ Лежандра $\left(\frac{a}{p}\right) = \sigma$. Если $\sigma = -1$, то решений нет. Если $\sigma = 1,$ то $x \equiv \pm a^{m+1} \pmod{p}$.

   Пример. Решить сравнение $x^2 \equiv 173 \pmod{419}$.
   Вычисляем символ Лежандра. Так как 173 — простое, то
   $\left(\frac{173}{419}\right) = (-1)^{\frac{173-1}{2}\cdot\frac{419-1}{2}}\left(\frac{419}{173}\right) = \left(\frac{73}{173}\right) = (-1)^{\frac{73-1}{2}\cdot\frac{173-1}{2}}\left(\frac{173}{73}\right) =$
   $= \left(\frac{27}{73}\right) = \left(\frac{3}{73}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{73-1}{2}}\left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$
   Следовательно, данное сравнение разрешимо.
   Далее, так как, $419 = 104\cdot 4 + 3$, то искомое решение
   $x = \pm 173^{105} \pmod{419} = \pm 173^{64}\cdot 173^{32}\cdot 173^{8}\cdot 103 = \pm 43 \pmod{419}$.

2) $n = p = 8m + 5,\ p$ — простое, $\left(\frac{a}{p}\right) = 1$.
   Вычисляем $\sigma = a^{2m+1}$. Если $\sigma = 1$, то $x \equiv \pm a^{m+1} \pmod{p}$ — искомое решение.
   Если $\sigma = a^{2m+1} = -1$, то $x = \pm a^{m+1}\cdot 2^{2m+1} \pmod{p}$.

   Пример. Решить сравнение $x^2 \equiv 165 \pmod{421}$.
   Так как $421 = 8\cdot 52 + 5$, то вычисляем
   $\sigma = 165^{105}\cdot 165^{32}\cdot 165^{8}\cdot 165 \pmod{421} \equiv -1 \pmod{421}$.
   Поэтому, $x = \pm 165^{53}\cdot 2^{105} \pmod{421}$.
   $2^{105} = 29 \pmod{421},\ 165^{53} \equiv 405 \pmod{421}$.
   Отсюда следует, что $x = \pm 43 \pmod{421}$.

3) $p = 2^m s + 1,\ \left(\frac{a}{p}\right) = 1,\ m \geq 3,\ \text{НОД}(s, 2) = 1.$
   Находим невычет b по модулю p. Затем вычисляем следующие параметры:

$r \equiv a^{\frac{s+1}{2}} \pmod p,\ c \equiv b^s \pmod p,\ h \equiv r^2 a^{-1} \pmod p$.
Искомое решение ищем в виде:
$x \equiv \pm c^j r \pmod p,\ j = j_0 + j_1 \cdot 2 + \ldots + j_{m-2} \cdot 2^{m-2},\ j_k \in \{0, 1\}$.
Далее последовательно определим $j_k,\ k = \overline{0, m-2}$.

- $k = 0$. Вычисляем $\epsilon_0 = h^{2^{m-2}} \pmod p,\ \epsilon_0 = \pm 1$.
  Находим $j_0 = \frac{1-\epsilon_0}{2}$.
- $k = 1$. Вычисляем $\epsilon_1 = h^{2^{m-3}} \cdot c^{2^{m-2} \cdot \epsilon_0} \equiv \pm 1$ и находим $j_1 = \frac{1-\epsilon_1}{2}$.
- Далее индуктивно, если мы уже вычислили $j_0, \ldots, j_{t-1}$, то вычисляем $\epsilon_t = h^{2^{m-2-t}} \cdot c^{j_0 2^{m-t-1} + j_1 2^{m-t} + \cdots + j_{t-1} 2^{m-2}} = \pm 1$, и находим $j_t = \frac{1-\epsilon_t}{2},\ t = 2, \ldots, m-2$.

Пример. Решить сравнение $x^2 \equiv 30 \pmod{241}$.

а) Находим невычет b по модулю 241. Например, $b = 13$.

б) Выписываем разложение $p - 1 = 240 = 2^4 \cdot 15$, $w = 4, s = 15$.
Проверим, что $a = 30$ вычет. Для этого вычисляем символ Лежандра:

$$\left(\frac{30}{241}\right) = \left(\frac{2}{241}\right)\left(\frac{3}{241}\right)\left(\frac{5}{241}\right) = 1.$$

Вычисляем $c = b^s = 13^{15} = 13^8 \cdot 13^4 \cdot 13^2 \cdot 13 = 76 \pmod{241}$.
$r = a^{\frac{s+1}{2}} = 30^8 \equiv 1 \pmod{241}$,
$a^{-1} = 30^{-1} \pmod{241} = -8 \equiv 233 \pmod{241}$,
$h = r^2 \cdot a^{-1} \equiv -8 \pmod{241}$.
Искомое решение $x = \pm c^{j_0 + 2j_1 + \cdots + 2^{m-2} j_{m-1}} \cdot r$ в нашем случае имеет вид:

$$x = \pm 76^{j_0 + 2j_2 + 4j_2}.$$

в) Последовательно вычисляем j_0, j_1 и j_2:
- $\varepsilon_0 = h^{2^2} = (-8)^4 \pmod{241} = -1$, следовательно $j_0 = \frac{1-\varepsilon_0}{2} = 1$,
- $\varepsilon_1 \equiv h^2 c^4 = 64 \cdot 76^4 \equiv -1 \pmod{241}$, $j_1 = \frac{1-\varepsilon_1}{2} = 1$,
- $\varepsilon_2 \equiv h c^6 = -8 \cdot 76^6 \equiv -1 \pmod{241}$, $j_2 = \frac{1-\varepsilon_2}{2} = 1$.
  Поэтому $x = \pm 76^{1+2+4} \cdot 1 = \pm 76^7 = 111 \pmod{241}$.

Алгоритм решения сравнения второй степени по примарному модулю $p^m,\ p \geq 3$

Напомним, что сравнение

$$x^2 \equiv a \pmod{p^m} \tag{10}$$

имеет ровно два решения тогда и только тогда, когда $\left(\frac{a}{p}\right) = 1$.

1) Находим любое из двух решений $\lambda_0 \in \mathbb{Z}$ сравнения $x^2 \equiv a \pmod{p}$.

   Полагаем $x_0 = \lambda_0$ и вычисляем $\delta_0 = (-2\lambda_0)^{-1} \pmod{p}$.

2) Далее последовательно при $i = 1, \ldots, m-1$ вычисляем

   а) $x_{i-1}^2 = (\lambda_0 + \cdots + \lambda_{i-1}p^{i-1})^2$,

   б) находим $t_i \pmod{p}$ такое, что $x_{i-1}^2 = a + t_i p^i$,

   в) вычисляем $\lambda_i = \delta_0 t_i \pmod{p}$,

   г) находим $x_i = \lambda_0 + \cdots + \lambda_i p^i$.

3) Искомое решение $x = \pm x_{m-1}$.

Пример. Решить сравнение $x^2 \equiv 136 \pmod{625}$.

Так как $625 = 5^4$, то $m = 4, \delta_0 = (-2)^{-1} \equiv 2 \pmod{5}$, искомое решение будет иметь вид:

$$x = \pm(\lambda_0 + \lambda_1 \cdot 5 + \lambda_2 \cdot 5^2 + \lambda_3 \cdot 5^3).$$

Последовательно находим λ_i:

1) $i = 0$. Так как $136 \equiv 1 \pmod{5}$, то можно положить $x_0 = 1 = \lambda_0$. Поскольку $1^2 = 136 - 27 \cdot 5$, то $t_1 = -27 \equiv 3 \pmod{5}$, $\lambda_1 = \delta_0 t_1 = 2 \cdot 3 \equiv 1 \pmod{5}, x_1 \equiv 1 + 1 \cdot 5 = 6$.

2) $i = 1$. Так как $x_1^2 \equiv 36 = 136 - 4 \cdot 25$, то $t_2 = -4 \equiv 1 \pmod{5}, \lambda_2 = 2 \cdot 1 \equiv 2$, $x_2 = 1 + 1 \cdot 5 + 2 \cdot 25 = 56$.

3) $i = 2$. Так как $x_2^2 \equiv 3136 = 136 + 24 \cdot 125$, то $t_3 = 24 \equiv 4 \pmod{5}, \lambda_3 = 2 \cdot 4 \equiv 3 \pmod{5}$, и искомое решение $x = x_3 = \pm(1 + 1 \cdot 5 + 2 \cdot 25 + 4 \cdot 125) \equiv 194 \pmod{625}$.

Алгоритм решения сравнения $x^2 \equiv a \pmod{2^m}, m \geq 3$

Это сравнение разрешимо тогда и только тогда, когда $a \equiv 1 \pmod{8}$ и в этом случае будет иметь 4 решения.

Искомое решение будет иметь вид

$$x = 1 + \lambda_2 \cdot 2^2 + \ldots + \lambda_{n-2} \cdot 2^{n-2}.$$

1) Вычислим $\lambda_2 = \frac{a-1}{8} \pmod{2}$ и полагаем $x_2 = 1 + 4\lambda_2$.

2) Последовательно для $i = 3, \ldots, n-2$ вычисляем $\lambda_i = \frac{a - x_{i-1}^2}{2^{i+1}} \pmod{2}$, $x_i = x_{i-1} + \lambda_i 2^i$.

3) При $i = n-2$ получим $x_{n-2} = X_1$. Остальные решения это:

   $X_2 = -x_1 = 2^n - X_1$,

   $X_3 = X_1 + 2^{n-1}$,

   $X_4 = -X_1 - 2^{n-1}$.

Пример. Решить сравнение $x^2 \equiv 209 \pmod{512}$.

В нашем примере $n = 8$, поэтому $X_1 = x_6$. Последовательно вычисляем $x_i,\ i = 2, \ldots, 6$:

1) $\lambda_2 = \frac{209-1}{8} \equiv 0 \pmod 2,\ x_2 = 1$,

2) $\lambda_3 = \frac{209-1^2}{16} = 13 \equiv 1 \pmod 2,\ x_3 = 1 + 2^3 = 9$,

3) $\lambda_4 = \frac{209-9^2}{32} = 4 \equiv 0 \pmod 2,\ x_4 = 9$,

4) $\lambda_5 = \frac{209-9^2}{64} = 2 \equiv 0 \pmod 2,\ x_5 = 9$,

5) $\lambda_6 = \frac{209-9^2}{128} \equiv 0 \pmod 2,\ x_5 = 9 + 2^6 = 73 = X_1$.

Следовательно, $X_2 = -73 = 183, X_3 = 73+128 = 201, X_4 = -201 = 55$.

Алгоритм решения сравнения $x^2 \equiv a \pmod{p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}}$

1) Определяем разрешимость сравнения по модулю $p_1^{n_1},\ i = 1, \ldots, k$.

2) В случае разрешимости по каждому примарному модулю, находим решение x_i по каждому примарному модулю.

3) Общее решение исходного сравнения вычисляем на основе Китайской теореме об остатках.

Пример. Решить сравнение $x^2 \equiv 1081 \pmod{2^4 \cdot 3^3 \cdot 5^2}$.

Выписываем систему сравнений:

$$\begin{cases} x^2 = 1081 \equiv 9 \pmod{16}, \\ x^2 = 1081 \equiv 1 \pmod{27}, \\ x^2 = 1081 \equiv 6 \pmod{25}. \end{cases}$$

Первое сравнение имеет четыре решения $x_1 \in \{\pm 3, \pm 5\}$.

Второе сравнение — два решения $x_2 = \pm 1$.

Третье сравнение — два решения $x_3 = \pm 9$.

Общее решение будет иметь вид

$X = x_1(27 \cdot 25)[(27 \cdot 25)^{-1} \pmod{16}] + x_2(16 \cdot 25)[(16 \cdot 25)^{-1} \pmod{27}] + x_3(16 \cdot 27)[(16 \cdot 27)^{-1} \pmod{25}] \pmod{10800} = 7425 \cdot x_1 + 4400 \cdot x_2 + 3024 \cdot x_3 \pmod{10800}$.

Например, если $x_1 = -3, x_2 = -1, x_3 = 9$, то получим частное решение: $X_0 = -22275 - 4400 + 27216 \equiv 541 \pmod{10800}$.

2.1. Задачи

2.1. Доказать, что если НОД$(2a, m) = 1$, то сравнение $ax^2+bx+c \equiv 0 \pmod m$ равносильно сравнению $x^2 \equiv A \pmod m$.

2.2. Доказать, что если НОД$(a, m) = 1$, то $x \equiv ba^{\varphi(n)-1}$ — решение сравнения $ax \equiv b \pmod m$.

2.3. Доказать, что если $a \in \mathbb{Z}_p^*$, то $x \equiv b(-1)^{a-1}\binom{p-1}{a-1} \pmod p$ есть решение сравнения $ax \equiv b \pmod p,\ p > 2$.

2.4. Доказать, что если p — простое, $p > 2$, то $\frac{2^p-2}{p} \equiv 1 + 2^{-1} + 3^{-1} + ... + (p-1)^{-1} \pmod p$.

2.5. Доказать, что $(p-1)! \equiv -1 \pmod p,\ p > 2,\ p$ — простое.

2.6. Доказать, что если простое $p = 4m+1,\ m > 0$, то $x = \pm 1 \cdot 2 \cdot ... \cdot 2m$ есть решение сравнения $x^2 + 1 \equiv 0 \pmod p$.

2.7. Доказать, что сравнение $x^2 + 1 \equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod 4$.

2.8. Доказать, что сравнение $x^2 + 2 \equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p = 1, 3 \pmod 8$.

2.9. Доказать, что сравнение $x^2 + 3 \equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod 6$.

2.10. Доказать бесконечность количества простых чисел вида $(a)\ 4m \pm 1$, $(b)\ 6m \pm 1$.

2.11. Доказать, что если $p = 2^n + 1$ — простое, $n > 2$, то $\left(\frac{3}{p}\right) = -1$ и $< 3 >= \mathbb{Z}_p^*$.

2.12. Доказать, что если $p = 2^n + 1$ — простое и $\left(\frac{a}{p}\right) = -1$, то $< a >= \mathbb{Z}_p^*$.

2.13. Доказать, что если $p = 4q + 1,\ p$ и q — простые, то $< 2 >= \mathbb{Z}_p^*$.

2.14. Доказать, что если $p = 2^{2^n} + 1$ — простое и $\left(\frac{a}{p}\right) = -1$, то $< a >= \mathbb{Z}_p^*$.

2.15. Доказать, что если $p = 2^{2^n} + 1$ — простое, $n > 2$, то $< 7 >=< 3 >=< 5 >= \mathbb{Z}_p^*$.

2.16. Доказать, что если $n > 1,\ p$ — простое, $n|p-1$, НОД$(a, b) = 1$, то сравнение $x^n \equiv a \pmod p$ разрешимо тогда и только тогда, когда $a^{\frac{n-1}{p}} \equiv 1 \pmod p$ и в этом случае оно имеет n решений.

2.17. Доказать, что если p — простое и $p|2^{2^n}+1$, то
(a) $p \equiv 1 \pmod{2^{n+1}}$ если $n \geqslant 1$
(b) $p \equiv 1 \pmod{2^{n+2}}$ если $n > 1$.

2.18. Доказать, что если p — простое и $p|b^n+1$, то либо $p|b^d+1$ и $\frac{n}{d}$ — нечетное, либо $p \equiv 1 \pmod{2n}$.

2.19. Доказать, что если $p = 4m+1$ — простое и НОД$(k,p) = 1$, $S(k) = \sum_1^{p-1} \left(\frac{x(x^2+k)}{p}\right)$, то
(a) $S(k) \equiv 0 \pmod 2$,
(b) $S(kt^2) = \left(\frac{t}{p}\right) S(k)$.

2.20. Доказать, что если НОД$(k,p) = 1$, то $\sum_1^{p-1} \left(\frac{x(x+k)}{p}\right) = -1$.

2.2. Указания к решению задач

2.1. Выделить полный квадрат.

2.2. Использовать теорему Эйлера.

2.4. $2^p = (1+1)^p$.

2.5. Разложить многочлен $f(x) = x^{p-1} - 1$ на множители над полем $\mathbb{Z}_p$.

2.6. Использовать задачу 2.5: $(p-1)! = (4m)!$, и $-k \equiv p - k \pmod p$.

2.7.-2.9. Использовать символ Лежандра для $a = -1, -2, -3$.

2.10. Пусть $p_1, ...p_k$ — различные простые числа и $p_i \equiv 1 \pmod 6$, $i = \overline{1,k}$. Положим $N = (2p_1...p_k)^2 + 3$. Так как $p_i \equiv 1 \pmod 6$, то и $N \equiv 1 \pmod 6$. Пусть p — наименьший простой делитель числа N. Очевидно, что $p \neq p_i,\ i = \overline{1,k}$ и $N \equiv 0 \pmod p$, то есть $x_0 = 2p_1...p_k$ есть решение сравнения $x^2 + 3 \equiv 0 \pmod p$. Из задачи 2.9 следует, что $p \equiv 1 \pmod 6$.

2.11.-2.15. Воспользоваться критерием примитивности элемента из поля $\mathbb{Z}_p$.

2.16. Необходимость. Если $x_0^n \equiv a \pmod p$, то по теореме Эйлера: $a^{\frac{p-1}{n}} \equiv x_0^{p-1} \equiv 1 \pmod p$.
Достаточность. Пусть $t = \frac{p-1}{n}$ и $a^t \equiv 1 \pmod p$. Из теоремы Ферма следует:

$$x^p - x \equiv x\left(x^{p-1} - 1\right) \equiv x\left(x^{tn} - a^t\right) + x\left(a^t - 1\right) \equiv x\left(\left(x^n\right)^t - a^t\right) +$$
$$+ x\left(a^t - 1\right) \equiv x\left(x^n - a\right)\left(x^{n(t-1)} + x^{n(t-2)}a + \ldots + x^n a^{t-2} + a^{t-1}\right) +$$
$$+ x\left(a^t - 1\right) \equiv x\left(x^n - a\right)h(x) + x\left(a^t - 1\right) \pmod p, \quad (11)$$

$$deg\left[h(x)\right] = n(t-1) = nt - n = p - 1 - n.$$

Так как $a^t \equiv 1 \pmod p$, то из (11) следует, что

$$x^p - x \equiv x\left(x^n - a\right)h(x) \pmod p. \quad (12)$$

Многочлен $x^p - x$ имеет p корней над полем $\mathbb{Z}_p$. Многочлен в правой части (12) также имеет степень p. Поэтому многочлен $f(x) = x^n - a$ должен иметь равно n корней над полем $\mathbb{Z}_p$, то есть сравнение $x^n \equiv a \pmod p$ разрешимо и имеет n решений.

2.17. Из $p | 2^{2^n} + 1$ следует, что $2^{2^n} \equiv -1 \pmod p$. Следовательно, $2^{2^{n+1}} \equiv 1 \pmod p$. Поэтому $or_p(2) = 2^{n+1}$. Так как $ord_p(2) | p - 1$, то $p = 1 + v \cdot 2^{n+1}$, то есть $p = 1 \pmod{2^{n+1}}$.

2.18. Из задачи 2.17 следует, что $p = 1 + 2^{n+1} \cdot v$. С другой стороны, при $n > 1$,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{2^{2n+2}v^2+2^{n+2}v}{8}} = (-1)^{2^{2n-1}v^2+2^{n-1}v} = 1.$$

Но $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Так как по условию, $2^{2^n} \equiv -1 \pmod{p}$, то $or_p(2) = 2^{n+1}$. Поэтому $2^{n+1} | \frac{p-1}{2}$, то есть $p \equiv 1 \pmod{2^{n+2}}$.

2.19. Из $p = 4k + 1$ следует, что $\left(-\frac{x}{p}\right) = \left(\frac{x}{p}\right)$. Поэтому

$$\sum_1^{p-1} \left(\frac{x(x^2+k)}{p}\right) = \sum_1^{\frac{p-1}{2}} \left(\frac{x(x^2+k)}{p}\right) + \sum_1^{\frac{p-1}{2}} \left(\frac{-x(x^2+k)}{p}\right) \equiv 0 \pmod{p}.$$

2.20. Заметим, что

$$\sum_1^{p-1} \left(\frac{x(x+k)}{p}\right) = \sum_1^{p-1} \left(\frac{x^2(1+x^{-1}k)}{p}\right) \equiv \sum_1^{p-1} \left(\frac{1+x^{-1}k}{p}\right) = S.$$

Так как $\{1 + x^{-1}k | x \in \mathbb{Z}_p^*\} = \mathbb{Z}_p^* \backslash \{1\}$, то $S \equiv -1$.

2.3. Упражнения

2.21. Решить сравнение $x^2 \equiv a \pmod{p},\ p \equiv 3 \pmod{4}$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
p	67	71	79	83	67	71	79	83	67	71	79	83	67	71	79	83
a	37	32	-6	28	23	3	-29	-20	29	24	26	33	-27	-11	22	27

2.22. Решить сравнение $x^2 \equiv a \pmod{101}$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	24	19	22	33	52	-22	13	56	6	65	31	5	88	78	58	17

2.23. Решить сравнение $x^2 \equiv a \pmod{p},\ p \equiv 1 \pmod{8}$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	89	97	137	113	89	97	137	113	89	97	137	113	89	97	137
a	40	66	-30	-16	21	6	-2	62	34	75	56	-8	-10	-22	8

2.24. Решить сравнение $x^2 \equiv a \pmod{p^n}$.

N	1	2	3	4	5	6	7	8
p	5	7	3	5	7	3	5	7
n	5	4	7	5	4	7	5	4
a	766	263	1048	764	130	385	946	-488

N	9	10	11	12	13	14	15	16
p	3	5	7	3	5	7	3	5
n	7	5	4	7	5	4	7	5
a	-230	976	1059	-482	-411	1961	118	696

2.25. Решить сравнение $x^2 \equiv a \pmod{1024}$.

N	1	2	3	4	5	6	7	8
a	689	641	721	929	241	705	273	993
N	9	10	11	12	13	14	15	16
a	817	769	849	33	369	833	401	97

2.26. Решить сравнение $x^2 \equiv a \pmod{p \cdot q}$.

N	1	2	3	4	5	6	7	8
p	29	29	29	29	29	29	31	31
q	31	41	43	37	47	53	41	43
a	312	892	633	86	632	479	10	1000
N	9	10	11	12	13	14	15	16
p	31	31	31	41	41	41	41	43
q	37	47	53	43	37	47	53	37
a	411	444	820	2031	860	1207	187	728

2.27. Решить сравнение: $x^2 \equiv a \pmod{m}$, $a = a_i,\ i \in \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$, $m \in \{p_1,\ p_2,\ p_3,\ p_4^n,\ 2^n,\ n\}$.

NP	p_1	a_1	p_2	a_2	p_3	a_3	p_4^n	a_4	2^n	a_5	n	a_6
1	263	46	173	136	193	23	5^6	-299	2^9	-47	3600	481
2	271	228	197	41	241	79	3^8	619	2^{10}	249	10800	312
3	283	278	229	135	257	-15	7^4	-698	2^9	-159	9800	14809
4	307	215	269	120	281	20	11^3	-380	2^{10}	161	137200	79801
5	311	63	277	165	337	91	19^3	123	2^{10}	-23	7056	3145
6	331	296	293	10	353	317	13^3	-493	2^9	-199	21168	9193
7	347	83	317	313	401	176	17^3	2112	2^{10}	145	49392	47329
8	359	34	349	243	409	385	5^5	-461	2^9	-15	148176	19105
9	367	137	373	88	433	242	3^8	2974	2^{10}	-167	26000	22489
10	383	8	389	141	449	329	7^4	387	2^9	201	34000	26249
11	263	145	173	90	193	-48	11^3	542	2^9	65	46000	1761
12	271	32	197	178	241	-58	19^3	1924	2^{10}	-63	38000	9849
13	283	34	229	53	257	72	13^3	-339	2^{10}	-183	15984	9505
14	307	182	269	56	281	143	17^3	-1993	2^9	217	17712	9241
15	311	18	277	13	337	162	5^5	-1419	2^{10}	113	18576	16633
16	331	191	293	268	353	19	19^3	134	2^9	41	20304	15817
17	347	277	317	38	401	183	11^3	500	2^{10}	121	60368	56065
18	359	204	349	346	409	384	7^4	-598	2^9	-103	71344	15409
19	367	291	373	208	433	217	3^8	-1130	2^{10}	137	104272	48409
20	383	130	389	313	449	282	17^3	-1912	2^9	-127	126224	26601

3. Конечные поля

Конечное поле $GF(p^n)$ определяется характеристикой p (p — простое) и неприводимым над полем $\mathbb{Z}_p$ многочленом $f(x)$ степени n. Элементы поля $GF(p^n)$ это многочлены над полем $\mathbb{Z}_p$ степени не более $n-1$, то есть

$$GF(p^n) = \mathbb{Z}_p[x]/(f(x)) = \{\sum_{i=0}^{n-1} \alpha_i x^i \mid \alpha_i \in \mathbb{Z}_p\}$$

Число n — это степень поля. Относительно операции сложения $GF(p^n)$ — это линейное пространство над полем $\mathbb{Z}_p$.

Если $a_1(x), a_2(x) \in GF(p^n)$, то $a_1(x)a_2(x) = a_3(x)$ — это остаток от деления произведения многочленов $a_1(x)$ и $a_2(x)$ на неприводимый многочлен, определяющий данное поле $GF(p^n)$.

Пример 1. $GF(7^2) = \mathbb{Z}_7[x]/(x^2+x+3) = \{\alpha x + \beta \mid \alpha, \beta \in \mathbb{Z}_7\}$.

Пусть $a_1(x) = 2x+1,\ a_2(x) = x+2$.

Тогда $a_1(x) + a_2(x) = (2x+1) + (x+2) = 3x+3$. $a_1(x)a_2(x) = (2x+1)(x+2) = 2x^2 + 4x + x + 2 = 2(-x-3) + 5x + 2 = 3x - 4 = 3x + 3$.

Вычисление обратного к элементу $a(x) \in \mathbb{Z}_p[x]/(f(x)) = GF(p^n)$, как правило, аналогично нахождению обратного элемента в поле $\mathbb{Z}_p$ на основе алгоритма Евклида.

Алгоритм вычисления обратного к элементу $\mathbf{a(x)}$ в поле $\mathbf{GF(p^n)} = \mathbb{Z}_\mathbf{p}[\mathbf{x}]/(\mathbf{f(x)})$

Полагаем $r_0 = f(x),\ r_1 = a(x)$. Далее, применяем алгоритм Евклида вычисления НОД(r_0, r_1):

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, \\ r_1 &= r_2 q_2 + r_3, \\ &\vdots \\ r_{k-2} &= r_{k-1} q_{k-1} + \varepsilon, \\ r_{k-1} &= \varepsilon(\varepsilon^{-1} r_{k-1}). \end{aligned}$$

Заметим, что так как $f(x)$ неприводимый, то НОД $(f(x), a(x)) = \varepsilon \in \mathbb{Z}_p^*$. Далее, полагаем $P_0 = 1,\ P_1 = q_1$ и последовательно вычис-

ляем

$$P_i = q_i P_{i-1} + P_{i-2},\ i = \overline{2,k} \tag{13}$$

При этом $P_k = \varepsilon^{-1} \cdot f(x),\ a^{-1}(x) = (-1)^{k+1} \cdot \varepsilon^{-1} P_{k-1}(x)$.

Пример 2. Найти $a^{-1}(x)$ для $GF(5^4) = \mathbb{Z}_5[x]/(x^4+x^2+2x+2),\ a(x) = x^3 + x^2 + 1$.

Решение. Применим алгоритм Евклида:
$x^4 + x^2 + 2x + 2 = (x^3 + x^2 + 1)(x - 1) + 2x^2 + x - 2,$
$x^3 + x^2 + 1 = (2x^2 + x - 2)(-2x - 1) + 2x - 1,$
$2x^2 + x - 2 = (2x - 1)(x + 1) - 1,$
$(2x - 1) = (-1)(1 - 2x),\ k = 4,\ \varepsilon = -1.$

Проводим вычисления по формуле (13):
$P_0 = 1,\ P_1 = x - 1,\ P_2 = (-2x - 1)(x - 1) + 1 = -2x^2 + x + 2,\ P_3 = (x + 1)(-2x^2 + x + 2) + x - 1 = -2x^3 - x^2 - x + 1,\ P_4 = (1 - 2x)(-2x^3 - x^2 - x + 1) - 2x^2 + x + 2 = (-1)(x^4 + x^2 + 2x + 2).$

Таким образом, $(x^3 + x^2 + 1)^{-1} = (-1)(-1)^{4+1}(-2x^3 - x^2 - x + 1) = -2x^3 - x^2 - x + 1$.

Пример 3. Найти обратный к $a(x) = 3x^2 + x + 3$ в поле $GF(7^3) = \mathbb{Z}_7[x]/(x^3 + 2x + 1)$.

Решение. Находим НОД$(x^3 + 2x + 1,\ 3x^2 + x + 3)$ по алгоритму Евклида:
$x^3 + 2x + 1 = (3x^2 + x + 3)(-2x + 3) - 2x - 1,$
$3x^2 + x + 3 = (-2x - 1)(2x + 2) - 2,$
$-2x - 1 = -2(x - 3).$
Следовательно, $k = 3,\ \varepsilon = -2$.

Далее, вычисляем:
$P_0 = 1,\ P_1 = -2x + 3,$
$P_2 = (2x + 2)(-2x + 3) + 1 = 3x^2 + 2x,$
$P_3 = (x - 3)(3x^2 + 2x) - 2x + 3 = 3(x^3 + 2x + 1) = \varepsilon^{-1}(x^3 + 2x + 1).$
Таким образом,

$$(3x^2 + x + 3)^{-1} = (-1)^{3+1} \cdot 3 \cdot (3x^2 + 2x) = 2x^2 - x.$$

Напомним, что примитивный элемент поля $GF(q)$ — это образующий элемент мультипликативной циклической группы $GF^*(q)$.

Утверждение 1. (Критерий примитивности элемента конечного поля)

Элемент $a \in GF(q)$ является примитивным тогда и только тогда, когда выполнено условие:

$$a^{\frac{q-1}{p}} \neq e$$

для любого простого $p \mid q - 1$.

Многочлен степени n — примитивный над полем $GF(q)$ тогда и только тогда, когда

$$f(x) \nmid x^{\frac{q^n-1}{p}} - 1$$

для любого простого $p \mid q^n - 1$.

3.1. Упражнения

Упражнение 1. Проверить, является ли многочлен $f(x)$ примитивным над полем $\mathbb{Z}_p$.

N	p	$f(x)$
1	7	$x^3 + 2x + 1$
2	3	$x^5 + 2x + 1$
3	5	$x^4 + x^2 + 2x + 2$
4	5	$x^2 - 2x + 2$
5	7	$x^2 + x + 3$
6	2	$x^6 + x + 1$
7	2	$x^6 + x^5 + 1$
8	2	$x^5 + x^2 + 1$
9	2	$x^5 + x^3 + 1$
10	3	$x^4 + x - 1$
11	3	$x^5 + 2x^4 + 1$
12	5	$x^4 + x^3 + 2x^2 + 1$
13	5	$x^3 - 2x^2 + 2$
14	2	$x^6 + x^5 + x^2 + x + 1$
15	2	$x^8 + x^4 + x^3 + x^2 + 1$

Упражнение 2. Убедиться, что элемент

$$a \in GF(7^2) = \mathbb{Z}_7[\theta]/(\theta^2 + \theta + 3),\ a = \alpha a + \beta,\ \alpha, \beta \in \mathbb{Z}_7,$$

является примитивным элементом данного поля.

N	1	2	3	4	5	6	7	8	9	10
α	1	3	-2	3	-1	1	-3	-2	-3	2
β	2	-3	-2	-1	1	1	3	0	1	2

Упражнение 3. Показать, что многочлен $f(x) = x^2 + \theta x + 1$ неприводим над полем $F_4 = \mathbb{Z}_2[\theta]/(\theta^2+\theta+1) = \{0, 1, \theta, \theta+1 \mid \theta^2 = \theta+1\}$ и в поле $F_{16} = \mathbb{F}_4[x]/(x^2+\theta x+1) = \{\alpha x+\beta \mid \alpha, \beta \in F_4,\ x^2 = \theta x+1\}$ найти произведение элементов $a_1 = (\alpha_1 x + \beta_1)$ и $a_2 = (\alpha_2 x + \beta_2)$.

N	1	2	3	4	5	6
α_1	1	θ	$\theta+1$	$\theta+1$	$\theta+1$	θ
β_1	θ	$\theta+1$	1	θ	0	$\theta+1$
α_2	$\theta+1$	1	θ	θ	0	θ
β_2	1	1	0	θ	θ	0

Пример 4.

$a_1 = \theta x + 1,\ a_2 = x + 1,\ (x^2 = \theta x + 1,\ \theta^2 = \theta + 1)$

Решение.

$a_1 a_2 = \theta x^2 + \theta x + x + 1 = \theta(\theta x + 1) + \theta x + x + 1 = \theta^2 x + \theta + \theta x + 1 = \theta x + x + \theta + \theta x + x + 1 = \theta + 1$.

Упражнение 4.

Для элементов a_1 и a_2 упражнения 3 найти обратный в поле F_{16}.

Пример 5.

Найдём обратный к элементу $a = \theta x + 1$.

Применим алгоритм Евклида:

$x^2 + \theta x + 1 = (\theta x + 1)[(\theta x + 1)x + (\theta + 1)] + \theta$

$\theta x + 1 = \theta[(\theta + 1)(\theta x + 1)]$

$P_0 = 1,\ P_1 = (\theta+1)x+\theta+1,\ P_2 = P_0+(\theta+1)(\theta x+1)P_1+P_0 = \varepsilon(x^2+\theta x+1)$

$P_2 = (\theta + 1)x^2 + x + \theta + 1 = (\theta + 1)[x^2 + \theta x + 1]$,

$\varepsilon = \theta,\ \varepsilon^{-1} = \theta + 1$

$(\theta x+1)^{-1} = \varepsilon^{-1} \cdot P_2 = [(\theta+1)x+(\theta+1)](\theta+1) = (\theta+1)^2(x+1) = \theta x+\theta$.

Упражнение 5.

Проверить, что $a \in \mathbb{Z}_p$ является примитивным элементом.

N	1	2	3	4	5	6	7	8	9	10
a	8	8	6	27	-11	8	27	-11	8	6
p	101	107	109	113	127	131	137	139	149	151

N	11	12	13	14	15	16	17	18	19	20
a	5	2	5	5	8	2	3	3	2	3
p	157	163	103	167	179	107	113	137	139	127

Упражнение 6.

В поле $GF(5^3) = \mathbb{Z}_5[\theta]/(\theta^3 - 2\theta + 2)$ найти обратный к элементу $a(\theta) = \alpha_2\theta^2 + \alpha_1\theta + \alpha_0,\ \alpha_i \in \mathbb{Z}_5$.

N	1	2	3	4	5	6	7	8
α_0	1	2	-1	-2	1	2	-1	1
α_1	2	2	2	2	1	1	1	2
α_2	-1	1	-1	1	-2	2	-2	2

N	9	10	11	12	13	14	15
α_0	2	-1	-2	1	-1	2	-2
α_1	-2	2	2	-1	-1	-1	-1
α_2	-1	2	-1	1	2	-2	-1

Упражнение 7.

В поле $GF(7^3) = \mathbb{Z}_7[\theta]/(\theta^3 + 2\theta + 1)$ найти обратный к элементу $a(\theta) = \alpha_2\theta^2 + \alpha_1\theta + \alpha_0,\ \alpha_i \in \mathbb{Z}_7$.

N	1	2	3	4	5	6	7	8
α_0	1	2	3	-1	-2	-3	1	2
α_1	-1	-3	-2	2	1	3	-1	-3
α_2	2	2	1	1	3	3	-2	-2

N	9	10	11	12	13	14	15
α_0	3	1	2	3	1	2	3
α_1	-2	2	1	3	-3	-2	2
α_2	-2	-3	-3	-3	-1	-1	-1

Упражнение 8.

В поле $GF(2^7) = \mathbb{Z}_2[\theta]/(\theta^7 + \theta + 1)$ найти обратный к элементу $a(\theta) = \sum_{i=0}^{6} \alpha_i\theta^i,\ \alpha_i \in \mathbb{Z}_2,\ \tilde{a} = \alpha_6, \ldots, \alpha_0,\ N(a) = \sum_{i=0}^{6} 2^i\alpha_i$.

N	1	2	3	4	5	6	7
$N(a)$	50	43	13	27	30	34	41

N	8	9	10	11	12	13	14
$N(a)$	14	18	21	13	41	53	24

N	15	16	17	18	19	20	21
$N(a)$	36	73	68	91	61	39	47

Упражнение 9.

В поле $GF(5^4) = \mathbb{Z}_5[\theta]/(\theta^4+\theta^2+2\theta+2)$ найти обратный к элементу $a(\theta) = \sum_{i=0}^{3} \alpha_i \theta^i,\ \alpha_i \in \mathbb{Z}_5$.

N	1	2	3	4	5	6	7
α_3	1	-1	2	-2	0	0	0
α_2	1	1	2	2	-1	1	2
α_1	1	0	-1	-1	2	-2	-1
α_0	0	1	2	-1	-2	1	2

N	8	9	10	11	12	13	14
α_3	0	2	2	2	2	1	1
α_2	-2	0	0	0	0	2	-2
α_1	-1	1	-2	2	-1	0	0
α_0	1	-1	1	1	2	-1	1

N	15	16	17	18	19	20	21
α_3	1	1	1	2	-2	1	-1
α_2	-1	1	2	1	-1	2	-2
α_1	2	0	0	-2	1	2	1
α_0	-2	2	2	0	0	0	1

Упражнение 10.

1. Показать, что над полем $F = GF(2^2) = \{0, 1, \theta, \theta+1 \mid \theta^2 = \theta+1\}$ многочлен $f(x) = x^2 + \theta x + 1$ неприводим и описать поле $GF(2^4) = F[x]/(x^2+\theta x+1) = F_{16}$.

2. Выписать в поле F_{16} произведение $(\theta x + 1) \cdot (\theta + 1)x$.

3. Найти $(\theta x + \theta)^{-1}$.

Упражнение 11.

Построить поле $GF(2^6) = F[x]/(x^3 + \theta x + 1)$,

$F = GF(2^2) = \{0, 1, \theta, \theta+1 \mid \theta^2 = \theta+1\}$, убедившить, что многочлен $f(x) = x^3 + \theta x + 1$ неприводим над полем F.

Упражнение 12.

Для отображения $\psi\ :\ GF(8) \to GF(8)$, заданного таблицей, выписать соответствующий многочлен $GF = \mathbb{Z}_2[\theta]/(\theta^3 + \theta + 1)$.

$a(\theta) \in GF(8),\ a(\theta) = \alpha_2\theta^2 + \alpha_1\theta + \alpha_0 \iff \alpha_2\alpha_1\alpha_0 \iff 2^2\alpha_2 + 2\alpha_1 + \alpha_0$. Например, $\theta^2 + \theta = a(\theta) \iff 4 + 2 = 6$.

N	1	2	3	4	5	6	7	8	9	10
0	1	7	1	3	3	1	3	3	0	7
1	2	6	1	2	3	0	2	7	1	5
2	2	5	1	0	4	3	1	2	2	4
3	0	4	2	1	4	2	0	4	0	6
4	4	3	2	7	7	5	7	0	1	3
5	7	2	2	6	7	4	6	1	2	2
6	5	1	5	5	0	7	5	5	0	1
7	6	0	5	4	0	6	4	6	1	0

N	11	12	13	14	15	16	17	18	19	20
0	0	0	5	6	7	4	6	2	7	4
1	2	1	0	1	5	4	6	3	5	1
2	3	7	0	1	5	0	1	4	3	5
3	4	6	4	0	1	0	2	5	1	2
4	5	5	4	0	1	1	3	0	6	6
5	6	4	3	4	0	1	4	1	4	3
6	7	3	3	4	0	1	5	7	2	7
7	1	2	1	2	0	3	0	6	0	0

Упражнение 13.
Найти порядок элемента $a = \alpha\theta + \beta \in \mathbb{Z}_7[\theta]/(\theta^2 + 1),\ \alpha, \beta \in \mathbb{Z}_7$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
α	1	3	1	-2	-2	3	-3	-1	3	-1	1	1	2	2	2	-3
β	3	2	-3	3	1	-1	2	2	-2	3	-2	2	-3	1	-1	1

Пример 6.
$a = 2\theta + 3$. Пусть $ord(a) = N$. Так как $|GF^*(7^2)| = 48$, то $N \mid 48$, то есть $N \in \{2, 3, 4, 6, 8, 12, 16, 24, 48\}$.

1. Вычисляем $a^2 = 4\theta^2 + 6\theta + 9 = -3\theta^2 - \theta + 2 = 3 - \theta + 2 = \theta - 2$.
Так как $a^2 \neq e$, то $N \neq 2$.

2. Вычисляем $a^4 = (-\theta - 2)^2 = \theta^2 + 4\theta + 4 = -3\theta + 3 = 3(-\theta + 1)$.
Так как $a^4 \neq e,\ a^4 \neq a$, то $N \neq 3,\ N \neq 4$.

3. Вычисляем $a^8 = (-3\theta + 3)^2 = 2(\theta^2 - 2\theta + 2) = -2 - 4\theta + 2 = 3\theta$.
Так как $a^8 \neq a^2,\ a^8 \neq e$, то $N \neq 6,\ N \neq 8$.

4. Вычисляем $a^{16} = 2\theta^2 = -2$.
Так как $a^{16} \neq e,\ a^{16} \neq a^4$, то $N \neq 12,\ N \neq 16$.

5. Вычисляем $a^{32} = 4 = -3$.
0 Так как $a^{32} \neq a^8$, то $N \neq 24$.

Следовательно, $ord(a) = 48$, то есть a — примитивный элемент данного поля.

Упражнение 14.
Найти порядок элемента $a = \alpha\theta + \beta \in GF(5) = \mathbb{Z}_5[\theta]/(\theta^2+2),\ \alpha, \beta \in \mathbb{Z}_5$.

N	1	2	3	4	5	6	7	8
α	1	1	1	2	2	-1	-1	-2
β	2	-2	-1	1	-1	2	1	1

Упражнение 15.
Найти порядок элемента $a \in GF^*(2^6) = \mathbb{Z}_2[\theta]/(\theta^6+\theta+1)$, $a = \sum_{i=0}^{5} \alpha_i\theta^i$, если $R(a) = \sum_{i=0}^{5} \alpha_i \cdot 2^i,\ \alpha_i \in \{0,1\}$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
R	29	31	19	42	14	21	10	24	52	49	57	38	47	11	59

Пример 7.
Пусть $N(a) = 25 = 2^4 + 2^3 + 1$, то есть $a = \theta^4 + \theta^3 + 1,\ ord(a) = T$.
Так как $|GF^*(2^6)| = 63$, то $T \mid 63$ и, следовательно, $T \in \{3, 7, 9, 21, 63\}$.
1. Вычисляем $a^2 = (\theta^4+\theta^3+1)^2 = \theta^8+\theta^6+1 = \theta^2(\theta+1)+\theta+1+1 = \theta^3+\theta^2+\theta \neq e$.
2. Вычисляем $a^4 = (\theta^3+\theta^2+\theta)^2 = \theta^6+\theta^4+\theta^2 = \theta^4+\theta^2+\theta+1 \neq e$.
Так как $a^4 \neq a$, то $T \neq 3$.
3. Вычисляем $a^8 = (\theta^4+\theta^2+\theta+1)^2 = \theta^8+\theta^4+\theta^2+1 = \theta^3+\theta^2+\theta^4+\theta^2+1 = \theta^4+\theta^3+1$.
Так как $a^8 \equiv a$, то $ord(a) = 7$.

4. Реккурентные последовательности над конечным полем

Рекуррентная последовательность (РП) ранга n

$$\alpha = (a_1,\ a_2, \dots,\ a_n,\ a_{n+1}, \dots) \in F_q^{\infty}$$

задается характеристическим уравнением

$$\alpha_i + f(\alpha_{i-1},\ \alpha_{i-2}, \dots,\ \alpha_{i-n}) = 0, \qquad i = n+1,\ n+2, \dots, \tag{14}$$

где $f:\ F_q^n \to F_q$.

Набор $(\alpha_1,\ \alpha_2, \dots, \alpha_n)$ — начальный отрезок РП называется начальным заполнением.
Уравнение (14) эквивалентно уравнению

$$\alpha_i = g(\alpha_{i-1},\ \alpha_{i-2}, \dots,\ \alpha_{i-n}), \qquad i = n+1,\ n+2, \dots \tag{15}$$

Уравнение (15) определяет автономный автомат — регистр сдвига (РС) R_g с одной обратной связью. Функция $g(x_1, \dots,\ x_n)$ — это функция обратной связи. Схематично РС, соответствующий РП (15), имеет вид такой как показано на рис 1.

Регистр сдвига R_g аналитически задается системой уравнений:

$$R_g: \quad \begin{cases} y_1 = x_2, \\ y_2 = x_3, \\ \quad \vdots \\ y_n = g(x_1,\ \dots,\ x_n) \end{cases} \tag{16}$$

Система (16) определяет преобразование $\phi_g:\ F_q^n \to F_q^n$. Например, пусть $F = \mathbb{Z}_3,\ n = 2,\ g = x_1x_2 + 1$. Тогда преобразование ϕ_g будет иметь вид:

$$\begin{aligned} y_1 &= x_2, \\ y_2 &= x_1x_2 + 1 \end{aligned} \tag{17}$$

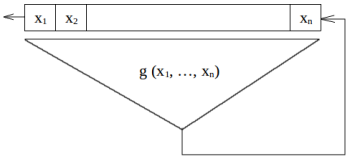

Рис. 1: Регистр сдвига с обратной связью

Характеристическое уравнение, соответствующей РП, примет вид:

$$\alpha_i = \alpha_{i-1}\alpha_{i-2} + 1, \qquad i = 3, 4, \dots,$$

(α_1, α_2) — начальное заполнение, $\alpha_1, \alpha_2 \in \mathbb{Z}_3$.
Начальное заполнение $(1, -1)$ порождает РП

$$\tilde{\alpha}_1 = (1, -1, 0, 1, 1, -1, 0, 1, \dots).$$

Начальное заполнение $(1, 0)$ порождает РП

$$\tilde{\alpha}_2 = (1, 0, 1, 1, -1, 0, 1, 0, \dots).$$

РП будет периодической тогда и только тогда, когда отображение ϕ_g — взаимнооднозначно, то есть ϕ_g — подстановка на множестве F_q^n. Соответствующий регистр сдвига называется регулярным.
Это условие будет выполняться тогда и только тогда, когда для любого набора $(\alpha_2, \dots, \alpha_n) \in F_q^{n-1}$ функция $g(x_1, \alpha_2, \dots, \alpha_n)$ — подстановка на множестве F_q. Если $F_q = GF(2)$, то функция $g(x_1, \dots, x_n)$ должна иметь вид:

$$g(x_1, \dots, x_n) = x_1 \oplus h(x_2, \dots, x_n).$$

Преобразование ϕ_g однозначно определяет ориентированный граф F_q. Например, для ϕ_g, заданного системой (17), это граф, изображенный на рис.2

Если R_g — регулярный, то соответствующая РП для любого начального состояния — периодическая. В этом случае цикловую структуру подстановки ϕ_g будем называть цикловой структурой соответствующей РП.
Если в уравнении (14) функция $f(x_1, \dots, x_n)$ — линейная, то характеристическое уравнение (14) примет вид:

$$\alpha_i + c_{n-1}\alpha_{i-1} + \dots + c_1\alpha_{i-n+1} + c_0\alpha_{i-n} = 0. \qquad (18)$$

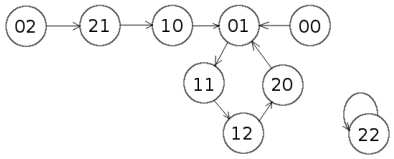

Рис. 2: Граф преобразования (17).

В этом случае РП называется линейной рекуррентной последовательностью (ЛРП).
Уравнение (18) однозначно задает многочлен

$$h(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \tag{19}$$

который называется характеристическим многочленом ЛРП. Если L — линейный оператор сдвига на F_q^∞, то есть $L(a_1,\ \ldots,\ a_n,\ a_{n+1}, \ldots) = (a_2, \ldots,\ \alpha_n,\ \alpha_{n+1},\ \ldots)$, то уравнение (19) эквивалентно уравнению

$$h(L)\tilde{\alpha} = \tilde{0}. \tag{20}$$

Множество всех ЛРП, удовлетворяющих уравнению (20), образует линейное подпространство $M(h)$ размерности n в F_q^∞.
Если $\tilde{\alpha} \in M(h)$, то многочлен минимальной степени g_α такой, что

$$g_\alpha(L)\tilde{\alpha} = \tilde{0},$$

называется минимальным (аннулирующим) многочленом ЛРП $\tilde{\alpha}$.
Напомним, что период ЛРП $\tilde{\alpha} \in M(h)$ — это минимальное $T = \text{per}\tilde{\alpha}$ такое, что $\alpha_{i+T} = \alpha_i,\ i = 1,\ 2, \ldots$.
Если $\tilde{\alpha_1} \in M(h_1),\ \tilde{\alpha_2} \in M(h_2),\ \text{НОД}(h_1,\ h_2) = 1$, то

$$\text{per}(\tilde{\alpha_1} + \tilde{\alpha_2}) = \text{НОК}(\text{per}\tilde{\alpha_1}, \text{per}\tilde{\alpha_2}).$$

Период многочлена $f(x)$ степени n над полем $GF(q)$ — это минимальное $T(f) \in \mathbb{N}$ такое, что

$$f(x) \mid x^{T(f)} - 1.$$

Например, если $f(x) = x^4 + x^3 + x^2 + x + 1$ и $F = GF(2)$, то $T(f) = 5$, так как $f(x) \mid x^5 + 1$.
Если $f(x) = x^2 - x - 1$ над полем $GF(3)$, то $T(f) = 8$. Это следует из того, что

$$f(x) \nmid x^4 - 1 = (x^2 - 1)(x^2 + 1),\ \text{то есть } T(f) \neq 4.$$

Следовательно, $T(f) = 8$, поскольку $T(f) \mid 8 = 3^2 - 1$.
Если $F = GF(2^n)$ и $2^n - 1$ — простое число (число Мерсенна), то любой неприводимый многочлен степени n над полем $GF(2)$ будет примитивным и, следовательно, иметь максимальный период $T = 2^n - 1$.
Если многочлен степени n неприводим над полем $GF(q)$, но не является примитивным, от его период $T(f)|q^n - 1$ и цикловая структура ЛРП, соответствующая этому многочлену, состоит из $\frac{q^n-1}{T(f)}$ циклов длины $T(f)$ и одного цикла длины 1.
Например, если $f(x) = x^4 + x^3 + x^2 + x + 1$ над полем $GF(2)$, то $T(f) = 5$ и соответствующая цикловая структура ЛРП состоит из 3 циклов длины 5 и одного цикла длины 1.
Если многочлен $f(x)$ степени n неприводим над полем $GF(q),\ r \in (p^k, p^{k+1}],\ k \geq 0$ и $\mathrm{per}(f) = T$, то цикловая структура ЛРП многочлена $F(x) = f^r(x)$ состоит из $N_1 = \frac{q^n-1}{T}$ циклов длины $T_1 = T$,
$N_{j+1} = \frac{q^{nq^j} - q^{np^{j-1}}}{p^j T}$ циклов длины $T_{j+1} = q^j T,\ j = \overline{1,\ k}$,
$N_{k+2} = \frac{q^{nr} - q^{np^k}}{q^{k+1}T}$ — циклов длины $T_{k+2} = q^{k+1}T$ и одного цикла длины 1.

Пример 4.1. Определить цикловую структуру ЛРП, заданной характеристическим многочленом $f(x) = (x^2 + x + 1)^3$ над полем $GF(2)$.
Решение. $T(f) = 3,\ r = 3 \in (2^1,\ 2^2]$, следовательно, $k = 2,\ n = 2,\ j = 1,\ 2$.
$N_1 = \frac{2^2-1}{3} = 1,\ T_1 = T = 3$.
$j = 1:\quad T_2 = p^1 T = 2 \cdot 3 = 6,\ N_2 = \frac{2^{2\cdot 2} - 2^1}{6} = \frac{12}{6} = 2$.
$T_3 = 2^2 \cdot 3 = 12,\ N_3 = \frac{2^{2\cdot 3} - 2^{2\cdot 3}}{12} = \frac{64-16}{12} = 4$.
Таким образом,

$$C(f) = (1,\ 3,\ 6,\ 6,\ 12,\ 12,\ 12,\ 12), \quad 1 + 3 + 2 \cdot 6 + 4 \cdot 12 = 64.$$

Пример 4.2. Определить цикловую структуру ЛРП, заданного характеристическим многочленом $f(x) = (x^2 + 1)^3$ над полем $GF(3)$.
Решение. $\mathrm{per}(x^2 + 1) = 4$, так как $x^2 + 1 | x^4 - 1$ и $x^2 + 1 \nmid (x^3 - 1)$.
$n = 2,\ r = 3 \in (3^0,\ 3^1]$, то есть $k = 0$. Следовательно,
$T_0 = 1,\ T_1 = 4,\ T_2 = 3 \cdot 4 = 12$.
$N_1 = \frac{3^2-1}{4} = 2,\ N_2 = \frac{3^{2\cdot 3} - 3^2}{12} = 6$.
Таким образом, $C(f)$ состоит из цикла длины 1, двух циклов длины 4 и 6-ти циклов длины 12, то есть $1 + 2 \cdot 4 + 6 \cdot 12 = 81$.

4.1. Упражнения

Упражнение 4.1. Проверить, что многочлен $f(x)$ является примитивным над полем $\mathbb{Z}_n$, выписать характеристические уравнение соответствующей ЛРП.

N	1	2	3	4
f	x^3+x+1	x^3+x^2+1	x^4+x+1	x^4+x^3+1
N	5	6	7	8
f	x^5+x^2+1	x^5+x^3+1	x^6+x+1	x^6+x^5+1

Упражнение 4.2. Определить период многочлена $f(x) = x^2 + a_1x + a_0$ над полем $GF(7)$.

N	1	2	3	4	5	6	7	8	9	10
a_1	1	-3	2	-2	-3	3	2	1	-1	-2
a_0	3	-1	2	3	-2	1	-2	-3	-1	-2
Ответы	48	16	24	48	48	8	24	48	16	24

Пример 4.3. $f(x) = x^2 - 2x + 2$.
Проверяем, что $f(x)$ не имеет корней в поле $GF(7)$ и, следовательно, является неприводимым.
Период T этого многочлена — делитель $q^2 - 1 = 7^2 - 1 = 48$. Напомним, что T — это минимальное натуральное число такое, что $f(x)|x^T - 1$ над полем $GF(q)$.
Для определения T последовательно вычислим

$$\begin{aligned}
x^2 &\equiv 2x - 2 \pmod{f(x)}\\
x^4 &\equiv 4(x^2 - 2x + 1) \equiv -3(2x - 2 - 2x + 1) \equiv 3 \pmod{f(x)}\\
x^8 &\equiv 2 \pmod{f(x)}\\
x^{12} &\equiv -6 \equiv -1 \pmod{f(x)}\\
x^{24} &\equiv 1 \pmod{f(x)}.
\end{aligned}$$

Таким образом, $T = 24$.

Упражнение 4.3. Найти максимальный период ЛРП над полем $GF(7)$, заданную характеристическим уравнением:

$$x_i + a_2x_{i-1} + a_1x_{i-2} + a_0x_{i-3} = 0.$$

Пример 4.4. Пусть ЛРП задана следующим характеристическим уравнением:

$$x_i - 3x_{i-2} + 3x_{i-3} = 0.$$

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_0	1	-2	-3	2	-1	-1	1	2	-1	1	-3	1	2	3	-3
a_1	1	-1	2	1	3	0	3	2	1	1	2	2	-3	2	-3
a_2	-1	3	-3	-3	0	-3	0	-1	-2	2	3	-3	-3	-3	0

1) Составляем соответствующий характеристический многочлен:
$$f(x) = x^3 - 3x + 3$$

2) Определяем его корень: $x = 3$.

3) Разлагаем на множители
$$f(x) = (x-3)(x^2 + 3x - 1).$$

4) Определяем период T_1 многочлена $f_1(x) = x - 3$ и период T_2 многочлена $f_2(x) = x^2 + 3x - 1$.
$T_1 = 6,$ так как $GF(7) =< 3 >$.
Цикловая структура ЛРП с характеристическим многочленом f_1 состоит из цикла длины 6 и цикла длины 1.
Для нахождения T_2 последовательно вычисляем:

$$x^2 \equiv 1 - 3x \pmod{f_2(x)}$$
$$x^4 \equiv (1-3x)^2 \equiv 1 + x + 2x^2 \equiv 1 + x + 2(1-3x) = 3 + 2x \pmod{f_2(x)}$$
$$x^8 \equiv 2 - 2x - 3x^2 \equiv 2 - 2x - 3(1-3x) = -1 \pmod{f_2(x)}$$
$$x^{16} \equiv 1 \pmod{f_2(x)}.$$

Таким образом, $T_2 = 16$ и цикловая структура ЛРП с характеристическим многочленом f_2 состоит из 3 циклов длины 16 и цикла длины 1.
Длина максимального цикла ЛРП равна НОК$(16,\ 6) = 48$.

Упражнение 4.4. Определить максимальный период ЛРП над полем $GF(3)$, заданной характеристическим уравнением:

1) $x_i + x_{i-1} + x_{i-2} + x_{i-5} = 0.$

2) $x_i + x_{i-1} - x_{i-2} + x_{i-4} - x_{i-5} = 0.$

3) $x_i - x_{i-1} + x_{i_3} - x_{i-4} - x_{i-5} = 0.$

4) $x_i - x_{i-3} - x_{i-4} - x_{i-5} = 0.$

Упражнение 4.5. Определить максимальный период ЛРП над полем $GF(5)$, заданной каноническим уравнением:

1) $x_i + 2x_{i-1} - x_{i-2} = 0.$

2) $x_i + 2x_{i-1} - 2x_{i-2} = 0.$

3) $x_i - x_{i-1} + 2x_{i-2} = 0.$

4) $x_i - 2x_{i-1} - x_{i-2} = 0.$

5) $x_i - 2x_{i-1} - 2x_{i-2} = 0.$

6) $x_i + x_{i-1} + 2x_{i-2} = 0.$

Упражнение 4.6. Определить максимальный период ЛРП над полем $GF(2)$, заданной характеристическим уравнением:

1) $x_i + x_{i-1} + x_{i-5} + x_{i-6} + x_{i-7} = 0.$

2) $x_i + x_{i-1} + x_{i-2} + x_{i-6} + x_{i-7} = 0.$

3) $x_i + x_{i-2} + x_{i-4} + x_{i-5} + x_{i-7} = 0.$

4) $x_i + x_{i-2} + x_{i-3} + x_{i-5} + x_{i-7} = 0.$

5) $x_i + x_{i-1} + x_{i-2} + x_{i-3} + x_{i-4} + x_{i-6} + x_{i-7} = 0.$

6) $x_i + x_{i-2} + x_{i-3} + x_{i-5} + x_{i-7} = 0.$

7) $x_i + x_{i-1} + x_{i-3} + x_{i-4} + x_{i-5} + x_{i-6} + x_{i-7} = 0.$

8) $x_i + x_{i-1} + x_{i-2} + x_{i-3} + x_{i-5} + x_{i-7} = 0.$

9) $x_i + x_{i-2} + x_{i-5} + x_{i-6} + x_{i-7} + x_{i-8} = 0.$

10) $x_i + x_{i-2} + x_{i-6} + x_{i-7} + x_{i-8} = 0.$

Упражнение 4.7. Определить цикловую структуру и характеристическое уравнение ЛРП над полем $GF(2)$, заданную характеристическим многочленом:

		Ответ:
1	$x^7+x^5+x^4+1$	1, 1, 2, 31, 31, 62
1	$x^7+x^3+x^2+1$	1, 1, 2, 31, 31, 62
3	$x^7+x^6+x^4+x^3+x^2+x+1$	1, 3, 31, 93
4	$x^8+x^5+x^4+x+1$	1, 7, 31, 217
5	$x^7+x^6+x^5+x^4+x^3+x+1$	1, 3, 31, 93
6	$x^8+x^6+x^3+x^2+x+1$	1, 1, 2, 63, 63, 126
7	$x^8+x^7+x^6+x^5+x^2+1$	1, 1, 2, 63, 63, 126
8	$x^8+x^6+x^2+x+1$	1, 7, 31, 217
9	$x^8+x^7+x^4+x^3+1$	1, 7, 31, 217
10	$x^6+x^4+x^3+x^2+x+1$	1, 1, 2, 15, 15, 30
11	$x^6+x^5+x^4+x^3+x^2+1$	1, 1, 2, 15, 15, 30
12	$x^7+x^5+x^3+x^2+1$	1, 7, 15, 105
13	$x^7+x^6+x^5+x+1$	1, 7, 15, 105
14	$x^7+x^5+x^4+x^2+1$	1, 7, 15, 105
15	$x^7+x^6+x^2+x+1$	1, 7, 15, 105
16	$x^8+x^7+x^6+x^2+1$	1, 7, 15, 105
17	$x^7+x^6+x^5+x^4+x^2+1$	1, 1, 2, 3, 3, 6, 7, 7, 14, 21, 21, 42
18	x^7+x^3+1	1, 127
19	x^7+x+1	1, 127
10	x^7+x^4+1	1, 127

Пример 4.5. Пусть $f(x)=x^{10}+x^9+x^7+x^6+x^4+x^2+1$.
Характеристическое уравнение: $x_i+x_{i-1}+x_{i-3}+x_{i-4}+x_{i-6}+x_{i-8}+x_{i-10}$.
Разлагаем $f(x)$ на множители. Для этого используем неприводимые многочлены степени 2, 3, 4, 5:

$$x^2+x+1,\qquad x^3+x+1,\qquad x^3+x^2+1,\qquad x^4+x+1,\qquad x^4+x^3+x^2+x+1,$$

$$x^5+x^4+x^2+x+1,\qquad x^5+x^2+1,\qquad x^5+x^3+1.$$

Убеждаемся, что

$$f(x)=(\underbrace{x^2+x+1}_{f_1})(\underbrace{x^3+x+1}_{f_2})(\underbrace{x^5+x^2+1}_{f_3})$$

$$T_1=3,\quad T_2=7,\quad T_3=31.$$

Максимальный период $T_{max}=3\cdot 7\cdot 31=651$.
Искомая цикловая структура: {651, 217, 93, 31, 21, 7, 3, 1}
Сумма длин циклов равна $2^{10}=1024$.

Упражнение 4.8. Над полем $F = GF(q)$ определить цикловую структуру ЛРП, заданной многочленом $f(x)$.

I. $F = GF(2)$.

N	$f(x)$
1	$(x^2+x+1)^4$
2	$(x^3+x+1)^3$
3	$(x^4+x+1)^2$
4	$(x^5+x^2+1)^2$
5	$(x^3+x^2+1)^3$
6	$(x^2+x+1)^5$
7	$(x^5+x^3+1)^3$
8	$(x^4+x^3+1)^3$
9	$(x^2+x+1)^5$
10	$(x^3+x+1)^4$
11	$(x^2+x+1)^2(x^3+x+1)$
12	$(x^2+x+1)^3(x^3+x+1)$
13	$(x^3+x+1)^2(x^2+x+1)$
14	$(x^3+x^2+1)^2(x^2+x+1)$
15	$(x^2+x+1)^2(x^3+x^2+1)$
16	$(x^2+x+1)^2(x^4+x+1)$
17	$(x^2+x+1)^2(x^4+x^3+1)$
18	$(x^2+x+1)^2(x^4+x^3+x^2+x+1)$
19	$(x^2+x+1)^2(x^5+x^2+1)$
20	$(x^2+x+1)^2(x^3+x^2+1)$

II. $F = GF(p)$

N	$f(x)$	p
1	$(x^2+1)^4$	3
1	$(x^2+x+2)^3$	3
3	$(x^4+x+1)^2$	3
4	$(x^5+2x^4+1)^3$	3
5	$(x^2+x+3)^2$	7
6	$(x^2+x+3)^3$	7
7	$(x^3-2x+2)^3$	5
8	$(x^3-2x^2+2)^3$	5
9	$(x^3+2x+1)^2$	7
10	$(x^4+x^2+2x+2)^2$	5

Упражнение 4.9. Над полем $GF(2)$ построить ЛРП периода T и ранга n и указать начальное заполнение.

N	1	2	3	4	5	6	7	8
T	42	210	93	126	60	124	252	155
n	7	9	7	8	7	8	9	9
N	9	10	11	12	13	14	15	
T	28	217	35	84	315	310	140	
n	6	8	7	8	10	11	10	

Пример 4.6. $T = 140,\ n = 10.$
Раскладываем 140 на множители: $140 = 4 \cdot 7 \cdot 5.$
ЛРП$_1$ с периодом 4 соответствует минимальный многочлен

$$f_1(x) = x^3 + x^2 + x + 1.$$

ЛРП$_2$ с периодом 5 соответствует минимальный многочлен

$$f_2(x) = x^4 + x^3 + x^2 + x + 1.$$

ЛРП$_3$ с периодом 7 соответствует, например, минимальный многочлен

$$f_3(x) = x^3 + x + 1.$$

Искомый характеристический многочлен

$$f(x) = (x^3+x^2+x+1)(x^4+x^3+x^2+x+1)(x^3+x+1) = x^{10}+x^7+x^4+x^3+x^2+x+1.$$

Характеристическое уравнение будет иметь вид:

$$x_i = x_{i-3} + x_{i-6} + x_{i-7} + x_{i-8} + x_{i-9} + x_{i-10}.$$

Начальное заполнение формируется следующим образом. Для каждой ЛРП выбирается начальное заполнение $\widetilde{\alpha}_i$ $(i = \overline{1,3})$ отличное от нулевого. Для каждой ЛРП вычисляется начальный отрезок ЛРП $\widetilde{\beta}_i,\ (i = \overline{1,3})$ длины 10. Начальное заполнение $\widetilde{\beta} = \widetilde{\beta}_1 \oplus \widetilde{\beta}_2 \oplus \widetilde{\beta}_3$.
Характеристические уравнения этих ЛРП будут следующими:

$$x_i = x_{i-1} + x_{i-2} + x_{i-3},\ \ \widetilde{\alpha}_1 = 001$$
$$x_i = x_{i-1} + x_{i-2} + x_{i-3} + x_{i-4},\ \ \widetilde{\alpha}_2 = 0001$$
$$x_i = x_{i-2} + x_{i-3}.\ \ \widetilde{\alpha}_3 = 001$$

Вычисляем 10 разрядов каждой ЛРП:

$$\widetilde{\beta}_1 = 0011001100$$
$$\widetilde{\beta}_2 = 0001100011$$
$$\widetilde{\beta}_3 = 0010111001$$
$$\widetilde{\beta} = \widetilde{\beta}_1 \oplus \widetilde{\beta}_2 \oplus \widetilde{\beta}_3 = 0000010110.$$

$\widetilde{\beta} = 0000010110$ — искомое начальное заполнение.

5. Теория групп

Если Ω — конечное множество, то S^Ω — это множество всех взаимнооднозначных отображений $\Omega \longleftrightarrow \Omega$. В частности, если $\Omega = \{1, 2, \ldots, n\}$, то $S^\Omega = S_n$ — симметричная группа степени n.

Любая $g \in S^\Omega$ представляется в виде произведения независимых циклов.

Порядок подстановки $g \in S^\Omega$ равен наименьшему общему кратному длин циклов g.

Если $G < S^\Omega$ и $\alpha \in \Omega$, то множество $\alpha^G = \{\beta \in \Omega \mid \exists g \in G : \alpha^g = \beta\}$ называется орбитой группы G.

Стабилизатор $G_\alpha,\ \alpha \in G$ группы G, это множество $\{g \in G \mid \alpha^g = \alpha\}$, при этом $|\alpha^G| = [G : G_\alpha]$

Группа $G < S^\Omega$ называется транзитивной на Ω, если для $\forall \alpha, \beta \in \Omega\ \exists g \in G$ такой, что $\alpha^g = \beta$.

Группа $G < S^\Omega$ называется k-транзитивной на Ω, если для $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_k)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_k),\ \alpha_i, \beta_i \in \Omega$, существует $g \in G$, такой, что $\alpha_i^g = \beta_i,\ i = \overline{1,k}$

Множество $\triangle \subset\ \Omega$ называется блоком группы G, если $\forall g \in G$ либо $\triangle^g = \triangle$ либо $\triangle^g \cap \triangle = \oslash$

Тривиальные блоки это $\forall \alpha \in \Omega$ и Ω. Группа G называется примитивной, если все блоки её тривиальные.

Если группа G циклическая и $|G| = n$, то для любого $k|n$ в G существует единственная циклическая подгруппа порядка k.

Если G абелева группа и $|G| = p_1^{k_1}, \ldots, p_t^{k_t}$, то группа G разлагается в прямое произведение своих силовских подгрупп, т.е. $G = S(p_1) \times S(p_2) \times \ldots \times S(p_t)$.

Любая примарная абелева группа $H,\ |H| = p^n$, разлагается в прямое произведение своих циклических подгрупп.

Автоморфизм группы G это $\varphi \in S^G$ такой, что $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$ для любых $a, b \in G$.

Группа простая, если она не содержит собственных нормальных делителей.

Теорема 1 (Первая теорема Силова). *Пусть* $|G| = p^m s,\ (s, p) = 1,\ p \in \mathbb{P}$. *Тогда для любого* $i = \overline{1,m}$ *в* G *существует подгруппа*

порядка p^i, причём если $i < m$, то каждая такая подгруппа инвариантна в некоторой подгруппе порядка p^{i+1}.

Теорема 2 (Вторая теорема Силова). *Все силовские p-подгруппы конечной группы сопряжены.*

Теорема 3 (Третья теорема Силова). *Число силовских p-подгрупп конечной группы делит порядок группы и сравнимо с единицей по модулю p.*

5.1. Упражнения и задачи

5.1. Найти порядок подстановки $g = ax + b \in S^{Z_q}$.

№	1	2	3	4	5	6	7	8	9	10
q	3	7	11	13	11	7	13	11	7	13
a	3	1	3	5	5	2	4	4	3	2
b	2	2	5	1	3	1	7	6	2	6

5.2. Найти порядок подстановки $g = ax^k + b \in S^{Z_q}$.

№	1	2	3	4	5	6	7	8	9	10
q	7	11	13	7	11	13	7	11	13	7
a	2	2	2	3	5	1	4	4	3	1
b	3	5	1	2	2	2	1	3	1	4
k	5	3	5	5	3	5	5	3	5	5

5.3. Найти порядок подстановки $g = ax + b \in S^{GF(3^2)}$
$GF(3^2) = Z_2[\theta]/(\theta^2 + 1)$.

№	1	2	3	4	5	6	7	8	9	10
a	-1	θ	1	$\theta+1$	1	-1	θ	$\theta+1$	θ	$-\theta$
b	θ	1	θ	1	$\theta+1$	θ	-1	θ	$\theta+1$	1

5.4. Найти порядок подстановки $g = ax^2 + b \in S^{GF(2^3)}$
$GF(2^3) = Z_2[\theta]/(\theta^3 + \theta + 1)$.

№	1	2	3	4	5	6	7	8	9	10
a	θ	$\theta+1$	θ^2	$\theta^2+\theta$	1	θ^2+1	$\theta+1$	θ	1	$\theta^2+\theta$
b	θ^2+1	θ	1	θ	$\theta^2+\theta$	θ	θ^2	$\theta+1$	$\theta^2+\theta$	1

5.5. Подсчитать число элементов порядка $k = 2, 3, 4$ в группе S_4.

5.6. Доказать, что $K_4 = \{e, (12)(34), (13)(24), (14)(23)\} \lhd A_4$.

5.7. Подсчитать число элементов порядка k групп A_n и S_n для

5.7.1. $n = 5$,

5.7.2. $n = 6$.

5.8. Найти силовские подгруппы групп A_4 и S_4.

5.9. Определить число и строение 2-силовских подгрупп групп A_5 и S_5.

5.10. Определить строение и число 2-силовских подгрупп группы A_6.

5.11. Определить строение и число 2-силовских подгрупп группы S_6.

5.12. Пусть $g_1 = (12354), g_2 = (12453)$. Найти $h \in S_5$, такой, чтобы $g_2 = h^{-1} g_1 h$.

5.13. Показать, что $\langle(12\alpha\beta\gamma)\rangle \neq \langle(12\alpha'\beta'\gamma')\rangle$, если $(\alpha\beta\gamma) \neq (\alpha'\beta'\gamma')$.

5.14. Пусть K — группа кватернионов $k = \{\pm 1, \pm i, \pm j, \pm k\}$, где $i^2 = j^2 = k^2 = 1$, $ij = -ji = -k$, $ik = ki = -j$, $jk = kj = -i$, $H_1 = \langle -1, 1\rangle$, $H_2 = \langle 1, i\rangle$.

5.14.1. Найти все подгруппы группы K.

5.14.2. Разложить K по подгруппе H_1.

5.14.3. Убедиться, что H_1 — нормальная подгруппа и описать её структуру.

5.14.4. Разложить группу K по подгруппе H_2.

5.14.5. Найти все классы сопряжённых элементов группы K.

5.15. Доказать $S_4/K_4 \simeq S_3$, где $K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$

5.16. Найти орбиты групп $G_1 = \langle(123)(456), (1346)\rangle$, $G_2 = \langle(1234)(56), (123)\rangle$, $G_3 = \langle(134)(56), (123)(567)\rangle$,

5.17. Доказать, что $G_2 \simeq S_4$.

5.18. Доказать, что $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$, $\mathrm{ord}(ab) = \mathrm{ord}(ba)$, $\mathrm{ord}(abc) = \mathrm{ord}(cab)$.

5.19. Подсчитать число элементов порядка q в группе G, если $|G| = p^2 q,\ q > p$, p и q — простые.

5.20. Подсчитать число элементов порядка p и q в группе G, если $|G| = pq,\ q > p,\ p \nmid q - 1,\ p$ и q — простые.

5.21. Пусть $|G| = pq,\ q > p,\ p$ и q — простые. Доказать, что $\exists! H \lhd G,\ |H| = q$.

5.22. Доказать, что если $G = \langle a, b\rangle,\ a^2 = e,\ b^4 = e,\ ba = ab^{-1} = ab^3$, то $G = \langle a^i b^j |\ i = \overline{0,1},\ j = \overline{0,3}\rangle$.

5.23. Найти все примитивные и импримитивные подгруппы группы S_4.

5.24. Подсчитать число элементов порядка 7 в группе $G,\ |G| = 168$, если известно, что G–простая.

5.25. Пусть $N = N_G(G_\alpha)$ и $\Psi = \{\beta \in G_\alpha | \beta^{G_\alpha} = \beta\}$. Доказать, что N транзитивна на Ψ.

5.26. Доказать, что если $G = \langle (12...k)\rangle, n = kt$, то $\Delta_i = \{i, i+k, \ldots, i+k\cdot(t-1)\},\ i = 1, t$ — блоки группы G.

5.27. Доказать, что если G — регулярна на Ω, а $|\Omega|$ - составное число, что G - импримитивная подгруппа.

5.28. Доказать, что пересечение блоков группы G является блоками.

5.29. Доказать, что если Δ - блок подгруппы $H < G$, то Δ^g - блок группы $g^{-1}Hg, g \in G$.

5.30. Доказать, что если группа дважды транзитивная, то она примитивная.

5.31. Доказать, что транзитивная группа простой степени примитивная.

5.32. Пусть $G = \langle a\rangle,\ |G| = n,\ gcd(k, n) = 1$. Доказать, что $g = x^k \in S^G$.

5.33. Если $k|q-2$, то $g = ax^k + b,\quad a \neq 0,\ a, b \in GF(q)$, то $g \in S^{GF(q)}$.

5.34. Доказать, что $G = \langle ax + b | a \in F_q^k, b \in F_q\rangle$ — дважды транзитивная.

5.35. Пусть $G \neq \langle e\rangle$. Доказать, что если G примитивна на Ω, то G — транзитивна на Ω.

5.36. Доказать, что если G примитивна на Ω; $N \triangleleft G, N \neq \langle e\rangle$, то N — транзитивна на Ω.

5.37. Доказать, что если степень примитивностй группы четная и больше 2, то порядок группы делится на 4.

5.38. Доказать, что если $\alpha = \beta^g$, то G_α и G_β сопряжены.

5.39. Доказать, что если G - транзитивна на Ω, и P — силовская подгруппа группы G_α, то $N_G(P)$ - транзитивен на множестве

$$\Phi = \{\beta \in \Omega : \beta^g = \beta, g \in G_\alpha\}.$$

5.40. Доказать, что

5.40.1. $S_n = \langle (i\ i+1) :\ i = 0, n-2\rangle,\ n \geqslant 2$

5.40.2. $S_n = \langle (0\ n-1) : (k\ k+1)\rangle,\ n \geqslant 2,\ k = 0, 1, ..., n-2$

5.40.3. $A_n = \langle (i\ j\ k) :\ 1 \leqslant i < j < k \leqslant n\rangle$

5.40.4. $A_n = \langle (0\ 1\ i) : i = 2, ..., n-1\rangle, n \geqslant 3$

5.40.5. $A_n = \langle (i\ i+1\ i+2) : i = 0, ..., n-1\rangle$

43. Доказать, что если $G < S_n$ и G — транзитивна, то существует $g \in G$ такой, что $Fix(g) = \varnothing$, $Fix(g) = \{\alpha \in \Omega : \alpha^g = \alpha\}$.

44. Доказать, что если n - составное число, то любая силовская p - подгруппа S_n не является транзитивной.

45. Пусть $G < S_n,\ p$ — простое и $|G| \vdots p$. Доказать, что существует $g \in G$, такой, что в его циклическом представлении содержится цикл длины p.

46. Пусть G — нециклическая группа порядка p^2, p — простое. Доказать, что $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

47. Пусть G — группа порядка n, $g \in G, \mathrm{ord}(g) = m,\ C(g) = \{x^{-1}gx | x \in G\},\ |C(g)| = k$. Доказать, что $k | \frac{n}{m}$

48. Пусть G — группа порядка p^n, p — простое, $A \lhd G,\ |A| = p$. Доказать, что $A < Z(G)$.

49. Пусть $H \lhd G,$ НОД$([G : H], p) = 1$. Доказать, что любая силовская p-подгруппа группы G содержится в H.

50. Описать все неабелевы группы порядка 8.

51. Доказать, что две подстановки сопряжены тогда и только тогда, когда у них одинаковая цикловая структура.

52. Доказать, что группа автоморфизмов циклической группы G порядка n имеет порядок $\varphi(n)$ и $Aut(G) = \{x^k | k \in \mathbb{Z}_n,$ НОД$(k, n) = 1\}$.

53. Доказать, что группа $\mathbb{Z}^*_{2^n}$ при $n \geqslant 3$ не является циклической

54. Доказать, что группа невырожденных матриц размера n над полем $GF(q) = F_q$ транзитивна на множестве $F_q^n \setminus \{0\}^n$, но не дважды транзитивна.

55. Пусть $G = \langle (12...n) \rangle$, n — составное. Доказать, что G — импримитивна и найти все её блоки.

56а.

1. Проверить, что g — примитивный элемент группы $\mathbb{Z}^*_p$.

2. Найти образующий элемент h группы $\mathbb{Z}^*_{p^2}$ и подсчитать числе элементов различных порядков этой группы.

3. Найти элемент порядка m группы $\mathbb{Z}^*_{p^2}$

№	1	2	3	4	5	6	7	8	9	10	11	12
p	11	13	17	19	17	13	23	11	13	29	23	19
g	2	2	3	-4	-3	-2	-3	-4	-3	2	-2	2
m	22	26	34	57	17	39	46	11	13	116	46	38

56. Определить строение группы $\mathbb{Z}^*_n$.

№	1	2	3	4	5	6	7	8	9
n	63	100	189	280	117	144	677	88	188

57. Определить структуру группы $\mathbb{Z}^*_n$, разложить её в прямое

произведение циклических подгрупп и подсчитать число элементов различного порядка.

№	1	2	3	4	5	6	7	8	9	10	11	12
n	750	675	1323	1539	945	616	1404	1100	1225	980	2975	84

58. Описать строение группы $Aut(\mathbb{Z}_{13})$.

5.2. Указания и решения

7.1. Пусть $N(k)$ число элементов порядка k группы $S_5(A_5)$

а) $N(2) = \binom{5}{2} + \binom{5}{2}\binom{3}{2} = 10 + 15 = 25$. $N(2)$ — число элементов вида $(\alpha\beta)$ и $(\alpha\beta)(\gamma\delta)$.

б) $N(3) = \binom{5}{3} \cdot 2 = 20$ (число 3-циклов группы S_5).

в) $N(4) = \binom{5}{4} \cdot 3! = 30$ (число циклов длины 4 в S_5).

г) $N(5) = 4! = 24$ (число циклов длины 5 в S_5).

д) $N(6) = \binom{5}{2} \cdot 2 = 20$ (число элементов вида $(\alpha\beta)(\delta\gamma\varepsilon)$).

$\sum_1^6 N(k) = 1 + 25 + 20 + 30 + 24 + 20 = 120 = |S_5|$.

Для группы A_5: $N(2) = \binom{5}{2}\binom{3}{2},\ N(3) = 20,\ N(5) = 24,\ N(1) = 1$.

$N(1) + N(2) + N(3) + N(5) = 60 = |A_5|$.

7.2. Элементы порядка 2 группы S_6 имеют вид:

$(\alpha\beta),\ (\alpha\beta)(\gamma\delta),\ (\alpha\beta)(\gamma\delta)(\varepsilon\nu) = \{(1\alpha)(\beta\gamma)(\varepsilon\delta),\ \beta < \gamma,\ \varepsilon < \delta\}$, поэтому $N(2) = \binom{5}{2} + \binom{6}{2}\binom{4}{2}/2 + 5 \cdot 3 = 75$.

$N(3) = \binom{6}{3} \cdot 2 + \binom{6}{3} \cdot 2 = 80$, т.к. элементы порядка 3 имеют вид: $(\alpha\beta\gamma),\ (\alpha\beta\gamma)(\varepsilon\nu\delta)$.

$N(4) = [\binom{6}{4} \cdot 3!] \cdot 2 = 180$, т.к. элементы порядка 4 имеют вид: $(\alpha\beta\gamma\delta)$, $(\alpha\beta\gamma\delta)(\varepsilon\nu)$.

$N(5) = \binom{6}{5} \cdot 4! = 144$.

$N(6) = 5! + \binom{6}{2}\binom{4}{3} \cdot 2! = 240$, т.к. элементы порядка 6 имеют вид: $(\alpha\beta\gamma\delta\varepsilon\nu),\ (\alpha\beta\gamma)(\delta\varepsilon)$.

Для группы A_6.

$N_2 = 45 = \binom{6}{2}\binom{4}{2}/2$, $N_3 = 80$, $N_4 = 90$, $N_5 = 144$.

8. Группа A_4 содержит единственную силовскую 2-подгруппу порядка 4 — группу Клейна.

$$K_4 = \{e, (12)(34), (13)(24), (14)(23)\} = K_4(1, 2, 3, 4).$$

Группа S_4 содержит силовскую 2-подгруппу порядка 8. Такая группа должна содержать все элементы четвертого порядка. Следовательно, относительно группы Клейна это силовская группа $\mathcal{P}$ будет иметь разложение вида:

$\mathcal{P}(\alpha, \beta, \gamma, \delta) = (\alpha\beta\gamma\delta)K_4(1, 2, 3, 4) + K_4(1, 2, 3, 4),$ где $(\alpha\beta\gamma\delta) \in \{(1234), (1324), (1423)\}$

Число таких подгрупп равно $3!/2 = 3$.

Силовские 3-подгруппы группы A_4 и S_4 это суть следующая подгруппа: $\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle$.

9. Силовская 2-группа A_5 имеет порядок 4, должна содержать подгруппу изоморфную группе Клейна и, следовательно, будет следующей: $\mathcal{P}(\alpha\beta\gamma\delta) = K_4(\alpha, \beta, \gamma, \delta),\ \{\alpha, \beta, \gamma, \delta\} \subset \{1, 2, 3, 4, 5\}$. Число таких групп равно 5.

Силовская 2-группа группы S_5 имеет порядок 8, должна содержать подстановку порядка 4 (4-цикл) и подгруппу изоморфную K_4. Поэтому эта группа будет иметь следующее разложение на смежные классы

$$\mathcal{P}_8(\alpha, \beta, \gamma, \delta) = (\alpha\beta\gamma\delta)K_4(\alpha, \beta, \gamma, \delta) + K_4(\alpha, \beta, \gamma, \delta).$$

Пример. $\mathcal{P}_8(1, 3, 4, 5) = (1345)\{e, (13)(45), (14)(35), (15)(34)\} + \{e, (13)(45), (14)(35), (15)(34)\} = \{(1345), (35), (1543), (14), (13)(45), (14)(35), (15)(34), e\}$

Число таких групп равно $\binom{5}{4} \cdot 3! = 15$, так как каждая такая группа содержит ровно 2 элемента порядка 4. Число силовских 3-групп равно половине числа 3-циклов, т.е. 10(см. упражнение 5.7.2). Число силовских 5-групп равно $24/4 = 6$ (см. упражнение 5.7.2)

10. Каждая силовская 2-группа группы A_6 имеет порядок 8 и содержит соответствующую подгруппу $K_4(\alpha\beta\gamma\delta) \cong K_4$ При этом каждой силовская 2-группа группы A_6 должны содержать элементы порядка 4. Такие элементы имеют следующую цикловую структуру:

$$(\alpha\beta\gamma\delta)(\varepsilon\nu)$$

Заметим, что число таких элементов (см. упражнение 5.7.2) равно 90. Следовательно, силовская 2-группа $\mathcal{P}$ группы A_6 будет иметь следующее разложение относительно группы $K_4(\alpha, \beta, \gamma, \delta)$:

$$\mathcal{P}_8((\alpha, \beta, \gamma, \delta)(\varepsilon, \nu)) = (\nu\varepsilon)(\alpha\beta\gamma\delta)K_4(\alpha, \beta, \gamma, \delta) + K_4(\alpha, \beta, \gamma, \delta)$$

Например, $\mathcal{P}_8((1, 2, 4, 6)(3, 5)) = (1246)(35)K_4(1, 2, 4, 6) + K_4(1, 2, 4, 6) = (35)(1246)[e, (12)(46), (14)(26), (16)(24)] + [e, (12)(46), (14)(26), (16)(24)] = \{(35)(26), (35)(1642), (1246)(35), (35)(14), (12)(46), (14)(26), (16)(24), e\}$

Каждая такая группа содержит ровно 2 элемента порядка 4. Поэтому число таких групп равно 45.

11. Каждая силовская 2-группа $\mathcal{P}_{16}((\alpha, \beta, \gamma, \delta)(\nu, \varepsilon))$ группы S_6 должна содержать нечетную подстановку $(\alpha\beta\gamma\delta)$ порядка 4 и соответствующую силовскую 2-группу $\mathcal{P}_8$ группы A_6. Следовательно, $\mathcal{P}_{16}(\alpha, \beta, \gamma, \delta)$ будет иметь следующее разложение относительно группы $\mathcal{P}_8((\alpha, \beta, \gamma, \delta)(\nu, \varepsilon))$:

$$\mathcal{P}_{16}((\alpha, \beta, \gamma, \delta)(\nu, \varepsilon)) = (\alpha\beta\gamma\delta)\mathcal{P}_8((\alpha, \beta, \gamma, \delta)(\nu, \varepsilon)) + \mathcal{P}_8((\alpha, \beta, \gamma, \delta)(\nu, \varepsilon))$$

Каждая группа $\mathcal{P}_{16}(\alpha,\beta,\gamma,\delta)$ — содержит 4 элемента порядка 4 поэтому число таких групп равно $180/4 = 45$ (см.задачу 5.7.2)

19. По третьей теореме Силова T-число силовских q-подгрупп является делителем $|G| = p \cdot q$ и $T \equiv 1 \pmod q$. Из всех делителей $1, p, pq, q^2, q, p^2q$ только 1 удовлетворяет этому условию (при $p < q$). Следовательно, число элементов порядка q равно $q - 1$.

20. Как и в задаче 19 применить 3-ю теорему Силова.

21. Показать, что силовская группа порядка q в группе G — единственная, а значит нормальная.

22. Убедиться, что $b^i a = ab^k$, $i = 1, 2, 3$.

24. Воспользоваться третьей теоремой Силова.

56a. Образующий элемент группы $\mathbb{Z}^*_{p^n}$, $n \geqslant 2$ имеет вид $h = g + t_0 p$, где $t_0 \neq g \cdot v \pmod p$, $v = \frac{g^{p-1}-1}{p}$

Для вычисления v используем соотношение

$$v = \frac{(g^{\frac{p-1}{2}}+1)(g^{\frac{p-1}{2}}-1)}{p}, \quad p \nmid g^{\frac{p-1}{2}} - 1, \quad p \mid g^{\frac{p-1}{2}} + 1,$$

т.е.

$$v \equiv (\frac{g^{\frac{p-1}{2}}+1}{p}) \pmod p \cdot (g^{\frac{p-1}{2}} - 1) \pmod p$$

Пример. $p = 7,\ g = 3$. Очевидно, что g — примитивный элемент $\mathbb{Z}^*_7$. Вычисляем v:

$$v \equiv (\frac{3^3+1}{7}) \pmod 7 \cdot (3^3 - 1) \pmod 7 \equiv (4 \cdot 5) \pmod 7 \equiv -1$$

Следовательно, $t \neq -3$. Например, положим $t = 1$ и $h = 3 + 7 = 10$

Подсчитаем число элементов различных порядков. Порядок группы $\mathbb{Z}^*_{7^2} = 6 \cdot 7 = 42$. Возможные порядки элементов это делители числа $42 : 1, 2, 3, 6, 7, 14, 21, 42$. Если N_k — число элементов порядка k, то $N_1 = 1,\ N_2 = \varphi(2) = 1,\ N_3 = \varphi(3) = 2,\ N_6 = \varphi(6) = 2,\ N_7 = N_{14} = \varphi(7) = \varphi(14) = 6,\ N_{21} = N_{42} = \varphi(21) = \varphi(42) = 12.$

$$\sum N_k = 1 + 1 + 2 + 2 + 6 + 6 + 12 + 12 = 42 = |\mathbb{Z}^*_{7^2}|$$

Элемент порядка m в циклической группе порядка $N = m \cdot k$ имеет вид h^k, где h — образующий элемент.

В нашем примере элемент порядка 6 группы $\mathbb{Z}^*_{49}$ есть $h^7 \equiv 10^7 \pmod{49} = (10^2)^3 \cdot 10 \equiv 8 \cdot 10 \equiv 31 \equiv -18 \pmod{49}$

56. Пример при $n = 57$.

1. Определим порядок группы $\mathbb{Z}^*_n$.

$$|\mathbb{Z}^*_{57}| = \varphi(3)\varphi(19) = 2 \cdot 18 = 36 = 2^2 \cdot 3^2.$$

2. По теореме о разложении абелевой группы в прямое произведение своих силовских подгрупп имеем

$$\mathbb{Z}^*_{57} = S_1(2) \times S_2(3),\ |S_1(2)| = 4,\ |S_2(3)| = 9.$$

3. Определим число элементов группы $\mathbb{Z}_{57}^*$ порядка 2. Для этого решаем сравнение

$$x^2 \equiv 1 \pmod{57}$$

Число решений по Китайской теореме об остатках равно 20, следовательно

$$S_1(2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

4. Определим число элементов порядка 3. Для этого решаем сравнение

$$x^3 \equiv 1 \pmod{57}$$

это сравнение равносильно системе

$$\begin{cases} x^3 \equiv 1 \pmod{3} \\ x^3 \equiv 1 \pmod{19} \end{cases}$$

Первое сравнение имеет единственное решение $x = 1$. Второе сравнение имеет 3 решения $x_1 = 1, x_2 = 7, x_3 = 11$. Следовательно, группа $S_2(3)$ содержит 2 элемента 3 порядка. Это означает, что группа $S_2(3)$ — циклическая.

Таким образом, $\mathbb{Z}_{57}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$.

57. Пример 1. Найдём все разложения примарной группы $\mathbb{Z}_{16}^*$ в произведение циклических подгрупп.

Решение.

$\mathbb{Z}_{16}^* = \{\pm 1, \pm 3, \pm 5, \pm 7\}$ Находим собственные максимальные подгруппы:

$\langle 3 \rangle = A_1 = \{1, 3, -7, -5\},\ A_2 = \{1, 5, -7, -3\} = \langle -3 \rangle$.

Так как $\mathrm{ord}(7) = \mathrm{ord}(-1) = 2$, то других подгрупп порядка 4 нет и $B_1 = \langle 7 \rangle, B_2 = \langle -1 \rangle$ — подгруппы второго порядка, отличные от группы $\langle 7 \rangle = A_1 \cap B_1$. Отсюда, согласно теореме об абелевой группе, имеем:

$\mathbb{Z}_{16}^* = A_1B_1 = A_1B_2 = A_2B_1 = A_2B_2 = \langle 3 \rangle\langle 7 \rangle = \langle 3 \rangle\langle -1 \rangle = \langle -3 \rangle\langle -1 \rangle = \langle -3 \rangle\langle -7 \rangle$.

Пример 2. Для $n = 567$.

Решение.

1. Находим $|G| = \varphi(567) = \varphi(81) \cdot \varphi(7) = 54 \cdot 6 = 324 = 2^2 \cdot 3^4$. Следовательно, $G \cong S_1(4) \times S_2(3^4)$.

2. Определим структуру примарной группы $S_1(4)$. Для этого нужно определить число элементов второго порядка в группе G, т.е. определить число решений сравнения

$$x^2 \equiv 1 \pmod{567}. \tag{21}$$

Это сравнение по К.Т.О. равносильно системе

$$\begin{cases} x^2 \equiv 1 \pmod{81} \\ x^2 \equiv 1 \pmod{7} \end{cases} \tag{22}$$

Очевидно, что число решений (22) равно 4. Для первого и второго сравнений (22) решениями будут $x = \pm 1$, т.е. $S_1(4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Найдём решения (21) по К.Т.О.:

$$x = \pm 1 \cdot 81 \cdot (81^{-1} \pmod 7) \pm 1 \cdot 7 \cdot (7^{-1} \pmod{81}) \pmod{587}.$$

Т.к. $81^{-1} \pmod 7 = 4^{-1} \pmod 7 = 2, \quad 7^{-1} \pmod{81} = -23$, то

$$x = \pm 162 \pm 161 \pmod{587}.$$

Таким образом элементы второго порядка группы G это:

$$a_1 = -1, \ a_2 = 264, \ a_3 = -264.$$

Итого получаем:

$$S_1(4) = \langle -1 \rangle \cdot \langle 264 \rangle = \langle -1 \rangle \cdot \langle 264 \rangle = \langle -1 \rangle \cdot \langle -264 \rangle. \tag{23}$$

3. Определим структуру группы $S_2(3^4)$. Для этого определим число элементов группы G порядка 3, т.е. найдём решение сравнения

$$x^3 \equiv 1 \pmod{567} \tag{24}$$

Это сравнение эквивалентно системе

$$x^3 \equiv 1 \pmod 7 \tag{25}$$

$$x^3 \equiv 1 \pmod{81} \tag{26}$$

Сравнение (25) имеет 3 решения $x_1 \in \{1, 2, 4\}$. Сравнение (26) имеет 3 решения, т.к. группа $\mathbb{Z}^*_{81}$ является циклической порядка 54. Следовательно, число элементов порядка 3 группы G равно 8. Таким образом, $S_2(3^4) \cong \mathbb{Z}_3 \times \mathbb{Z}_{27}$, и

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{27}. \tag{27}$$

4. Чтобы решить сравнение (26) напомним, что $\mathbb{Z}^*_{p^n}$ — циклическая группа ($p \geq 3$), и если $\langle g_0 \rangle = \mathbb{Z}^*_p$, то $g = g_0 + p \cdot t$ — является образующим группы $\mathbb{Z}^*_{p^n}$, если $t \neq t_0 \cdot g_0 \pmod p$, где $t_0 = \frac{g_0 - 1}{p}$, т.е.

$$\langle g \rangle = \mathbb{Z}^*_{p^n}, \ \mathrm{ord}(g) = (p-1) \cdot p^{n-1}.$$

В нашем случае: $p = 3, \ n = 4, \ g_0 = 2, \ t_0 = \frac{2^2 - 1}{3} = 1$. Следовательно, $t \neq 2$. Возьмём $t = 1$, тогда получим $g = 5, \ \langle 5 \rangle = \mathbb{Z}^*_{81}, \ |\langle 5 \rangle| = 54$. Поэтому корни сравнения (26) в нашем случае это:

$$x_1 \equiv 5^{18} \pmod{81}, \ x_2 \equiv 5^{36} \pmod{81}$$

Находим $x_1 = 5^{16} \cdot 5^2 \pmod{81}$ используя метод повторного возведения в квадрат.

$$5^2 \equiv 25 \pmod{81},\ 5^4 \equiv -23 \pmod{81},$$

$$5^8 \equiv -38 \pmod{81},\ 5^{16} \equiv -14 \pmod{81}.$$

Таким образом, решениями будут:

$$x_1 \equiv 5^{18} \pmod{81} \equiv -14 \cdot 25 \pmod{81} \equiv 26 \pmod{81},$$

$$x_2 = x_1^2 = 28.$$

Учитывая, что $7^{-1} \pmod{81} \equiv -23,\ 81^{-1} \pmod{7} \equiv 2$, общее решение (24) будет иметь вид:

$$X = z_1 \cdot 81 \cdot (81^{-1} \pmod 7) + z_2 \cdot 7 \cdot (7^{-1} \pmod{81}) \pmod{567} = z_1 \cdot 162 - z_2 \cdot 161,$$

где $z_1 \in \{1, 2, 4\},\ z_2 \in \{1, 28, -26\}$. Подставляя значения z_1 и z_2, получим:

$x_1 = 1$, $x_2 = 2 \cdot 162 - 161 = 163$,
$x_3 = 4 \cdot 162 - 161 = -80$, $x_4 = 162 - 28 \cdot 28 = 162 + 28 = 190$,
$x_5 = 2 \cdot 162 + 28 = 352 = 215$, $x_6 = 4 \cdot 162 + 28 = 109$,
$x_7 = 162 + 161 \cdot 26 = 379 = -188$, $x_8 = 2 \cdot 162 + 217 = 541 = -26$,
$x_9 = 4 \cdot 162 + 217 = 298$.

Таким образом, множество элементов порядка 3 группы $\mathbb{Z}_{567}^*$ это $M_3 = \{163, -80, 190, -215, 109, -188, -26, 298\}$. Множеству M_3 соответствуют четыре подгруппы $\mathbb{Z}_{567}^*$

$$\begin{cases} H_1 = \langle 163 \rangle = \{1, 163, -80\}, & H_2 = \langle 190 \rangle = \{1, 190, -188\}, \\ H_3 = \langle 109 \rangle = \{1, 109, -264\}, & H_4 = \langle 298 \rangle = \{1, 298, -215\}, \end{cases} \tag{28}$$

5. Найдём теперь элементы группы G, имеющие порядок 27. Для этого нужно решить систему

$$x^{27} \equiv 1 \pmod 7 \tag{29}$$

$$x^{27} \equiv 1 \pmod{81} \tag{30}$$

Сравнение (29) имеет три решения, т.к. в $\mathbb{Z}_7^*$ выполняется $x^6 \equiv 1$ и, следовательно, (29) эквивалентно сравнению $x^3 \equiv 1 \pmod 7$ и его решения это $x_1 \in \{1, 2, 4\}$.
Сравнение (30) имеет 18 решений. Это следует из того, что $\mathbb{Z}_{81}^*$ — циклическая группа порядка $\varphi(81) = 54$. Следовательно, в $\mathbb{Z}_{81}^*$ существует единственная циклическая подгруппа порядка 27, и

число её образующих равно $\varphi(27) = 18$.
Т.к. $\mathbb{Z}_{81}^* = \langle 5 \rangle, \mathrm{ord}(5) = 54$, то элементы 27 порядка это

$$x_i = (5^2)^i, \text{где } i \in \mathbb{Z}_{27}^*.$$

Для описания группы $S_2(81)$ найдём один элемент y порядка 27. По К.Т.О. имеем $(x_1 = 1,\ x_2 = 25)$:

$$y = x_1 \cdot 162 - x_2 \cdot 161 = 162 - 56 \equiv 106 \pmod{567}$$

6. Найдём элементы c_1, c_2 группы $H_5 = \langle 106 \rangle$ порядка 3. Т.к.

$$c_1 = 106^9 = 106^8 \cdot 106 = -188 \pmod{567}.$$

Второй элемент третьего порядка

$$x_2 = c_1^2 = 190 \pmod{567}$$

Таким образом, $H_4 = \langle 190 \rangle < H_5,\ |H_5| = 27$.

7. Из (24), (28) и (27) получаем все разложения группы $G = \mathbb{Z}_{567}^*$ в прямые произведения циклических подгрупп, $i \in \{1, 2, 3, 4\}$:

$$G = \langle -1 \rangle \cdot \langle 264 \rangle \cdot H_i \cdot H_5 = \langle -1 \rangle \cdot \langle -264 \rangle \cdot H_i \cdot H_5 = \langle 264 \rangle \cdot \langle -264 \rangle \cdot H_i \cdot H_5$$

8. Определим число элементов группы G различных порядков. Так как $|G| = 324$, то $k = \mathrm{ord}(a) \in \{2, 3, 4, 9, 18, 27, 54\},\ a \in G$. Пусть N_k - число элементов порядка k. Из ранее изложенного следует, что $N_2 = 3, N_3 = 8$. Так как $\mathrm{ord}(a \cdot b) = \text{НОК}(a, b)$, получаем, что $N_6 = 3 \cdot 8 = 24$. В группе H_5 число элементов порядка 9 равно $\varphi(9) = 6$, так как в H_5 существует единственная подгруппа порядка 9. Следовательно, $N_9 = N_3 \cdot 6 = 18$. Порядок $\mathrm{ord}(c) = 18$, где $c = a \cdot b$, если

- $\mathrm{ord}(a) = 2,\ \mathrm{ord}(b) = 9,\ b \in H_5,$ или
- $\mathrm{ord}(a) = 6,\ a = u \cdot v,\ \mathrm{ord}(u) = 2,\ \mathrm{ord}(v) = 3,\ v \notin H_5,\ \mathrm{ord}(b) = 9.$

Количество элементов первого типа равно $3 \cdot 6 = 18$.
Второго типа — $3 \cdot 2 \cdot 6 = 36$. В итоге $N_{18} = 54$. Порядок $\mathrm{ord}(c) = 27$, где $c = a \cdot b$, если
$\mathrm{ord}(a) \in \{1, 3\},\ \mathrm{ord}(b) = 27$. Так как $\varphi(27) = 18$, то $N_{27} = 3 \cdot 18 = 54$. Для подсчёта N_{54} заметим, что $\mathrm{ord}(c) = 54$, где $c = a \cdot b$, если $\mathrm{ord}(b) = 27$, и

- $\mathrm{ord}(a) = 2,$ или
- $a = u \cdot v,\ \mathrm{ord}(u) = 2,\ \mathrm{ord}(v) = 3,\ v \notin H_5.$

Следовательно, $N_{54} = 3 \cdot 18 + 6 \cdot 18 = 162$.

Проверка:

$$N_1+N_2+N_3+N_6+N_9+N_{18}+N_{27}+N_{54} = 1+3+8+24+18+54+54+162 = 324 = |G|.$$

5.3. Простейшие алгоритмы дискретного логарифмирования

Алгоритм решения уравнения $a^x = b$ в группе $G,\ a,b \in G,\ ord(a) = n$ (задача дискретного логарифмирования)

I. Алгоритм согласования

1. Выбираем минимальное m, такое, что $m^2 \geq n$.

2. Искомое значение ищем в виде $x = mi - j,\ i = \overline{1,m},\ j = \overline{1,m-1}$.

3. Вычисляем $c = a^m$.

4. Составить множество $A = \{c^i \mid i = \overline{1,m}\}$ и упорядочить его.

5. Составить множество $B = \{ba^j \mid j = \overline{0,m-1}\}$ и упорядочить его.

6. Найти номера i и j совпадающих элементов множеств A и B. Будем иметь $ba^j = c^i$. Следовательно, $x = mi - j$.

Пример 8.

$G = F^*,\ F = GF(49) = \mathbb{Z}_7[\theta]/(\theta^2 + \theta + 3),\ |G| = 48,\ m = 7,\ \theta^x = -\theta + 2.$

Искомое x — значение дискретного логарифма, ищем в виде $x = 7i - j,\ i = \overline{1,7},\ j = \overline{0,6}$.

1. Вычисляем $c = \theta^7 = \theta^4 \cdot \theta^2 \cdot \theta = -\theta - 1$ и упорядочиваем множество $A = \{c^i \mid i = \overline{1,7}\} = \{-\theta - 1,\ \theta - 2,\ 2\theta - 2,\ 2\theta + 1,\ -\theta - 2,\ 2\theta - 1,\ 1\}$.

2. Вычислим и упорядочим множество $B = \{(-\theta+2)\theta^i \mid i = \overline{0,6}\} = \{-\theta + 2,\ 3\theta + 3,\ -2,\ -2\theta,\ 2\theta - 1,\ 1 - 3\theta,\ 2 - 3\theta\}$.

Сравним A и B — общий элемент $2\theta - 1$. Следовательно, $i = 6,\ j = 4$ и $x = 7 \cdot 6 - 4 = 38$.

Упражнение 15.

Решить уравнение $\theta^x = b$ в группе $G = \mathbb{Z}_7[\theta]/(\theta^2 + \theta + 3),\ b = \alpha\theta + \beta,\ \alpha, \beta \in \mathbb{Z}_7[\theta]$.

N	1	2	3	4	5	6	7	8	9	10
α	1	3	-2	3	-1	1	-3	-2	-3	2
β	1	-3	-2	-1	1	1	3	0	1	2
Ответ:	11	13	23	19	29	31	37	41	43	47

II. Алгоритм Полига-Хеллмана

Пусть $G = \langle a \rangle,\ |G| = p = p_1^{k_1} \dots p_t^{k_t},\ a^x = b,$ найти $x =?$

1. Вычисляем элементы:

$$\{(p_i, j) = a^{\frac{n_j}{p_i}}\},\ (j = 0,\ p_i - 1),\ i = \overline{1,t} \tag{31}$$

2. Для каждого $p_1 = p,\ k_i = k,\ x_i = log_a b \pmod{p^k} = \gamma_0 + \gamma_1 p + \ldots + \gamma_{k-1} p^{k-1},\ \gamma_i \in \mathbb{Z}_p$. Коэффициенты $\gamma_0,\ \gamma_1,\ \ldots,\ \gamma_{k-1}$ находим последовательно.

2.1. Вычисляем $b^{\frac{n}{p}} = a^{\frac{\gamma_0 n}{p}} = c(p_1 \gamma_0)$. На основе (31) вычисляем γ_0.

2.2. Вычисляем $b_1 = ba^{-\gamma_0},\ b_1^{\frac{n}{p^2}} = c(p_1 \gamma_1)$. На основе (31) вычисляем γ_1.

Далее, индуктивно, если мы определили уже $\gamma_0, \dots, \gamma_{i-1}$, то вычислим:

$$b_i = ba^{-\gamma_0 - \gamma_1 p - \ldots - \gamma i - 1 p^{i-1}},\ b_i^{\frac{n}{p^{i+1}}} = c(p, \gamma_i)$$

и определяем γ_i.

3. На основе вычисленных $x_1, \dots, x_t$ и китайской теоремы об остатках находим искомый логарифм x :

$$x = \sum x_i \frac{n}{p_i^{k_i}} [(\frac{n}{p_i^{k_i}})^{-1} \pmod{p_i^{k_i}}] \pmod{n}$$

Пример 9.

Найти дискретный логарифм $x = log_3(-52)$ в поле $\mathbb{Z}_{401}^*$.

Решение. $p - 1 = 401 - 1 = 400 = 2^4 \cdot 5^2$.

Найдём $x \equiv x_1 \pmod{2^4}$ и $x \equiv x_1 \pmod{5^2}$. Тогда искомый x можно вычислить по китайской теореме об остатках: $x = [x_1 \cdot 25 \cdot 25^{-1} \pmod{16} + x_2 \cdot 16 \cdot 16^{-1} \pmod{25}] \pmod{400}$.

1. Находим $a(2,0) = 3^{\frac{400}{2} \cdot 0} = 1,\ a(2,1) = 3^{200} \equiv -1 \pmod{401}$. Напомним, что $\mathbb{Z}_{401}^* = \langle 3 \rangle$, и, следовательно, $(\frac{3}{401}) = -1 = 3^{200} \pmod{401}$,

$$a(5,0) \equiv 1,\ a(5,1) = 3^{\frac{400}{5}} = 3^{80} = 3^{64} \cdot 3^{16} \equiv 72,$$

$$a(5,2) = 3^{160} = (a(5,1))^2 \equiv -29,$$

$$a(5,3) = 3^{240} = a(5,1) \cdot a(5,2) \equiv -83,\ a(5,4) = 3^{320} = (a(5,2))^2 \equiv 39.$$

3^2	3^4	3^8	3^{16}	3^{32}	3^{64}
9	81	145	173	-146	63

2. Находим $q = 2,\ x_1 = \lambda_0 + 2\lambda_1 + 4\lambda_2 + 8\lambda_3,\ \lambda_i \in \mathbb{Z}_2$

2.1. Вычисляем $b^{\frac{p-1}{2}} \equiv (-52)^{200} \equiv (-1)^{200} \cdot (\frac{4\cdot 13}{401}) = (\frac{13}{401}) = (\frac{11}{13}) = (-\frac{2}{13}) = (-\frac{1}{13}) = (+1)(-1^{\frac{13^2-1}{8}}) = -1 = a(2, \lambda_0)$.

Из п.1 следует, что $\lambda_0 = 1$.

2.2. Вычислим $b_1 = b \cdot 3^{-\lambda_0} = (-52) \cdot 3^{-1} \pmod{401} \equiv -52 \cdot 134 = 151$.

Вычисляем $a(2, \lambda_1) = b_1^{\frac{q-1}{2^2}} = (151)^{100} \equiv -1$

151^2	151^4	151^8	151^{16}	151^{32}	151^{64}
-56	-72	-29	39	-83	72

Из п.1 следует, что $\lambda_1 = -1$.

2.3. Вычислим $b_2 = b \cdot 3^{-\lambda_0 - 2\lambda_1} = (-52) \cdot 3^{-3} = (-52)(134)^3 = 206$.

Находим $a(2, \lambda_2) = b_2^{\frac{p-1}{2^3}} = (206)^{50} = (206)^{32}(206)^{16}(206)^2 \equiv 1 \pmod{401}$.

206^2	206^4	206^8	206^{16}	206^{32}
-70	88	125	-14	196

Из п.1 следует, что $\lambda_2 = 0$.

2.4. Вычислим $b_3 = b_2 = b \cdot 3^{-\lambda_0 - 2\lambda_1 - 4\lambda_2}$

Находим $b_3^{\frac{p-1}{8}} = b_2^{25} = (206)^{16}(206)^8(206) = (-14)(125)(206) \equiv -1$

Следовательно, $\lambda_3 = 1$.

Таким образом, $x_1 = 1 + 2 + 8 = 11$.

3. $q = 5,\ x_2 = \beta_0 + \beta_1 5,\ \beta_0, \beta_1 \in \mathbb{Z}_5$.

3.1. Вычисляем

$b^{\frac{p-1}{5}} = (-52)^{80} = (52)^{64}(52)^{16} = (-70) \cdot 125 \equiv 72 \pmod{401}$

52^2	52^4	52^8	52^{16}	52^{32}	52^{64}
298	183	206	-70	80	125

$a(5, \lambda_0) = 72$.

Из п.1 следует, что $\lambda_0 = 1$.

3.2. Находим $b_1 = (-52) \cdot 3^{-1} = (-52) \cdot 134 \equiv 151$. Вычисляем $a(5, \lambda_1) = b_1^{\frac{n-1}{q^2}} = 151 = 39$. Из п.1 следует, что $\lambda_1 = 4$. Таким образом, $x_2 = 1 + 4 \cdot 5 = 21 \pmod{25}$.

4. Вычислим искомый $log_3(-52) = x$:

$x = 11 \cdot 25 \cdot (25^{-1} \pmod{16}) + 21 \cdot 16 \cdot (16^{-1} \pmod{25}) \pmod{400}$,

$25^{-1} \pmod{16} \equiv 9^{-1} \pmod{16} \equiv 9$,

$16^{-1} \pmod{25} \equiv 11$,

$x = 11 \cdot 25 \cdot 9 + 21 \cdot 16 \cdot 11 \equiv 33 \cdot (75 + 112) \equiv 171 \pmod{400}$.

Ответ: $log_3(-52) \equiv 171$.

Упражнение 16.

Решить сравнение $a^x \equiv b \pmod p$.

N	1	2	3	4	5	6	7	8
p	541	421	601	641	701	751	811	541
a	2	2	7	3	2	3	3	2
b	101	103	109	113	127	131	137	139

N	9	10	11	12	13	14	15	16
p	421	601	641	701	751	811	541	601
a	2	7	3	2	3	3	2	7
b	149	151	157	163	167	173	179	181

Пример 10.

Вычислить дискретный логарифм $b = 3\theta - 1$ в поле $GF(121) = \mathbb{Z}_{11}[\theta]/(\theta^2 + 3\theta - 3)$.

Решение. $n = 121 - 1 = 120 = 2^3 \cdot 3 \cdot 5,\ p \in \{2, 3, 5\}$

1.Вычисляем элементы $a(p, i) = \theta^{\frac{n}{p}i},\ i = \overline{0, p-1}$.

$a(2, 0) = 1,\ a(2, 1) = -1$, так как θ — примитивный элемент поля, $a(3, 0) = 1,\ a(3, 1) = \theta^{40} = 5\theta - 4,\ a(3, 2) = \theta^{80} = 4\theta + 3,\ a(5, 0) = 1,\ a(5, 1) = \theta^{24} = -2,\ a(5, 2) = 4,\ a(5, 3) = 3,\ a(5, 4) = 5$.

Для вычисления $a(p, i)$ предварительно вычислим, используя соотношение $\theta^2 = 3 - 3\theta$, следующие величины:

$\theta^4 = 3 - \theta,\ \theta^8 = 2\theta + 1,\ \theta^{16} = 3\theta + 2,\ \theta^{32} = -4\theta - 2$.

Например, $a(3, 1) = \theta^{40} = \theta^{32}\theta^8 = (2\theta + 1)(-4\theta + 2) = 5\theta - 4$.

2. Вычислим $x_1 = log_\theta b \pmod 8 = \lambda_0 + 2\lambda_1 + 4\lambda_2$.

2.1. Находим λ_0. Для этого вычисляем $b^{\frac{120}{2}} = (3\theta - 1)^{60}$.

$b^2 = (3\theta - 1)^2 = 9\theta^2 - 6\theta + 1 = 9(3 - 3\theta) - 6\theta + 1 = -5$.

$b^4 = 3,\ b^8 = -2,\ b^{16} = 4,\ b^{20} = b^4 \cdot b^{16} = 3 \cdot 4 = 1,\ b^{10} = -1$.

Следовательно, $b^{60} = 1$, и, таким образом, $\lambda_0 = 0$.

2.2. Находим λ_1. Так как $b_1 = b \cdot \theta^{-\lambda_0} = b$, то вычисляем $b_1^{\frac{120}{4}} = b^{30} = (b^{10})^3 = -1$.

Следовательно, $\lambda_1 = -2,\ b_2 = b \cdot \theta^{-2} = (3\theta - 1)\theta^{-2}$. Учитывая, что $\theta^2 = 3 - 3\theta$, получам, что $\theta^{-2} = 4\theta + 5$ и $b_2 = (3\theta - 1)(4\theta + 5) = -3\theta - 2$. Находим λ_3, для этого вычисляем $b_2^{\frac{120}{8}} = -(3\theta + 2)^{15}$.

Последовательно вычисляем:

$b_2^2 = (3\theta + 2)^2 = -4\theta - 2$,

$b_2^4 = (4\theta + 2)^2 = \theta - 3$,

$b_2^8 = (\theta - 3)^2 = 2\theta + 1$,

$b_2^3 = (-4\theta - 2)(-3\theta - 2) = -4$,

$b_2^{12} = (2\theta + 1)(\theta - 3) = 3$.

Таким образом, $b_2^{15} = -4 \cdot 3 = -12 = -1$. Из п.1 следует, что $\lambda_2 = 1,\ x_1 = log_\theta b = 6 \pmod 8$.

3. Вычисляем $x_2 = log_\theta b \pmod 3$. Для этого нужно вычислить $b^{\frac{120}{3}} = b^{40}$. Из пункта 2.1 следует, что $b^{40} = 1$, следовательно $x_2 = 0$.

4. Вычисляем $x_3 = log_\theta b \pmod 5$. Для этого нужно вычислить $b^{\frac{120}{5}} = b^{24}$. Из пункта 2.1 следует, что $b^{24} = b^{16} \cdot b^8 = (-2) \cdot 4 = 3$, следовательно, $x_3 = 3$.

5. Искомый $x = log_\theta(3\theta - 1)$, находим из системы

$$\begin{cases} x \equiv 6 \pmod 8 \\ x \equiv 0 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \tag{32}$$

На основе китайской теоремы об остатках имеем:

$x = 6 \cdot 15 \cdot (15^{-1} \pmod 8) + 3 \cdot 24 \cdot (24^{-1} \pmod 5) \pmod{120} = -90 - 72 = -162 \equiv 78 \pmod{120}$.

Упражнение 17.

В поле $GF(7^2) = \mathbb{Z}_7[\theta]/(\theta^2 + \theta + 3)$ решить уравнение $\theta^x = b,\ b = \alpha\theta + \beta,\ \alpha, \beta \in \mathbb{Z}_7$.

N	1	2	3	4	5	6	7	8	9	10
α	1	3	-2	3	-1	1	-3	-2	-3	2
β	2	-3	-2	-1	1	1	3	0	1	2

Упражнение 18.

В поле $GF(3^4) = \mathbb{Z}_3[\theta]/(\theta^4 + \theta - 1)$ решить уравнение $\theta^x = b,\ b = \alpha_3\theta^3 + \alpha_2\theta^2 + \alpha_1\theta + \alpha_0,\ \alpha_i \in \mathbb{Z}_3 = \{0, 1, -1\}$.

N	1	2	3	4	5	6	7	8
α_3	0	0	1	-1	1	1	-1	0
α_2	0	1	0	1	1	1	-1	-1
α_1	1	1	0	0	0	-1	0	1
α_0	1	0	-1	-1	0	-1	-1	-1

N	9	10	11	12	13	14	15	16
α_3	0	1	1	1	-1	-1	1	-1
α_2	1	-1	1	1	0	-1	0	0
α_1	1	-1	1	0	1	1	-1	-1
α_0	1	1	1	0	0	-1	-1	-1

6. Эллиптические кривые

6.1. Эллиптические кривые над конечным полем $\mathbf{F_q} = \mathbf{GF(p^n)}$ при $\mathbf{p > 3}$

Каноническое уравнение эллиптической кривой (далее — ЭК):

$$y^2 = x^3 + ax + b. \tag{33}$$

Дискриминант ЭК:

$$D = 27b^2 + 4a^3.$$

Группа точек ЭК, заданной уравнением (33), — это множество $\mathcal{E}_q(a,b) = \{(x,y) \in F_q |\ y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\}$, где $\mathbb{O}$ — бесконечно удаленная точка — нейтральный элемент группы $\mathcal{E}_q(a,b)$.
По определению полагаем, если $\mathcal{M} = (x,y) \in \mathcal{E}_q(a,b)$, то

$$-\mathcal{M} = (x,-y), \qquad \mathcal{M} + \mathbb{O} = \mathcal{M}.$$

Если $\mathcal{M}_1 = (x_1,y_1) \in \mathcal{E},\ \mathcal{M}_2 = (x_2,y_2) \in \mathcal{E}$ и $x_1 \neq x_2$, то

$$\mathcal{M}_1 + \mathcal{M}_2 = \mathcal{M}_3, \qquad \mathcal{M}_3 = (x_3,y_3),\ \text{где}$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{34}$$

Если $\mathcal{M}_0 = (x_0,y_0) \in \mathcal{E}, y_0 \neq 0$, то

$$2\mathcal{M}_0 = \mathcal{M} = (X,\ Y),\ \text{где}$$

$$\begin{cases} X = \lambda^2 - 2x_0, \\ X = \lambda(x_0 - X) - y_0, \end{cases} \quad \lambda = \frac{3x_0^2 + a}{2 \cdot y_0}. \tag{35}$$

Теорема 4 (Хассе). *Если* $4a^3 + 27b^2 \neq 0 \pmod{p},\ p > 3$*, то число решений* N *сравнения*

$$y^2 = x^3 + ax + b \pmod{p}$$

удовлетворяет неравенству

$$|N - p| < 2\sqrt{p}.$$

Теорема 5 (Хассе-Вейля). *Если* $\#\mathcal{E}_q(a,b) = N$*, то* $\#\mathcal{E}_{q^n}(a,b) = q^n + 1 - (\alpha^n + \beta^n)$*, где* α *и* β *— корни уравнения* $x^2 - tx + q = 0,\ t = q + 1 - N$*.*

Если $q \equiv 2 \pmod{3}$, то $\#\mathcal{E}_q(0,b) = q + 1$ и $\mathcal{E}_q(a,b)$ — циклическая группа.

Если $q \equiv 3 \pmod{4}$, то $\#\mathcal{E}_q(a,0) = q + 1$. При этом, если a — вычет, то есть является четной степенью примитивного элемента поля F_q, то $\mathcal{E}_q(a,0)$ — циклическая группа. В противном случае, $\#\mathcal{E}_q(a,0) \cong \mathbb{Z}_2 \times \mathbb{Z}_{\frac{q+1}{2}}$.

Упражнение 6.1. Найти все точки группы $\mathcal{E}_q(a,b)$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	7	11	13	17	19	23	7	11	13	17	19	23	7	11	29
a	1	1	1	1	1	1	1	2	1	-1	-1	-1	-1	-1	7
b	1	1	1	1	1	1	2	1	1	1	1	-1	1	2	4

Пример. $\mathcal{E} : y^2 = x^3 + 7x + 4 \pmod{29}$.
Находим все вычеты по модулю 29:

x	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10	±11	±12	±13	±14
x^2	1	4	9	-13	-4	7	-9	6	-6	13	5	-1	-5	-7

Для каждого $x \in \mathbb{Z}_{29}$ вычисляем $f(x) = x^3 + 7x + 4$.
Определим те значения $f(x)$, которые являются вычетами по модулю 29:

x	0	3	4	6	9	10	11	13	14	-1	-4	-6	-8	-9	-10	-13	-14
$f(x)$	4	-6	9	1	13	1	-9	1	4	-4	-1	7	-13	-5	7	7	4

Таким образом, $\mathcal{E}_{29}(7,\ 4)$ кроме $\mathbb{O}$ содержит следующие точки:

x	0	3	4	6	9	10	11	13	14
y	± 2	± 9	± 3	± 1	± 10	± 1	± 7	± 1	± 2

x		-1	-4	-6	-8	-9	-10	-13	-14
y		± 5	± 12	± 6	± 4	± 13	± 6	± 6	± 2

Порядок группы $\mathcal{E}_{29}(7,\ 4)$ равен 35. Следовательно, эта группа циклическая.

Упражнение 6.2. Для двух точек $\mathcal{M}_1 = (x_1, y_1)$ и $\mathcal{M}_2 = (x_2, y_2)$ из группы $\mathcal{E}_q(a,\ b)$ из упражнения 6.1 вычислить координаты точек $\mathcal{M}_3 = \mathcal{M}_1 + \mathcal{M}_2$ и $\mathcal{M}_0 = 2\mathcal{M}_1 = (X,\ Y)$.

N	1	2	3	4	5	6	7	8	9	10	11	12
x_1	3	4	6	9	10	11	13	14	3	6	4	0
y_1	9	-3	-1	10	1	-7	1	2	-9	1	3	2
x_2	-1	-4	-8	-8	-9	-10	-6	-13	-4	11	9	3
y_2	5	12	4	-4	13	6	6	-6	-12	7	-10	-9

Пример. Вычислить координаты точки $\mathcal{M}_3 = \mathcal{M}_1 + \mathcal{M}_2$, $\mathcal{M}_1,\ \mathcal{M}_2 \in \mathcal{E}_{29}(7,\ 4), \mathcal{M}_1 = (0,\ 2),\ \mathcal{M}_2 = (3, -9)$.
Решение. Находим $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-9-2}{3-0} = -11 \cdot 3^{-1} \pmod{29} \equiv -11 \cdot 10 \equiv 6 \pmod{29}$.
Из (34) следует, что: $x_3 = \lambda^2 - x_1 - x_2 = 36 - 0 - 3 \equiv 4 \pmod{29},\ y_3 = 6(0-4) - 2 \equiv 3 \pmod{29}$.
Таким образом, $\mathcal{M}_3 = (4,\ 3)$.
Для вычисления $\mathcal{M}_0 = 2\mathcal{M}_1$, по формулам (35) вычисляем

$$\lambda = \frac{3 - 0^2 + 7}{4} \equiv -9 \pmod{29},\ \ \lambda^2 \equiv -6 \pmod{29},$$

$$X = -6 \pmod{29},\ \ Y = 9 \cdot 6 - 2 = -6.$$

Поэтому $2\mathcal{M}_1 = (-6,\ -6)$.

Упражнение 6.3. Вычислить порядок точки $\mathcal{M} = (x_0,\ y)$ группы $\mathcal{E}_{83}(4,\ 0)$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_0	-3	-7	-8	-9	-11	52	41	46	50	35	60	17	54	28	10

Так как 4 — вычет по модулю 83, то группа $\mathcal{E}_{83}(4,\ 0)$ — циклическая, $\#\mathcal{E}_{83}(4,\ 0) = 84$.

Следовательно, порядок любой точки есть делитель 84.

Пример. Определить порядок точки $\mathcal{M}_0(10,\ y_0)$.
Вычисляем $y_0 = \pm 58$. Положим $y_0 = 58$ и пусть T — порядок точки $\mathcal{M}_0$. Так как $\#\mathcal{E}_{83}(4,\ 0) = 84$, то $T \in \{2,\ 3,\ 4,\ 6,\ 7,\ 12,\ 14,\ 21,\ 28,\ 42,\ 84\}$. Вычисляем T.

1) Так как $\mathcal{M}_0 \neq (0,\ 0)$, то $T \neq 2$.

2) Вычисляем $2\mathcal{M}_0 = (-8,\ 28) \neq -\mathcal{M}_0,\ 2\mathcal{M}_0 \neq -2\mathcal{M}_0$, следовательно, $T \neq 3,\ 4$.

3) Вычисляем $4\mathcal{M}_0 = (-34,\ 20) \neq -2\mathcal{M}_0,\ 4\mathcal{M}_0 \neq -4\mathcal{M}_0$, то есть, $T \neq 6,\ 8$.

4) Вычисляем $8\mathcal{M}_0 = (26,\ 1) \neq \mathcal{M}_0,\ 8\mathcal{M}_0 \neq -4\mathcal{M}_0$, следовательно, $T \neq 7,\ 12$.

5) Вычисляем $16\mathcal{M}_0 = (16,\ 33) \neq 2\mathcal{M}_0$, то есть, $T \neq 14$.

6) Вычисляем $20\mathcal{M}_0 = 16\mathcal{M}_0 + 4\mathcal{M}_0 = (16,\ 33) + (-34,\ 20) = (10, -58) =$

$= -\mathcal{M}_0$.
Таким образом, $T = 21$.

Упражнение 6.4. Определить порядок эллиптической кривой $y^2 = x^3 + ax + b \mod p$ и определить порядока точки $\mathcal{M}(c, d)$.

N	1	2	3	4	5	6	7	8	9	10
p	17	17	17	17	23	23	23	23	19	19
a	11	3	15	0	15	6	11	21	3	15
b	14	14	21	15	1	15	14	4	4	4
c	15	3	1	12	13	9	18	6	12	2
d	1	4	1	3	1	4	15	1	1	2

N	11	12	13	14	15	16	17	18	19	20
p	19	19	19	19	17	17	19	23	23	23
a	11	8	17	17	15	9	17	14	17	21
b	12	5	10	13	2	6	7	10	14	4
c	8	7	6	2	7	7	4	16	8	1
d	2	9	9	6	5	2	5	11	8	7

Упражнение 6.5. Найти точку $\mathcal{M}(c, y) \in \mathcal{E}_p(a,\ b)$ и определить её порядок.

N	1	2	3	4	5	6	7	8	9	10
c	11	16	22	25	28	10	13	19	25	29
p	71	71	71	71	71	83	83	83	83	83
a	0	0	0	0	0	0	0	0	0	0
b	23	-17	21	33	7	25	-36	-16	27	-7

N	11	12	13	14	15	16	17	18	19	20
c	28	25	22	16	11	31	33	35	21	39
p	71	71	71	71	71	83	83	83	83	83
a	-9	-19	68	-13	6	20	41	-20	11	-2
b	0	0	0	0	0	0	0	0	0	0

Упражнение 6.6. Определить порядок и строение группы $\mathcal{E}_p(a,\ 0)$ и найти все точки второго порядка.

N	1	2	3	4	5	6	7	8
p	683	719	727	739	751	787	811	823
a	101	103	107	104	113	127	131	137

N	9	10	11	12	13	14	15	16
p	827	859	863	883	887	911	919	947
a	139	149	151	157	163	167	173	179

Упражнение 6.7. Найти точку второго порядка группы $\mathcal{E}_p(0,\ b)$.

N	1	2	3	4	5	6	7	8
p	401	419	431	449	461	467	491	521
b	31	37	41	43	47	53	54	61

N	9	10	11	12	13	14	15	16
p	557	563	569	587	593	599	617	641
b	67	67	71	73	79	83	89	101

Упражнение 6.8. Найти порядок группы ЭК $\mathcal{E}_{q^n}(a,\ b)$, заданной уравнением $y^2 = x^3 + ax + b$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
q	5	7	11	13	5	7	11	13	5	7	11	13	5	7	11
a	3	3	3	1	2	1	1	-1	1	1	2	2	-1	1	2
b	2	1	2	1	1	3	-1	1	1	1	2	2	1	1	2
n	8	5	6	7	5	8	7	5	8	6	5	5	9	7	6

Пример. Найти порядок группы $\mathcal{E}_{5^5}(2,\ 1)$.
Найдем порядок группы $\mathcal{E}_5(2,\ 1)$.
Уравнение соответствующей ЭК:

$$y^2 = x^3 + 2x + 1 \pmod 5.$$

Находим точки этой ЭК: $(0,\ \pm 1),\ (1,\ \pm 2),\ (-2,\ \pm 2)$. Таким образом, $\#\mathcal{E}_5(2,\ 1) = N = 7$.
Согласно теореме Хассе–Вейля, $\#\mathcal{E}_{5^5}(2,\ 1) = 5^5 + 1 - (\alpha^5 + \beta^5)$, где $t = q + 1 - N = 5 + 1 - 7 = -1,\ \alpha,\ \beta$ — корни уравнения $x^2 + x - 5 = 0$. Для вычисления $\alpha^5 + \beta^5$ воспользуемся рекуррентной формулой Люка:

$$S_n = \alpha^n + \beta^n,\ S_n = tS_{n-1} - qS_{n-2},\ t = \alpha + \beta.$$

В нашем случае:

$$S_1 = \alpha + \beta = t = -1,\ S_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 1 - 10 = -9,$$

$$S_3 = -S_2 - 5S_1 = 9 + 5 = 14,\ S_4 = -S_3 - 5S_2 = -14 + 45 = 31,$$

$$S_5 = -S_4 - 5S_3 = -31 - 70 = -101.$$

Таким образом, $\#\mathcal{E}_{5^5}(2,\ 1) = 5^5 + 1 + 101 = 3227$.
Упражнение 6.9. Убедиться, что порядок точки $M(c, d)$ равен q, $M \in \mathcal{E} : y^2 = x^2 + ax + b$ над $\mathbb{Z}_p$ и найти порядок $\#\mathcal{E}$, используя теорему Хассе. При $p = 101,\ a = -3,\ b = 0,\ q = 61$; при $p = 103,\ a = 36,\ b = 43,\ q = 53$.

N	1	2	3	4	5	6	7	8	9	10
p	101	103	101	103	101	103	101	103	101	103
c	4	8	9	9	13	11	24	13	31	32
d	31	15	55	13	21	88	4	37	2	30
N	11	12	13	14	15	16	17	18	19	20
p	101	103	101	103	101	103	101	103	101	103
c	54	36	65	50	70	65	87	73	88	84
d	34	10	35	36	20	12	96	44	8	15

Упражение 6.10. Из множества $C = \{\pm c\}$ выбрать элемент, при котором $x_0^3 + ax_0$ будет квадратичным вычетом и определить порядок точки $\mathcal{M}(x_0,\ y) \in \mathcal{E}_q(a,\ 0)$.

N	1	2	3	4	5	6	7	8
q	103	127	131	151	163	167	179	107
a	17	19	23	29	31	37	61	41
c	2	3	4	5	6	7	8	9
N	9	10	11	12	13	14	15	16
q	139	199	191	131	151	163	167	169
a	43	47	53	59	61	67	71	79
c	10	11	12	13	14	15	16	17

Задача 6.11. Доказать, что если $\#\mathcal{E} = q + 1$ над полем $GF(q)$ и T_n — порядок группы $\mathcal{E}$ над полем $GF(q^n)$, то

$$T_n = \begin{cases} q^n + 1, & \text{если } n = 1 \pmod 2, \\ (q^{\frac{n}{2}} + 1)^2, & \text{если } n = 2 \pmod 4, \\ (q^{\frac{n}{2}} - 1)^2, & \text{если } n = 0 \pmod 4. \end{cases}$$

Задача 6.12. Доказать, что если $\mathcal{E} : y^2 = x^3 + b$ над полем $GF(5^{2k+1})$, то $\#\mathcal{E} = 5^{2k+1} + 1$.

Задача 6.13. Доказать, что если $\mathcal{E} : y^2 = x^3 + ax$ над полем $GF(7^{2k+1})$, то $\#\mathcal{E} = 7^k + 1$.

Задача 6.14. Проверить, что порядок точки $\mathcal{P}(x, y) \in \mathcal{E}(a, b) : y^2 = x^3 + ax + b \pmod p$ равен d и определить порядок соответствующей группы ЭК.

N	a	b	p	x	y	d
1	-14	-31	97	2	6	29
2	30	47	101	1	49	39
3	-6	-9	101	4	43	29
4	36	43	103	8	15	53
5	-26	-36	97	2	5	47
6	-3	0	101	5	3	61
7	-19	19	97	1	1	107
8	-37	49	97	-2	-4	83

6.2. Эллиптические кривые над полем характеристики 3

Каноническое уравнение ЭК над конечным полем характеристики $p = 3$ имеет вид:

$$\mathcal{E} : y^2 = x^3 + ax^2 + bx + c. \tag{36}$$

Если $\mathcal{M}_1 = (x_1,\ y_1)$ и $\mathcal{M}_2 = (x_2,\ y_2)$ — точки ЭК (36) и $x_1 \neq x_2$, то координаты точки $\mathcal{M}_3 = (x_3, y_3)$ определяются по формулам:

$$\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{37}$$

Если $\mathcal{M} = (X,\ Y) = 2\mathcal{M}_0 = 2(x_0,\ y_0),\ y_0 \neq 0$, то

$$\begin{cases} X = \lambda^2 - a - 2x_0, \\ X = \lambda(x_0 - X) - y_0, \end{cases} \quad \lambda = \frac{ax_0 - b}{y_0}. \tag{38}$$

Пример. Над полем $G = (3^2) = \mathbb{Z}_3[\theta]/(\theta^2 + \theta - 1) = \{\alpha + \beta\theta \mid \alpha, \beta \in \mathbb{Z}_3\}$ найти все точки ЭК, заданной уравнением:

$$\mathcal{E} : y^2 = x^3 + \theta x + 1,\ a = 0,\ b = \theta,\ c = 1.$$

Для вычисления координат точек кривой используем таблицу представления степеней примитивного элемента поля GF_9:

θ^i	1	θ	θ^2	θ^3	θ^4	θ^5	θ^6	θ^7	θ^8
$\alpha + \beta\theta$	1	θ	$1 - \theta$	$-1 - \theta$	-1	$-\theta$	$\theta - 1$	$1 + \theta$	1

Используя эту таблицу вычисляем значения $f(x) = x^3 + \theta x + 1$ при всех $x \in \mathbb{F}_9$:

x	0	1	$-1 = \theta^4$	θ	θ^2	$-\theta^2 = \theta^6$	$-\theta = \theta^5$	θ^3	$-\theta^3 = \theta^7$
$f(x)$	1	θ^6	θ^5	θ^7	θ^4	0	θ^2	θ	θ^3

Таким образом, $\mathcal{E}_9(0,\ \theta,\ 1) = \{(0,\ \pm 1),\ (1,\ \pm\theta),\ (\theta^2,\ \pm\theta^2),\ (-\theta,\ \pm\theta),\ (-\theta^2,\ 0),\ \mathbb{O}\}$ и $\#\mathcal{E}_9(0, \theta, 1) = 10$.
Заметим, что $\#\mathcal{E}_9(0, \theta, 1)$ — циклическая группа.
Пусть $\mathcal{M}_1 = (1,\ \theta^3),\ \mathcal{M}_2 = (\theta^2,\ \theta^2)$.

A. Найдем точку $\mathcal{M}_3 = \mathcal{M}_1 + \mathcal{M}_2 = (x_3,\ y_3)$.

   1) Вычисляем $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\theta^2 - \theta^3}{\theta^2 - 1} = \frac{1}{\theta} = \theta^7$.
   2) Находим $x_3 = \lambda^2 - a - x_1 - x_2 = \theta^{14} - 1 - \theta^2 = -\theta$.
   3) Определяем $y_3 = \lambda(x_1 - x_3) - y_1 = \theta^7(1 + \theta) - \theta^3 = -\theta$.

   Таким образом, $\mathcal{M}_3 = (-\theta,\ -\theta)$.

B. Найдем точку $\mathcal{M} = (X,\ Y) = 2\mathcal{M}_1$.

   1) Вычисляем $\lambda = \frac{ax_1 - b}{y_1} = \frac{\theta}{\theta^3} = \theta^2$.
   2) Находим $X = \lambda^2 - a + x_1 = \theta^4 + 1 = 0$.

3) Определяем $Y = \lambda(x_1 - X) - y_1 = \theta^2 - \theta^3 = -1$.

Таким образом, $2(1,\ \theta^3) = (0,\ -1)$.

C. Найдем порядок T точки $\mathcal{M}_1 = (1,\ \theta^3)$.
Так как порядок группы равен 10, то $T \in \{2,\ 5,\ 10\}$.
Так как $y_1 = \theta^3 \neq 0$, то $T \neq 2$.
Вычислим $4\mathcal{M}_1 = 2(0,\ -1) = (X,\ Y)$.
Находим λ по формуле (37):

$$\lambda = \frac{-\theta}{-1} = \theta$$

и определяем

$$X = \lambda^2 + x = \theta^2.$$

И, наконец, по формуле (38) вычисляем:

$$Y = -\theta^3 + 1 = \theta - 1 = -\theta^2.$$

Итак, $4\mathcal{M}_1 = 4(1,\ \theta^3) = (\theta^2,\ -\theta^2) \neq -\mathcal{M}_1$.
Следовательно, $T \neq 5$ и значит $T = 10$, то есть точка $\mathcal{M}_1$ — образующая группы $\mathcal{E}_9(0,\ \theta,\ 1)$.

Упражнение 6.15. Вычислить все точки ЭК $y^2 = x^3 + ax^2 + bx + c$ над полем $GF(3^2) = \mathbb{Z}_2[\theta]/(\theta^2 + 1)$.

N	1	2	3	4	5	6	7	8	9	10	11	12
a	1	-1	θ	$-\theta$	θ^2	$-\theta^2$	θ^3	$-\theta^3$	-1	1	θ	$-\theta$
b	θ	θ	θ^2	$-\theta$	-1	1	θ	$-\theta$	θ^3	$-\theta^3$	0	θ^3
c	θ^2	$-\theta$	θ^3	1	θ	$-\theta^3$	1	θ^2	1	-1	θ^2	1

Задача 6.16. Доказать, что если $\mathcal{E} : y^2 = x^3 + b$ над полем $GF(3^n)$, то $\#\mathcal{E} = 3^n + 1$.

Задача 6.17. Доказать, что если $\mathcal{E} : y^2 = x^3 - x - 1$ над полем $GF(3^n)$, то

$$\#\mathcal{E} = \begin{cases} 3^n + 1 - 3^{\frac{n+1}{2}}, & n = \pm 1 \pmod{12}, \\ 3^n + 1 + 3^{\frac{n+1}{2}}, & n = \pm 5 \pmod{12}, \\ 3^n + 1, & n = \pm 3 \pmod{12}. \end{cases}$$

6.3. Эллиптические кривые над полем $\mathbf{GF}(2^{\mathbf{n}})$

Канонические уравнения кривых.
Уравнение суперсингулярной кривой имеет вид:

$$\mathcal{E} : y^2 + ay = x^3 + bx + c,\ a,\ b,\ c \in GF(2^n). \tag{39}$$

Уравнение несуперсингулярной кривой имеет вид:

$$\mathcal{E} : y^2 + xy = x^3 + ax^2 + b,\ a,\ b, \in GF(2^n). \tag{40}$$

Для кривой (39) правила сложения точек следующие:
$\mathcal{M}_1 = (x_1,\ y_1),\ \mathcal{M}_2 = (x_2,\ y_2),\ \mathcal{M}_3 = \mathcal{M}_1 + \mathcal{M}_2,\ x_1 \neq x_2.$

$$\begin{cases} x_3 = \lambda^2 + x_1 + x_2, \\ y_3 = \lambda(x_1 + x_3) + y_1 + a, \end{cases} \qquad \lambda = \frac{y_2 + y_1}{x_2 + x_1}. \tag{41}$$

$\mathcal{M}_0 = (x_0,\ y_0), \quad -\mathcal{M}_0 = (x_0,\ y_0 + a).$

Координаты удвоенной точки $(X,\ Y) = 2\mathcal{M}_0$ вычисляются по формулам:

$$\begin{cases} X = \lambda^2, \\ Y = \lambda(x_0 + X) + y_0 + a, \end{cases} \qquad \lambda = \frac{x_0^2 + b}{a}. \tag{42}$$

Если степень поля нечетная, то уравнение суперсингулярной кривой можно привести к виду:

$$y^2 + y = x^3 + ax + b,\ a, b \in GF(2). \tag{43}$$

Для ЭК (40) формулы сложения точек следующие:
$\mathcal{M}_1 = (x_1,\ y_1),\ \mathcal{M}_2 = (x_2,\ y_2),\ \mathcal{M}_3 = \mathcal{M}_1 + \mathcal{M}_2,\ x_1 \neq x_2.$

$$\begin{cases} x_3 = \lambda^2 + \lambda + a + x_1 + x_2, \\ y_3 = \lambda(x_3 + x_1) + y_1 + x_3, \end{cases} \qquad \lambda = \frac{y_2 + y_1}{x_2 + x_1}. \tag{44}$$

$\mathcal{M}_0 = (x_0,\ y_0), \quad -\mathcal{M}_0 = (x_0,\ y_0 + x_0).$

$2\mathcal{M}_0 = (X,\ Y),\ x_0 \neq 0.$

$$\begin{cases} X = \lambda^2 + \lambda + a, \\ Y = x_0^2 + (\lambda + 1)X, \end{cases} \qquad \lambda = x_0 + \frac{y_0}{x_0}. \tag{45}$$

При вычислениях в поле $GF(2^{2k+1})$ необходимо использовать следующее утверждение.

Утверждение 1. *Сравнение*

$$y^2 + y = a$$

в поле $GF(2^{2k+1})$ *разрешимо тогда и только тогда, когда*

$$Tr(a) = a^{2^0} + a^{2^1} + a^{2^2} + \cdots + a^{2^{2k}} = 0.$$

При этом решением будет иметь вид

$$y = a^{2^1} + a^{2^2} + \cdots + a^{2^{2k-1}}. \tag{46}$$

Алгоритм поиска точек ЭК над полем $GF(2^{2k+1})$**.**
Пусть $\mathcal{E}$ суперсингулярная кривая:

$$\mathcal{E} : y^2 + y = x^3 + ax + b,\ a,\ b \in GF(2).$$

Пусть $x = \theta^i,\ \theta$ — примитивный элемент.

1) Вычисляем $a = \theta^{3i} + a\theta^i + b = \theta^k$.
2) Вычисляем $Tr(a)$. Если $Tr(a) = 0$, то находим y_1 по формуле (46). Второе решение $y_2 = y_1 + 1$.

Если $Tr(a) = 1$, то точки с $x = \theta^i$ нет на данной ЭК.

Пусть $\mathcal{E}$ несуперсингулярная кривая над полем $GF(2^{2k+1})$:

$$\mathcal{E} : y^2 + xy = x^3 + ax^2 + b \tag{47}$$

От сравнения (47) переходим к сравнению

$$z^2 + z = x + a + b \cdot (x^{-1})^2, \qquad z = \frac{y}{x}. \tag{48}$$

Для данного $x = \theta^i$ вычисляем

$$d = \theta^i + a \cdot b \cdot \theta^{-2i}.$$

Далее вычисляем $Tr(d)$. Если $Tr(d) = 0$, то находим $z = \theta^k$ и соответствующий $y = x \cdot z = \theta^{k+i}$.
Если $Tr(d) = 1$, то точки с $x = \theta^i$ на ЭК нет.

Аномальная несуперсингулярная кривая $\mathcal{E}_a(n)$ над полем $GF(2^n)$ задается уравнением:

$$y^2 + xy = x^3 + ax^2 + 1, \quad a \in GF(2).$$

Из теоремы Хассе–Вейля следует, что

$$\#\mathcal{E}_a(n) = 2^n + 1 - (\alpha^n + \beta^n),$$

где $\alpha + \beta = 2 + 1 - N = (-1)^{(a+1)}, \quad \alpha \cdot \beta = 2.$ где N порядок $\#\mathcal{E}_a(n)$ над полем $GF(2)$. Нетрудно убедиться, что

$$N = \#\mathcal{E}_a(1) = \begin{cases} 4, & \text{если } a = 0 \\ 2, & \text{если } a = 1 \end{cases},$$

Если $\#\mathcal{E}_a(n) = p \cdot N,$ где p — простое, то группа $\mathcal{E}_a(n)$ — циклическая.

Точка $\mathcal{P} \in \mathcal{E}_a(n)$ является удвоенной тогда и только тогда, когда $Tr(x) = Tr(a)$.

Пусть n — нечетно и $\mathcal{E}_a(n) : y^2+xy = x^3+ax^2+1,\ a \in GF(2^n),\ Tr(a) = 0$. Тогда для точки $(x,\ y) \in \mathcal{E}_a(n)$ существует точка $(x_1,\ y_1) \in \mathcal{E}_a(n)$ такая, что $(x,\ y) = 4(x_1,\ y_1)$ тогда и только тогда, когда

$$Tr(x) = 0,\ Tr(y) = Tr(\lambda x),\ \text{где } \lambda^2 + \lambda = x + a. \tag{49}$$

Если $Tr(a_1) \neq Tr(a_2)$ и

$$\mathcal{E}_i : y^2 + xy = x^3 + a_i x + b,\ i = 1,\ 2,\ \mathbb{F} = GF(2^m), m = 2k + 1,$$

то $\#\mathcal{E}_1 + \#\mathcal{E}_2 = 2^{m+1} + 2$.

Если $\mathcal{M}(x,\ y) \in \mathcal{E}_1(2k+1) : y^2 = x^3 + ax^2 + 1,\ \#\mathcal{E}_1 = 2p$, то $\operatorname{ord}(M) = p$ тогда и только тогда, когда $Tr(a) = 1$.

Если $\mathcal{M}(x,\ y) \in \mathcal{E}_0(n) : y^2 = x^3 + 1,$ и $\#\mathcal{E} = 4p$, то $\operatorname{ord}(M) = p$ тогда и только тогда, когда $Tr(x) = Tr(y) = Tr(\lambda x),$ где $\lambda^2 + \lambda = x$.

Задача 6.19. $\mathcal{E} : y^2+y = x^3+x+1$ над полем $F = GF(2^m)$, $\mathcal{P}(x, y) \in \mathcal{E}$. Доказать, что

$$\begin{cases} 2^n \cdot \mathcal{P} = (x^{2^{2n}} + 1, x^{2^{2n}} + y^{2^{2n}}), & n \equiv 1 \pmod 4, \\ 2^n \cdot \mathcal{P} = (x^{2^{2n}}, y^{2^{2n}} + 1), & n \equiv 2 \pmod 4, \\ 2^n \cdot \mathcal{P} = (x^{2^{2n}} + 1, x^{2^{2n}} + y^{2^{2n}} + 1), & n \equiv 3 \pmod 4, \\ 2^n \cdot \mathcal{P} = (x^{2^{2n}}, y^{2^{2n}}), & n \equiv 0 \pmod 4. \end{cases}$$

Упражнение 6.20. Для $\mathcal{E}(1) : y^2 + ay = x^3 + bx + c$ при $a, b, c \in GF(4) = \mathbb{Z}_2[\theta]/(\theta^2+\theta+1)$ найти все точки. Определить порядок $\mathcal{E}(n)$.

N	1	2	3	4	5	6	7	8
a	θ	θ	θ	θ	θ	θ	θ	θ
b	1	$\theta+1$	1	$\theta+1$	θ	θ	$\theta+1$	$\theta+1$
c	θ	θ	$\theta+1$	0	$\theta+1$	1	$\theta+1$	1
n	6	5	7	6	7	5	5	6

N	9	10	11	12	13	14	15	16
a	θ	$\theta+1$	$\theta+1$	$\theta+1$	$\theta+1$	$\theta+1$	$\theta+1$	$\theta+1$
b	θ	0	1	θ	$\theta+1$	θ	1	$\theta+1$
c	0	$\theta+1$	θ	1	0	0	$\theta+1$	1
n	7	7	6	5	5	6	7	6

Упражнение 6.21. Найти все точки кривой $\mathcal{E}_1 : y^2 + y = x^3 + x$ над полем $GF(2)$.

Ответ: $\{(0,\ 0),\ (0,\ 1),\ (1,\ 0),\ (1,\ 1),\ \mathbb{O}\}$.

Упражнение 6.22. Найти все точки кривой

$$\mathcal{E}_2 : y^2 + \theta y = x^3 + x + \theta + 1$$

над полем $GF(4) = \mathbb{Z}_2[\theta]/(\theta^2 + \theta + 1) = \{0,\ 1,\ \theta,\ \theta + 1\},\ \theta^2 = \theta + 1$.

Ответ: $\{(0,\ 1),\ (0,\ \theta + 1),\ (1,\ 1),\ (1,\ \theta + 1),\ (\theta,\ 0),\ (\theta,\ \theta),\ \mathbb{O}\}$.

Упражнение 6.23. Найти точку $M = (x,\ y) = (\theta,\ 0) + (1,\ 1)$.
Ответ: $M = (0,\ 1)$.

Упражнение 6.24. Найти точку $M = (x,\ y) = 2(\theta,\ \theta)$.
Ответ: $M = (1,\ \theta + 1)$

Упражнение 6.25. Найти порядок группы точек кривой $\mathcal{E}_2$ над полем $GF(16)$, являющимся расширением степени 2 поля из упражнения 6.22.
Ответ: 21.

Упражнение 6.26. Найти все точки группы точек эллиптической кривой

$$y^2 + (\theta + 1)y = x^3 + \theta x$$

над полем $GF(4) = \mathbb{Z}_2[\theta]/(\theta^2 + \theta + 1)$.
Ответ: $\{(0,\ 0),\ (\theta,\ \theta + 1),\ (\theta,\ 1),\ (\theta,\ \theta),\ (\theta + 1,\ 0),\ (\theta + 1,\ \theta),\ \mathbb{O}\}$.

Упражнение 6.27. Определить порядок группы точек ЭК над расширением поля $GF(4) = \mathbb{Z}_2[\theta]/(\theta^2 + \theta + 1)$ степени 4, заданной уравнением $y^2 + xy = x^3 + (\theta + 1)x + 1$.
Ответ: 318.

Упражнение 6.28. Для $\mathcal{E} : y^2 + xy = x^3 + \theta x^2 + \theta + 1$ над полем $GF(4) = \mathbb{Z}_2[\theta]/(\theta^2 + \theta + 1)$:

1) Найти все точки $\mathcal{E}$.
2) Определить порядок $\mathcal{E}$ над полем $GF(4^3)$.
3) Найти координаты точки $M = (x, y) = (1,\ 1) + (\theta,\ 1)$.
4) Найти координаты точки $M = (x,\ y) = 2(\theta,\ \theta + 1)$.

Ответ:

1) $\{(1,\ 0),\ (1,\ 1),\ (\theta,\ 1),\ (\theta,\ \theta + 1),\ (0,\ \theta),\ \mathbb{O}\}$.
2) 54.
3) $(1,\ 0)$.
4) $(\theta,\ 1)$.

Упражнение 6.29. Для $\mathcal{E} : y^2 + xy = x^3 + (\theta + 1)x^2 + \theta$ над полем $GF(4) = \mathbb{Z}_2[\theta]/(\theta^2 + \theta + 1)$:

1) Найти все точки $\mathcal{E}$.
2) Определить порядок $\mathcal{E}$ над полем $GF(4^3)$.

3) Определить порядок $\mathcal{E}$ над полем $GF(4^6)$.

4) Найти координаты точки $M = (x,\ y) = (1,\ 1) + (\theta + 1,\ 1)$.

5) Найти координаты точки $M = (x,\ y) = 2(\theta + 1,\ \theta)$.

Ответ:

1) $\{(1,\ 0),\ (1,\ 1),\ (\theta + 1,\ 1),\ (\theta + 1,\ \theta),\ (0,\ \theta + 1),\ \mathbb{O}\}$.

2) 54.

3) 4104.

4) $(0,\ \theta + 1)$

5) $(\theta + 1,\ 1)$.

Упражнение 6.30. Найти все точки группы ЭК $\mathcal{E} : y^2 + xy = x^3 + \theta x$ над полем $GF(4) = \mathbb{Z}_2[\theta]/(\theta^2 + \theta + 1)$.
Ответ: $\{(0,\ 0),\ (\theta,\ \theta),\ (\theta,\ 0),\ (\theta + 1,\ 1),\ (\theta + 1,\ \theta),\ \mathbb{O}\}$

Упражнение 6.31. Найти точку $2(\theta, \theta)$ эллиптической кривой из упражнения 6.26.
Ответ: $(\theta,\ 0)$.

Упражнение 6.32. Найти все точки группы ЭК

$$\mathcal{E} : y^2 + xy = x^3 + \theta^4 x^2 + 1$$

над полем $GF(2^4) = \mathbb{Z}_2[\theta]/(\theta^4 + \theta + 1)$
Ответ: $\{(1,\ \theta^{13}),\ (\theta^3,\ \theta^{13}),\ (\theta^5,\ \theta^{11}),\ (\theta^6,\ \theta^{14}),\ (\theta^9,\ \theta^{13}),\ (\theta^{10},\ \theta^8),\ (\theta^{12},\ \theta^{12}),\ (1,\ \theta^6),\ (\theta^3,\ \theta^8),\ (\theta^5,\ \theta^3),\ (\theta^6,\ \theta^8),\ (\theta^9,\ \theta^{10}),\ (\theta^{10},\ \theta),\ (\theta^{12},\ \theta),\ (0,\ 1),\ \mathbb{O}\}$.
Указание. При вычислении точек данной ЭК воспользоваться следующей таблицей, выражающей степени примитивного элемента в виде многочленов $\varphi(\theta) = \lambda_3\theta^3 + \lambda_2\theta^2 + \lambda_1\theta^1 + \lambda_0$

θ^i	θ^4	θ^5	θ^6	θ^7	θ^8	θ^9	θ^{10}
$\varphi(\theta^i)$	$\theta + 1$	$\theta^2 + \theta$	$\theta^3 + \theta$	$\theta^3 + \theta + 1$	$\theta^2 + 1$	$\theta^3 + \theta$	$\theta^2 + \theta + 1$

θ^i	θ^{11}	θ^{12}	θ^{13}	θ^{14}
$\varphi(\theta^i)$	$\theta^3 + \theta^2 + \theta$	$\theta^3 + \theta^2 + \theta + 1$	$\theta^3 + \theta^2 + 1$	$\theta^3 + 1$

Упражнение 6.33. Найти порядок точки (θ^i, θ^j) из упражнения 6.32.

N	1	2	3	4	5	6	7	8
i	3	5	9	0	5	10	12	6
j	13	11	10	6	3	1	12	8

Пример. Найдем порядок r точки $M_0 = (\theta^3, \theta^8)$
Решение. Так как $\#\mathcal{E} = 16$ (см. упражнение 6.32), то $r \in \{2,\ 4,\ 8,\ 16\}$. Далее при вычислениях будем использовать таблицу

из упражнения 6.32. Поскольку $x_0 = \theta^3 \neq 0$, то $r \neq 2$. Вычислим точку $M_1 = 2M_0 = (x_1,\ y_1)$. Находим

$\lambda = x_0 + \frac{y_0}{x_0} = \theta^3 + \frac{\theta^8}{\theta^3} = \theta^3 + \theta^5 = \theta^3 + \theta^2 + \theta = \theta^1 1.$

И вычисляем

$x_1 = \theta^{22} + \theta^{11} + \theta^4 = \theta^7 + \theta^{11} + \theta^4 = \theta^3 + \theta + 1 + \theta^3 + \theta^2 + \theta + \theta + 1 = \theta^2 + \theta = \theta^5.$

$y_1 = \theta^6 + (\theta^{11} + 1)\theta^5 = \theta^6 + \theta^{16} + \theta^5 = \theta^3 + \theta^2 + \theta + \theta^2 + \theta = \theta^3$

Таким образом, $2M_0 = (\theta^5, \theta^3) \neq -2M_0$, следовательно, $r \neq 4$. Вычислим $4M_0 = 2M_1 = (x_2, y_2)$. Последовательно вычисляем:

$\lambda = x_1 + \frac{y_1}{x_1} = \theta^5 + \frac{\theta^3}{\theta^5} = \theta^5 + \theta^{13} = \theta^2 + \theta + \theta^3 + \theta^2 + 1 = \theta^3 + \theta + 1 = \theta^7,$

$x_2 = \lambda^2 + \lambda + a = \theta^{14} + \theta^7 + \theta^4 = \theta^3 + 1 + \theta^3 + \theta + 1 + \theta + 1 = 1,$

$y_2 = x_1^2 + (\lambda + 1)x_2 = \theta^{10} + (\theta^7 + 1) = \theta^2 + \theta + 1 + \theta^3 + \theta + 1 + 1 = \theta^3 + \theta^2 + 1 = \theta^1 3.$

Таким образом, $8(\theta^3, \theta^8) = (1, \theta^{13}) \neq -8(\theta^3, \theta^8)$.

Следовательно, $r = 16$ и группа данной ЭК — циклическая.

Упражнение 6.34. Найти точку $M = (x, y) = (\theta^i, \theta^j) + (\theta^k, \theta^m)$ группы ЭК из упражнения 8.32.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14
i	0	10	6	0	9	5	6	6	12	6	3	12	1	9
j	13	8	14	6	13	3	8	14	1	14	10	12	6	10
k	6	5	9	10	12	12	10	5	10	10	9	5	6	3
m	14	11	10	1	1	12	1	3	1	1	13	11	8	13

Пример. $M_1 = (\theta^3,\ \theta^{13}), M_2 = (\theta^6,\ \theta^8)$. Найти $M = (x,\ y) = M_1 + M_2$.

По правилам сложения точек находим:

$\lambda = \frac{y_1 + y_2}{x_1 + x_2} = \frac{\theta^{13} + \theta^8}{\theta^3 + \theta^6} = \frac{\theta^3 + \theta^2 + 1 + \theta^2 + 1}{\theta^3 + \theta^3 + \theta^2} = \frac{\theta^3}{\theta^2} = \theta,$

$X = \lambda^2 + \lambda + a + x_1 + x_2 = \theta^2 + \theta + \theta^4 + \theta^3 + \theta^6 = \theta^4 + \theta + 1$

$Y = \lambda(X + x_1) + X + y_1 = \theta(1 + \theta^3) + 1 + \theta^{13} = \theta^{13}$

Таким образом, $M_1 + M_2 = (\theta^3, \theta^{13}) + (\theta^6, \theta^8) = (1, \theta^{13})$.

Упражнение 6.35. Найти разложение в полиномиальном базисе степеней θ^i примитивного элемента θ поля $GF(2^5) = \mathbb{Z}_2[\theta]/(\theta^5 + \theta^2 + 1)$ и значения $Tr(\theta^i)$.

Ответ представлен в следующей таблице:

i	$\alpha_4\theta^4+\alpha_3\theta^3+\alpha_2\theta^2+\alpha_1\theta+\alpha_0$	$Tr(\theta^i)$	i	$\alpha_4\theta^4+\alpha_3\theta^3+\alpha_2\theta^2+\alpha_1\theta+\alpha_0$	$Tr(\theta^i)$
1	θ	0	16	$\theta^4+\theta^3+\theta+1$	0
2	θ^2	0	17	$\theta^4+\theta+1$	1
3	θ^3	1	18	$\theta+1$	1
4	θ^4	0	19	$\theta^2+\theta$	0
5	θ^2+1	1	20	$\theta^3+\theta^2$	1
6	$\theta^3+\theta$	1	21	$\theta^4+\theta^3$	1
7	$\theta^4+\theta^2$	0	22	$\theta^4+\theta^2+1$	1
8	$\theta^3+\theta^2+1$	0	23	$\theta^3+\theta^2+\theta+1$	0
9	$\theta^4+\theta^3+\theta$	1	24	$\theta^4+\theta^3+\theta^2+\theta$	1
10	θ^4+1	1	25	$\theta^4+\theta^3+1$	0
11	$\theta^2+\theta+1$	1	26	$\theta^4+\theta^2+\theta+1$	1
12	$\theta^3+\theta^2+\theta$	1	27	$\theta^3+\theta+1$	0
13	$\theta^4+\theta^3+\theta^2$	1	28	$\theta^4+\theta^2+\theta$	0
14	$\theta^4+\theta^3+\theta^2+1$	0	29	θ^3+1	0
15	$\theta^4+\theta^3+\theta^2+\theta+1$	0	30	$\theta^4+\theta$	0

Упражнение 6.36. Над полем $F=GF(2^5)=\mathbb{Z}[\theta]/(\theta^5+\theta^2+1)$ задана несуперсингулярная кривая $\mathcal{E}: y^2+xy=x^3+ax^2+b$. По $x\in F$ найти точку $M(x,y)\in\mathcal{E}$ и определить порядок этой точки при $a=\sum\limits_{i=0}^{4}\alpha_i\cdot\theta^i,\ b=\sum\limits_{i=0}^{4}\beta_i\cdot\theta^i,\ x=\sum\limits_{i=0}^{4}\gamma_i\cdot\theta^i,\quad \alpha_i,\beta_i,\gamma_i\in\{0,1\}$.

N	$\#\mathcal{E}$	$\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0$	$\beta_4\beta_3\beta_2\beta_1\beta_0$	$\gamma_4\gamma_3\gamma_2\gamma_1\gamma_0$
1	42	01100	10110	01110
2	36	10110	11100	11101
3	40	00010	10010	01101
4	24	11011	10110	00000
5	38	11000	00011	10010
6	30	10001	11000	10101
7	30	10111	11000	10001
8	24	10010	10100	00000
9	38	00011	10001	01010
10	24	11001	10100	10001

Упражнение 6.37. Над полем $F=GF(2^5)=\mathbb{Z}[\theta]/(\theta^5+\theta^2+1)$ задана суперсингулярная кривая $\mathcal{E}: y^2+y=x^3+ax+b$. По $x\in F$ найти точку $M(x,y)\in\mathcal{E}$ и определить её порядок при $a=\sum\limits_{i=0}^{4}\alpha_i\cdot\theta^i,\ b=\sum\limits_{i=0}^{4}\beta_i\cdot\theta^i,\ x=\sum\limits_{i=0}^{4}\gamma_i\cdot\theta^i$.

N	$\#\mathcal{E}$	$\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0$	$\beta_4\beta_3\beta_2\beta_1\beta_0$	$\gamma_4\gamma_3\gamma_2\gamma_1\gamma_0$
1	33	01001	10001	11011
2	25	11100	10100	01111
3	25	11010	00011	00111
4	25	10011	00111	11100
5	41	01010	10110	00101
6	25	10001	01010	10110
7	25	11110	11110	10101
8	41	11000	00001	01001
9	41	01110	00010	10111
10	33	00100	01010	01000

Упражнение 6.38. Для данной ЭК

$$\mathcal{E} : y^2 + xy = x^3 + (\theta + 1)x^2 + 1,$$

$F = \mathbb{Z}_2[\theta]/(\theta^5 + \theta^2 + 1)$ найти точку $M(x, y) \in \mathcal{E},\ M(x,\ y) = (\theta^s,\ \theta^t)$, если $x \in \{\theta^i,\ \theta^j,\ \theta^k\}$.

N	1	2	3	4	5	6	7	8	9	10
i	1	4	7	10	13	16	19	22	25	28
j	2	5	8	11	14	17	20	23	26	29
k	3	6	9	12	15	18	21	24	27	30

Ответ:

N	1	2	3	4	5	6	7	8	9	10
i	3	6	7	12	14	17	19	24	25	28
j	22	3	2	28	22	18	18	0	27	22

Упражнение 6.39. Для каждой из найденных точек из упражнения 6.38 найти её порядок T.

Ответ.

N	1	2	3	4	5	6	7	8	9	10
T	11	11	22	11	22	11	22	11	22	22

Упражнение 6.40. Для данной $\mathcal{E} : y^2 + xy = x^3 + 1$, $F = \mathbb{Z}_2[\theta]/(\theta^5 + \theta^2 + 1)$

1) Определить порядок группы $\mathcal{E}$.
2) Найти точку $M(\theta^k, Y) \in \mathcal{E}$ и определить её порядок T.
3) Найти точку $M_0 = (x_0,\ y_0) = 2M = (\theta^s,\ \theta^t)$.
4) Доказать, что группа $\mathcal{E}$ — циклическая.

N	1	2	3	4	5	6	7	8	9	10
k	1	2	4	5	8	9	10	11	13	15

N	11	12	13	14	15	16	17	18	19	20
k	16	18	20	21	22	23	26	27	29	30

Ответ.

N	1	2	3	4	5	6	7	8	9	10
T	11	11	11	44	11	44	44	44	44	22
N	11	12	13	14	15	16	17	18	19	20
T	11	44	44	44	44	22	44	22	22	22

Пример. Пусть $k = 21,$ и $x = \theta$.
Решение.

1) По теореме Хассе-Вейля $\#\mathcal{E} = 44$.

2) В уравнении ЭК делаем замену $y = zx = z\theta,\ x = \theta,\ \theta^2 z^2 + \theta^2 z = \theta^3 + 1$.

   После преобразования, используя таблицу из упражнения 6.35, получим:

   $z^2 + z = \frac{\theta^3+1}{\theta^2} = \theta + \frac{1}{\theta^2} = \theta + \theta^{29} = \theta^3 + \theta + 1 = \theta^{27}$

   Так как $Tr(\theta^{27}) = 0$, то это уравнение разрешимо. Находим, снова используя таблицу из упражнения 6.35,
   $z_0 = (\theta^{27})^{2^1} + (\theta^{27})^{2^3} = \theta^{23} + \theta^{30} =$ {см.таблицу из упражнения 6.35} $= \theta^3 + \theta^2 + \theta + 1 + \theta^4 + \theta = \theta^4 + \theta^3 + \theta^2 + 1 = \theta^{14}$.

   Следовательно, $y_0 = z_0\theta = \theta^{15}$ и искомая точка $M_0 = (\theta,\ \theta^{15})$.
   Второе решение $M_1 = (x_0,\ y_0 + x_0) = (\theta,\ \theta + \theta^{15}) = (\theta,\ \theta^{14})$.

   Найдем порядок точки $M_0 = (\theta,\ \theta^{15})$.
   Для этого найдем λ из уравнения $\lambda^2 + \lambda = \theta$:

   $$\lambda = \theta^{2^1} + \theta^{2^3} = \theta^2 + \theta^8 = \theta^3 + 1 = \theta^{29}.$$

   Далее, проверяем условия $Tr(x) = Tr(y) = Tr(\lambda y)$.

   $$Tr(\theta) = Tr(\theta^{15}) = Tr(\theta^{30}) = 0.$$

   Следовательно, $\mathrm{ord}(\theta,\ \theta^{15}) = 11$

Упражнение 6.41. Пусть $\mathcal{E}_\sigma : y^2 + xy = x^3 + 1 + \sigma x^2,\ \sigma = 0, 1$ над полем $GF(2^7) = \mathbb{Z}_2[\theta]/(\theta^7 + \theta + 1)$.

1) Найти порядок группы $\mathcal{E}_\sigma$.

2) Для данного $x = \sum_{i=1}^{n} \alpha_i \cdot \theta^i$ найти точку $M(x,\ y) \in \mathcal{E}_\sigma, \sigma \in \{0, 1\}$.

3) Определить, является ли эта точка удвоенной или учетверенной.

$\sigma = 0$

N	$\alpha_6\alpha_5\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0$
1	0001100
2	0110000
3	0101000
4	1010000
5	0100010
6	0011110
7	0100011
8	0001111
9	1110011
10	1001001

$\sigma = 1$

N	$\alpha_6\alpha_5\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0$
1	0011000
2	0001010
3	1000011
4	1000110
5	1111000
6	1100101
7	0000101
8	0000110
9	1010000
10	0111100
11	0000011

Замечание 1. При вычислениях воспользоваться следующей таблицей значения следов элементов θ^j:

Таблица значения следов элементов $\theta^j = \sum_{i=0}^{6} \alpha_i \cdot \theta^i \in GF(2^7)$:

j	$Tr(\theta^j)$	$\alpha_6\alpha_5\ldots\alpha_0$	j	$Tr(\theta^j)$	$\alpha_6\alpha_5\ldots\alpha_0$	j	$Tr(\theta^j)$	$\alpha_6\alpha_5\ldots\alpha_0$
1	0	0000010	43	1	0101001	85	1	1101101
2	0	0000100	44	0	1010010	86	1	1011001
3	0	0001000	45	1	0100111	87	1	0110001
4	0	0010000	46	0	1001110	88	0	1100010
5	0	0100000	47	1	0011111	89	1	1000111
6	0	1000000	48	0	0111110	90	1	0001101
7	1	0000011	49	0	1111100	91	0	0011010
8	0	0000110	50	1	1111011	92	0	0110100
9	0	0001100	51	1	1110101	93	0	1101000
10	0	0011000	52	1	1101001	94	1	1010011
11	0	0110000	53	1	1010001	95	1	0100101
12	0	1100000	54	1	0100001	96	0	1001010
13	1	1000011	55	0	1000010	97	1	0010111
14	1	0000101	56	1	0000111	98	0	0101110
15	0	0001010	57	0	0001110	99	0	1011100
16	0	0010100	58	0	0011100	100	1	0111011
17	0	0101000	59	0	0111000	101	0	1110110
18	0	1010000	60	0	1110000	102	1	1101111
19	1	0100011	61	1	1100011	103	1	1011101
20	0	1000110	62	1	1000101	104	1	0111001
21	1	0001111	63	1	0001001	105	0	1110010
22	0	0011110	64	0	0010010	106	1	1100111
23	0	0111100	65	0	0100100	107	1	1001101
24	0	1111000	66	0	1001000	108	1	0011001
25	1	1110011	67	1	0010011	109	0	0110010
26	1	1100101	68	0	0100110	110	0	1100100
27	1	1001001	69	0	1001100	111	1	1001011
28	1	0010001	70	1	0011011	112	1	0010101
29	0	0100010	71	0	0110110	113	0	0101010
30	0	1000100	72	0	1101100	114	0	1010100
31	1	0001011	73	1	1011011	115	1	0101011
32	0	0010110	74	1	0110101	116	0	1010110
33	0	0101100	75	0	1101010	117	1	0101111
34	0	1011000	76	1	1010111	118	0	1011110
35	1	0110011	77	1	0101101	119	1	0111111
36	0	1100110	78	0	1011010	120	0	1111110
37	1	1001111	79	1	0110111	121	1	1111111
38	1	0011101	80	0	1101110	122	1	1111101
39	0	0111010	81	1	1011111	123	1	1111001
40	0	1110100	82	1	0111101	124	1	1110001
41	1	1101011	83	0	1111010	125	1	1100001
42	1	1010101	84	1	1110111	126	1	1000001

Задача 6.42. Пусть $\mathcal{E} : y^2 + y = x^3$ над полем $GF(2^n)$. Доказать, что $\#\mathcal{E} = 2^n + 1$.

Задача 6.43. Пусть $\mathcal{E} : y^2 + y = x^3 + x$ над полем $GF(2^n)$. Доказать, что

$$\#\mathcal{E} = \begin{cases} 2^n + 1 + 2^{\frac{n+1}{2}}, & n = \pm 1 \pmod 8, \\ 2^n + 1 - 2^{\frac{n+1}{2}}, & n = \pm 3 \pmod 8. \end{cases}$$

Задача 6.44. Пусть $\mathcal{E} : y^2 + y = x^3 + x + 1$ над полем $GF(2^n)$. Доказать, что

$$\#\mathcal{E} = \begin{cases} 2^n + 1 - 2^{\frac{n+1}{2}}, & n = \pm 1 \pmod 8, \\ 2^n + 1 + 2^{\frac{n+1}{2}}, & n = \pm 3 \pmod 8. \end{cases}$$

Задача 6.45. Пусть $\mathcal{E} : y^2 + y = x^3 + x + 1$ над полем $GF(2^n)$. Доказать, что

$$2(x_0,\ y_0) = (x_0^4 + 1,\ x_0^4 + y_0^4).$$

Задача 6.46. Пусть $\mathcal{E} : y^2 + y = x^3 + x + b$ над полем $GF(2^n),\ n > 1$ и $\mathcal{P} = (x_0,\ y_0) \in \mathcal{E},\ x_0 \neq 0$ и $2\mathcal{P} = (X,\ Y)$. Доказать, что

$$X = x_0^2 + \frac{b}{x_0^2}.$$

Задача 6.47. Пусть $\mathcal{E}$ — ЭК из задачи 6.46 и $\mathcal{P}_1 = (x_1,\ y_1) \in \mathcal{E},\ \mathcal{P}_2 = (x_2,\ y_2) \in \mathcal{E},\ x_1 \neq x_2$ и $\mathcal{P}_1 + \mathcal{P}_2 = (x_3,\ y_3)$. Доказать, что

$$x_3 = \frac{x_2 y_1 + x_1 y_2 + x_1 x_2^2 + x_2 x_1^2}{(x_1 + x_2)^2}.$$

Задача 6.48. Доказать, что число решений сравнения $y^2 + xy = x^3 + ax^2$ при $(a \neq 0)$ над полем $GF(2^{2k+1})$ равно $2^{2k+1} + 1$.

Задача 6.49. Доказать без использования теоремы Хассе–Вейля, что

$$\#\mathcal{E} = 2^n + 1,$$

где $\mathcal{E} : y^2 + y = x^3 + 1,$ над $GF(2^{2k+1})$.

7. Криптографические приложения

Кольцо вычетов $\mathbb{Z}_n$ используется, например, в следующих криптографических приложениях:

- схема Диффи-Хеллмана — открытое распределение секретных ключей,
- криптосистема и схема ЭЦП Эль-Гамаля,
- криптосистема RSA,
- схема разделения секрета.

7.1. Схема Диффи-Хеллмана

В кольце $\mathbb{Z}_p$, p — простое, выбирается первообразный корень (примитивный элемент) g: $\operatorname{ord}(g) = p - 1$. Параметры g и p общедоступны.

Участник $A_\alpha,\ \alpha \in \{0, 1\}$ выбирает случайное $X_\alpha \in_{\mathbb{R}} \mathbb{Z}_{p-1}$ и вычисляет $Y_\alpha \equiv g^{X_\alpha} \pmod p$. Числа Y_0 и Y_1 — публичные.

Для формирования общего ключа K участник A_α вычисляет $K_\alpha = Y_{\bar{\alpha}}^{X_\alpha} = (g^{X_{\bar{\alpha}}})^{X_\alpha} = g^{X_{\bar{\alpha}} X_\alpha} \pmod p$. Очевидно, что $K_0 = K_1$.

Пример: Пусть $p = 83, g = 2, X_0 = 37, X_1 = 53$. Тогда $Y_0 = 57, Y_1 = 54$. $K_0 = Y_1^{X_0} = 54^{37} \pmod{83} = 24 \equiv K_1 \equiv Y_0^{X_1} \equiv 57^{53} \pmod{83}$ — общий ключ A_0 и A_1.

Замечание. Стойкость этой схемы основана на сложности решения задачи дискретного логарифмирования.

Упражнение 7.1. Для данных параметров схемы Диффи-Хеллмана выполнить все вычисления.

N	1	2	3	4	5	6	7	8
p	61	67	71	73	79	83	89	97
g_0	2	2	7	5	3	2	3	5
x_0	30	31	32	33	34	35	36	37
x_1	50	51	52	53	54	55	56	57

N	9	10	11	12	13	14	15	
p	101	103	109	113	127	131	137	
g_0	2	5	6	3	3	2	3	
x_0	38	39	40	41	42	43	44	
x_1	58	59	60	61	62	63	64	

7.2. Криптосистема Эль-Гамаля

Все вычисления в кольце $\mathbb{Z}_p$, p — простое, g — первообразный корень.

Каждый участник A_i выбирает секретное число $X_i \in_{\mathbb{R}} \mathbb{Z}_{p-1}$ и публикует открытый ключ $Y_i \equiv g^{X_i} \pmod p$. Если A_0 желает послать секретное сообщение $M \in \mathbb{Z}_p$ участнику A_1, то он выбирает сеансовый секретный ключ $r_0 \in_{\mathbb{R}} \mathbb{Z}_{p-1}$, вычисляет $Y_0 \equiv g^{r_0} \pmod p$, шифрующий множитель $T \equiv Y_1^{r_0} \equiv g^{r_0 X_1} \pmod p$, и шифрует сообщение:

$$M_{\text{Ш}} \equiv T \cdot M \pmod p.$$

По открытому каналу участник A_0 посылает пару $(Y_0, M_{\text{Ш}})$. Участник A_1 вычисляет $T^{-1} = Y_0^{-X_1} \equiv g^{-r_0 X_1} \pmod p$ и расшифровывает $M_{\text{Ш}} : M = T^{-1} M_{\text{Ш}} = M$.

Пример. Пусть $p = 89$, $g = 3$, $M = 27$, $r_0 = 32$, $Y_0 \equiv 3^{32} \pmod{89} = 4$, $X_1 = 43$, $Y_1 = 3^{43} \pmod{89} = 59$.

Решение. *Шифрование сообщения* $M = 27$:
Вычисляем шифрующий множитель

$$T = Y_1^{r_0} = 59^{32} \pmod{89} \equiv 67.$$

Шифруем сообщение M :

$$M_{\text{Ш}} \equiv T \cdot M = 67 \cdot 27 \pmod{89} \equiv 29.$$

Расшифрование $(Y_0, M_{\text{Ш}}) = (4, 29)$*:*
Вычисляем $T^{-1} \equiv Y_0^{-X_1} = 4^{-43} \pmod{89} \equiv 4$.
Следовательно, $M = T^{-1} \cdot M_{\text{Ш}} = 4 \cdot 29 \pmod{89} \equiv 27$.

Упражнение 7.2. Для заданных параметров криптосистемы Эль-Гамаля выполнить все вычисления.

N	1	2	3	4	5	6	7	8
p	109	113	127	131	137	139	149	151
g	6	3	3	2	3	2	2	6
x_0	21	22	23	24	25	26	27	28
x_1	51	52	53	54	55	56	57	58
r_0	11	12	13	14	15	16	17	18
M	71	72	73	74	75	76	77	78

N	9	10	11	12	13	14	15	
p	157	163	167	173	179	181	191	
g	5	2	5	2	2	2	19	
x_0	29	30	31	32	33	34	35	
x_1	59	60	61	62	63	64	65	
r_0	19	20	21	22	23	24	25	
M	79	80	81	82	83	84	85	

7.3. Схема подписи Эль-Гамаля

Вычисления, как и в предыдущих схемах, производятся в кольце $\mathbb{Z}_p$, g — первообразный корень.

Пусть участник A — подписывающий сообщение $M \in \mathbb{Z}_p$, B — проверяющий. Параметры протокола: $X \in_{\mathbb{R}} \mathbb{Z}_{p-1}$ — секретный ключ, $Y \equiv g^{-X} \pmod p$ — открытый ключ участника A, r — сеансовый секретный ключ, НОД$(r, p-1) = 1$.

Для формирования подписи под сообщением M участник A последовательно вычисляет $s \equiv g^r \pmod p$, $z = [M + sX]r^{-1} \pmod{p-1}$.

Пара $(z, s) \equiv SIG(M)$ — подпись под сообщением M. Сообщение M с подписью $SIG(M)$ посылается участнику A_1. Для проверки подписи участник A_1 вычисляет величины:

$$u \equiv g^M \pmod p, \qquad V \equiv Y^s \cdot s^z \pmod p$$

Если $u \equiv V \pmod p$, то подпись принимается. В противном случае — отвергается.

Пример. $\mathbb{Z}_p = \mathbb{Z}_{97}$, $g = 5$.
Формирование подписи:

$$X = 19,\ Y = 23,\ r = 37,\ s = 56,\ M = 40,$$
$$r^{-1} \equiv 37^{-1} \pmod{96} = 13.$$
$$z = [40 + 56 \cdot 19] \cdot 13 \pmod{96} = 48$$
$$SIG(40) = (48, 56)$$

Проверка подписи:

$$u \equiv 5^{40} \equiv 16 \pmod{97},$$
$$V \equiv 23^{56} \cdot 56^{48} \pmod{97} = 81 \cdot (-1) \equiv -81 \equiv 16 \pmod{97} = u.$$

Упражнение 7.3. Для заданных параметров схемы подписи Эль-Гамаля выполнить все вычисления.

N	1	2	3	4	5	6	7	8
x	30	31	32	33	34	35	36	37
r	17	19	23	29	20	25	31	35
M	70	71	72	73	74	75	76	77
p	191	193	197	211	223	227	229	233
g	19	5	2	2	3	2	6	3

N	9	10	11	12	13	14	15	
x	38	39	40	41	42	43	44	
r	39	23	19	17	29	31	37	
M	78	79	80	81	82	83	84	
p	239	241	251	257	263	269	271	
g	7	7	6	3	5	2	6	

7.4. Схема подписи RSA

Исходные параметры $n = p \cdot q,\ e,\ d$. Секретные параметры подписывающего — d, p, q.

Открытые параметры: n, e и хэш-функция $h : \{0,1\}^* \to \{0,1\}^m$, где $2^m \geqslant n$.

Формирование подписи по сообщению M:

1) $H = h(M)$,
2) $SIG(M) = H^d \pmod{n}$,
3) Пара $[SIG(M), M]$ посылается проверяющему участнику.

Проверка подписи:

1) $H = h(M)$,
2) $[SIG(M)]^e = H_1 \pmod{n}$,
3) Если $H_1 \equiv H \pmod{n}$, то подпись принимается, иначе отвергается.

Теорема 7. *Пусть $p \neq q,\ p, q$ — простые, $n = p \cdot q$. Тогда для $\forall x \in \mathbb{Z}$ и $\forall k \in \mathbb{Z}$*

$$x^{1+k(p-1)(q-1)} \equiv x \pmod{n}.$$

На этой теореме основано обоснование однозначного расшифрования в криптосистеме RSA.

В криптосистеме RSA заданы $n = p \cdot q,\ p \neq q$ — простые.
Заданы e и d такие, что $e \cdot d \equiv 1 \pmod{\varphi(n)} = (p-1)(q-1)$.
Секретные параметры p, q и d. Открытые параметры n и e.

Шифрование: $E(x) = Y \equiv x^e \pmod{n},\ x \in \mathbb{Z}$.
Расшифрование: $D(Y) = Y^d \pmod{n}$.

Пример. $n = 31 \cdot 17 = 527,\ x \in 100,\ e = 23,\ d \equiv 23^{-1} \pmod{480} \equiv 167$.

Шифрование:

$$Y = E(100) \equiv 100^{23} \pmod{527} \equiv 100^{16} \cdot 100^4 \cdot 100^2 \cdot 100^1 \pmod{527}.$$

Промежуточные вычисления:

$$100^2 \equiv -13 \pmod{527},\ 100^4 \pmod{527} \equiv 169,$$
$$100^8 \equiv 103 \pmod{527},\ 100^{16} \pmod{527} \equiv 69.$$

Поэтому, $Y = 69 \cdot 169 \cdot (-13) \cdot 100 \equiv 382 \pmod{527}$.

Расшифрование:

$$D(382) = 382^{167} = 382^{128} \cdot 382^{32} \cdot 382^4 \cdot 382^2 \cdot 382^1 \pmod{527}.$$

Промежуточные вычисления:

$382^2 = 472 \pmod{527}$, $382^4 = 390 \pmod{527}$, $382^8 = 324 \pmod{527}$,
$382^{16} = 103 \pmod{527}$, $382^{32} = 69 \pmod{527}$, $382^{64} = 18 \pmod{527}$,
$382^{128} = 324 \pmod{527}$.

Следовательно,

$$D(Y) = D(382) = 324 \cdot 69 \cdot 390 \cdot 472 \cdot 382 \equiv 100 \pmod{527}.$$

Упражнение 7.4. Для данных p, q и e в криптосистеме RSA найти секретный ключ d и зашифровать на нем сообщение M.

N	1	2	3	4	5	6	7	8	9	10
p	31	31	31	37	37	37	37	37	41	41
q	59	61	53	43	47	53	59	61	43	47
e	19	13	17	23	19	17	31	29	17	19
M	7	10	12	14	16	18	20	22	24	26

N	11	12	13	14	15	16	17	18	19	20
p	41	41	41	43	43	43	43	47	47	47
q	53	59	61	47	53	59	61	53	59	61
e	29	13	17	31	29	19	17	19	13	31
M	28	30	32	34	36	38	40	42	44	46

Упражнение 7.5. Найти e (открытый ключ) и d (секретный ключ) для криптосистемы RSA при данных p и q.

N	1	2	3	4	5	6	7	8
p	31	41	37	43	47	53	59	31
q	67	47	53	61	59	41	37	61

N	9	10	11	12	13	14	15	16
p	41	37	43	47	53	59	61	67
q	59	59	47	61	47	43	31	41

Упражнение 7.6. Используя криптосистему RSA, зашифровать сообщение M от имени абонента владельца секретного ключа d. Найти открытый ключ e и расшифровать это сообщение. Параметры RSA: $n = 1247,\ d = 821$.

N	1	2	3	4	5	6	7	8
M	ОЙ	РЕ	МИ	ДА	СИ	ЛЯ	ДО	АЙ

Кодирование алфавита приведено в следующей таблице:

А	00000	И	01000	Р	10000	Ш	11000
Б	00001	Й	01001	С	10001	Щ	11001
В	00010	К	01010	Т	10010	Ъ	11010
Г	00011	Л	01011	У	10011	Ы	11011
Д	00100	М	01100	Ф	10100	Ь	11100
Е	00101	Н	01101	Х	10101	Э	11101
Ж	00110	О	01110	Ц	10110	Ю	11110
З	00111	П	01111	Ч	10111	Я	11111

Таблица. Коды букв русского алфавита

Упражнение 7.7. Используя криптосистему RSA, зашифровать сообщение M. Открытый ключ $e = 121,\ n = 1247$. Результат представить в виде русского слова, заменив коды по таблице из упражнения 7.6.

N	1	2	3	4	5	6	7	8
M	67	257	321	367	171	298	191	197

Упражнение 7.8. Проверить подпись s под сообщением M, если известно, что подпись сформирована ЭЦП RSA с хэш-функцией h *(См. Описание хэш-функции)*. Для представления сообщения в виде числа использовать таблицу из упражнения 7.6. Параметры RSA: $n = 1247,\ e = 53$.

N	1	2	3	4	5
s	49	1235	60	563	710
M	БРАТ	МАМА	ПАПА	ПИЛА	МАМА

Упражнение 7.9. Используя ЭЦП RSA с хэш-функцией h *(см. Описание хэш-функции)*, сформировать подпись под сообщением M. Параметры RSA: $n = 1247,\ d = 25$.

N	1	2	3	4	5
M	ПАПА	МАМА	БРАТ	ПИЛА	ГРАД

7.9. Схема ЭЦП Рабина

1) Исходные параметры и обозначения.

   - p, q - различные простые числа, равные либо $3 \pmod 4$, либо $5 \pmod 8$, секретные;
   - $n = p \cdot q$ - модуль вычислений, публикуется;
   - k — минимальное целое, такое что $2^k \geqslant n$;
   - хэш-функция $h : \{0,1\}^k \to \{0,1\}^r$, $r < k$, $k - r = t$;
   - $\widetilde{a} = \alpha_0 ... \alpha_m$ - двоичный набор, $a = \sum_{i=0}^{m} \alpha_i 2^i$.

2) Алгоритм формирования подписи под сообщением $\widetilde{M}$.

   а) Вычислим $h(\widetilde{M}) = \widetilde{H}$

   б) Выбираем $\widetilde{\beta} \in_R \{0,1\}^t$

   в) Формируем $\widetilde{C} = \widetilde{H} \,||\, \widetilde{\beta}$ и находим C.

   г) Вычисляем $\sigma = \left(\dfrac{C}{p}\right) + \left(\dfrac{C}{q}\right)$ и проверяем условие $\sigma = 2$. Если $\sigma \neq 2$, то переходим к пункту 2.

   д) Решаем сравнение

   $$x^2 \equiv C \pmod{n = p \cdot q} \tag{50}$$

   Напомним, что это сравнение равносильно системе

   $$\begin{cases} x^2 \equiv C \pmod p \\ x^2 \equiv C \pmod q \end{cases}$$

   Решаем эту систему и по К.Т.О. находим четыре решения сравнения (50).

   е) Выбираем любое решение x_0 и формируем подпись

   $$SIG(\widetilde{M}) = (\widetilde{x_0}||\widetilde{\beta})$$

3) Проверка подписи.

а) На основе полученной пары $(\widetilde{M}, SIG(\widetilde{M}))$ вычисляем $h(\widetilde{M}) = \widetilde{H_1}$

б) Формируем $\widetilde{C_1} = \widetilde{H_1} \,||\, \widetilde{\beta}$ и определяем C_1 и x_0.

в) Вычисляем $C_2 = x_0^2 \pmod{n}$.

г) Проверяем условие $C_1 \equiv C_2 \pmod{n}$. Если оно выполняется, то подпись принимается, в противном случае подпись отвергается.

Упражнение 7.12. При данных $p = 23,\ q = 89,\ n = 2047$ сформировать подпись под сообщением M, при $k = 11$, $r = 5$, $t = 6$. Буквы кодируются согласно таблице из упражнения 7.6. Если $M = A_1...A_s$ - сообщение, $\widetilde{A_i}$ - код буквы A_i, то $h(\widetilde{M}) = \bigoplus_{i=1}^{s} \widetilde{A_i}$.

N	1	2	3	4	5	6	7	8	9	10
M	СТЕК	КОШИ	БЛИН	СТУК	КУСТ	РОСТ	ПОСТ	СВЕТ	УРОК	КЛИН
N	11	12	13	14	15	16	17	18	19	20
M	КЛОН	ПЛОТ	ТОРТ	ФИНТ	ФАНТ	ФРАК	ШАРМ	РАМА	МАМА	ПАПА

Пример. Пусть $M =$ ШИФР.

1) Составляем $\widetilde{M} = 11000\ 01000\ 10100\ 10000$
и вычисляем $h(\widetilde{M}) = (11000) \oplus (01000) \oplus (10100) \oplus (10000) = 10100$.

2) Возьмем $\widetilde{\beta} = 100101 \in_R \{0,1\}^6$.

3) Формируем $\widetilde{C} = 10100100101$ и находим $C = 2^{10} + 2^8 + 2^5 + 2^2 + 1 = 1317$.

4) Вычисляем $\sigma = \left(\frac{1317}{23}\right) + \left(\frac{1317}{89}\right) = 1 + 1 = 2$.

5) Решаем сравнение $x^2 \equiv 1317 \pmod{2047}$. Это сравнение равносильно системе

$$\begin{cases} x^2 \equiv 6 \pmod{23}, x = \pm 11 \\ x^2 \equiv 71 \pmod{89}, x = \pm 31 \end{cases}$$

По К.Т.О. находим

$$X = [\pm 11 \cdot 89 \cdot (89^{-1} \pmod{23}) \pm 31 \cdot 23 \cdot (23^{-1} \pmod{89})] \pmod{2047}$$

Окончательно получим $x_1 = \pm 58$, $x_2 = \pm 770$.

6) Положим $x_0 = 58$ и сформируем подпись:
SIG(ШИФР) $= (58 \parallel 37) = (00000\ 111010 \parallel 100101)$.

7.5. Описание хэш-функции h_8

Определим хэш-функцию $h_8(M)$ следующим образом. Представим сообщение M в виде двоичной строки. Для этого заменим каждую букву сообщения на двоичную строку длины 5 по таблице кодов букв русского алфавита.

Вычислим $H = M + \underbrace{11\ldots1}_{k}$. Обозначим через H_8 первые 8 бит H. Тогда

$$h_8(M) = H_8^2 \pmod{2^8},$$

если $h_8(M) = 0$, то положить $h_8(M) = 17$.

Пример. Вычислим хэш-значение h_8 от слова СЛОН.

Решение.

1) Представляем слово в виде двоичной строки. СЛОН = 10001 01011 01110 01101,

2) Вычисляем сумму СЛОН = 10001 01011 01110 01101 + 11111 11111 11111 11111 = 1 10001 01011 01110 01100,

3) Берем первые 8 бит и вычисляем $H_8 = 11000101$,

4) Переводим H_8 в десятичный вид $H_8 = 197$,

5) Вычисляем $h_8(\text{СЛОН}) = H_8^2 \mod 2^8 = 197^2 \mod 256 = 38809 \mod 256 = 153 = 10011001$.

Итак, $h_8(\text{СЛОН}) = 10011001 = 153$.

7.6. Модулярная схема разделения секрета

Каждый из n участников (n, t)-пороговой схемы имеет свой модуль вычисляя $m_i = 2^k + \sum_{i=0}^{k-1} \alpha_{ij} 2^j$, $i = \overline{1,n}$, $m_i < m_{i+1}$, $i = \overline{1,n-1}$ НОД$(m_i, m_j) = 1, i \neq j$

Обозначим за t - порог $(1 < t < n)$, тогда общий секрет S удовлетворяет условию

$$m_{n-t+1} \dots m_n < S < m_1 \cdot m_2 \cdot \ldots \cdot m_t$$

Частичный секрет $s_i \equiv S \pmod{m_i},\ i = \overline{1,t}$

Для определения общего секрета группа из t участников на основе китайской теоремы об остатках определяет общий секрет решая систему

$$\begin{cases} x_{i_1} \equiv s_{i_1} \pmod{m_{i_1}} \\ \quad \vdots \\ x_{i_t} \equiv s_{i_t} \pmod{m_{i_t}} \end{cases}$$

Решением этой системы будет общий секрет S.

Упражнение 7.10. Определить общий секрет по частичным секретам в пороговой $(10, 3)$ схеме

N	1	2	3	4	5	6	7	8
m_1	67	79	83	89	97	101	103	107
m_2	103	89	67	109	71	71	97	89
m_3	71	109	101	107	103	83	67	71
s_1	39	40	8	21	83	89	68	73
s_2	62	19	27	95	66	67	85	25
s_3	62	93	86	64	66	11	31	69

N	9	10	11	12	13	14	15	16
m_1	109	79	83	89	97	101	107	103
m_2	83	71	79	107	101	67	79	71
m_3	73	109	107	67	73	89	83	97
s_1	100	58	51	73	24	79	51	46
s_2	14	57	59	47	78	41	64	62
s_3	36	83	46	39	8	75	56	26

7.7. Интерполяционная схема разделения секрета

Общий секрет S — свободный член секретного многочлена над полем $\mathbb{Z}_p$:

$$f(x) = x^{t-1} + a_{t-2}x^{t-2} + \ldots + a_1 x + S$$

Каждый участник протокола имеет открытый параметр $x_i \in \mathbb{Z}_p,\ x_i \neq x_j,\ i,j = \overline{1,n}$ и частный секрет $s_i = f(x_i)$.

Любые t участников, объединив свои секреты, вычисляют общий секрет S по интерполяционной формуле Лагранжа:

$$S = (-1)^{t-1} \sum_{i=1}^{t} s_i \prod_{j \neq i} \frac{a_j}{a_i - a_j}$$

Упражнение 7.11. В интерполяционной $(n, 3)$ схеме разделения секрета вычислить общий секрет. Вычисления проводить в поле $\mathbb{Z}_{41}$

N	1	2	3	4	5	6	7	8
s_1	10	12	14	16	18	19	8	6
s_2	10	17	1	5	8	9	19	18
s_3	19	4	14	30	19	20	15	14
x_1	1	3	5	7	9	11	13	15
x_2	3	10	20	13	35	4	31	21
x_3	8	20	7	22	17	20	4	33

N	9	10	11	12	13	14	15	16
s_1	4	5	7	23	19	24	25	
s_2	11	20	18	2	3	4	19	
s_3	8	3	30	39	3	9	36	
x_1	17	19	20	4	6	8	10	
x_2	6	20	8	17	20	12	19	
x_3	10	3	14	20	23	25	36	

7.8. Шифр гаммирования

Напомним, что при гаммировании открытый текст — это двоичная последовательность, ключ — двоичная последовательность длины не менее длины открытого текста. Шифрование — побитовое сложение ключа и открытого текста. Расшифрование — побитовое сложение шифртекста и ключа.

Упражнение 10. Поточный шифр (шифр гаммирования) задан ЛРП с характеристическоим многочленом f, $\sigma = 0,1$ $f_0 = x^6 + x + 1, f_1 = x^6 + x^5 + 1$ над полем $GF(2)$. секретный ключ — начальное заполнение $\widetilde{k} = (\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ задается числом $K = \sum_{i=0}^{5} \alpha_i \cdot 2^i$. Буквы русского алфавита кодируются по таблице кодов букв русского алфавита (таблица из упражнения 7.6). На основе этой таблицы сформировать двоичную последовательность $\widetilde{M}$ соответствующего заданному тексту M и зашифровать двоичной гаммой на основе ЛРП с данным начальным дополнением. Ответ предоставить в буквенном виде.

Пример 5. Пусть ЛРП задана характеристическим многочленом $f(x) = x^4 + x + 1, \widetilde{x} = 0101$ и $M =$ ШИФР. 1. Согласно кодовой таблице из упражнения 7.6: $\widetilde{M} =$11000 01000 10100 10000.

2. Характеристическое уравнение ЛРП: $x_{i+1} = x_{i-3} + x_{i-4}, i = 4, 5, \ldots$

3. Для $\widetilde{k} = 0101$ получаем следующую гамму $\widetilde{\Gamma}$ для шифрования: 01011 11000 10011 01011 $= \widetilde{\Gamma}$

4. Шифруем: $\widetilde{T} = \widetilde{M} \oplus \widetilde{\Gamma}$

11000 01000 10100 10000

01011 11000 10011 01011

10011 10000 00111 11011

5. По кодовой таблице находим шифртекст в буквенном виде.

Ответ $T =$УРЗЫ.

N	K	M
1	19	АПТЕКАРСКИЙГОРОДОК
2	27	НАСТЯБЕСПАЛОВА
3	47	КРИПТОГРАФИЯ
4	38	ИЗМАЙЛОВСКИЙПАРК
5	47	ПЕРМСКИЙКРАЙ
6	62	КАСПЕРСКИЙХАКЕР
7	37	ГОРААРАРАТ
8	51	АСТАНАСТОЛИЦА
9	41	ЭСТОНИЯЕВРОПА
10	29	РОССИЙСКИЙГОСТ
11	40	НИЖНЕВАРТОВСК
12	25	ПРОСТАЯЗАМЕНА
13	30	КУЗМИНКИПАРК
14	56	ШИФРВЕРНАМА
15	18	МАТЕМАТИКАСОЛЬ
16	52	ГОРЯЧИЕКЛЮЧИ
17	23	НАБЕРЕЖНЫЕЧЕЛНЫ
18	44	КАПИТАНСКАЯДОЧКА
19	48	ЦЕНТРБЕЗОПАСНОСТИ

Таблица 2. Текст для шифрования.

7.10. Криптоалгоритмы на эллиптических кривых

Задача 7.13.

1. $\mathcal{E} : y^2 = x^3 - 3x \pmod{101}$

2. Проверить что $\mathcal{P} = (x_0, y_0) \in \mathcal{E}$ и $\mathrm{ord}(\mathcal{P}) = 61 \Rightarrow \#\mathcal{E} = 122$

3. Провести все вычисления по алгоритму ЭЦП Эль-Гамаля для данных параметров d, K, H.

N	x_0	y_0	d	K	H
1	4	31	17	31	71
2	5	3	19	42	75
3	6	20	23	37	77
4	9	46	11	25	79
5	13	21	29	13	81
6	14	50	34	53	82
7	17	32	41	19	85
8	22	49	45	29	93
9	24	4	20	49	97
10	25	20	30	54	95
11	31	2	51	15	88
12	33	36	47	10	98
13	36	47	14	59	99
14	-14	5	25	43	70
15	-13	8	38	55	90
16	-9	45	13	47	78
17	-12	5	39	44	92
18	-6	2	37	58	82
19	-4	7	40	28	73
20	-5	30	53	24	98

Протокол ЭЦП Эль-Гамаля(ГОСТ) на ЭК

Задана ЭК Порядка N и точка $\mathcal{P}$, $\mathrm{ord}(\mathcal{P}) = q, \quad q|N, \ q$ — простое. Задана хэш-функция $h : \{0,1\}^* \longrightarrow \{0,1\}^m, \quad 2^m > q$.

$Q = d\mathcal{P} = (x_Q, y_Q)$ — долговременный открытый ключ, d — секретный, $C = k\mathcal{P}$ — открытый сеансовый ключ, F — сеансовый секретный ключ.

Формирование подписи под сообщением M.

1. $h(M) = H, \quad H \equiv e \pmod q$
2. $C = k\mathcal{P} = (x_C, y_C), \quad x_C \equiv r \pmod q$
3. $rd + ke \equiv s \pmod q$
4. $(r, s) = sig(M)$.

Проверка подписи.

На основе M и $sig(M)$ вычисляем:

1. $h(M) = H, \quad H \equiv e_1 \pmod q$
2. $e^{-1}s \equiv z_1 \pmod q, \quad -re^{-1} \equiv z_2 \pmod q$
3. $C(x_1, y_1) = z_1\mathcal{P} + z_2\mathcal{Q}$
4. $x_1 \equiv r_1 \pmod q$
5. Проверка $r_1 \equiv r \pmod q$

Упражнение 7.14. Задана $\mathcal{E} : y^2 + xy = x^3 + x^2 + 1$, над полем $GF(2^7) = \mathbb{Z}_2[\theta]/(\theta^7 + \theta + 1)$. Заданы d, k, H.

1) Для данного $x = \theta^i$ найти $M(x, y) \in \mathcal{E}$.

2) Определить порядок $\#\mathcal{E}$ и порядок точки M

3) На основе M найти точку $C \in \mathcal{E}$ такую, что $\mathrm{ord}(C) = q, \quad q$ — простое, $q > 2$.

4) Провести все вычисления по протоколу ЭЦП Эль Гамаля с данными параметрами d, k, H.

Замечание 1. Элементу $a = \sum_{i=0}^{6} \alpha_i \cdot \theta^i \in GF(2^7)$ соответствует число $A = \sum_{i=0}^{6} \alpha_i \cdot 2^i,\ \alpha \in \{0, 1\}$

Замечание 2. При вычислениях воспользоваться таблицей значений следов элементов $\theta^j = \sum\limits_{i=0}^{6} \alpha_i \cdot \theta^i \in GF(2^7) = \mathbb{Z}_2[\theta]/(\theta^7 + \theta + 1)$ (из таблицы упражнения 6.41).

Варианты заданий:

N	1	2	3	4	5	6	7	8	9	10
i	7	13	14	26	27	28	31	35	47	52
d	13	20	40	31	24	51	43	38	25	45
k	10	31	44	59	11	35	20	41	64	19
H	81	82	83	84	85	86	87	88	89	93

N	11	12	13	14	15	16	17	18	19	20
i	56	61	62	63	67	70	79	81	87	94
d	39	26	47	37	28	42	51	61	37	63
k	30	53	42	17	40	67	19	50	27	33
H	95	99	101	102	103	104	105	106	107	108

Литература

[1] Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. — М.: Гелиос АРВ, 2002.

[2] Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. — М: Изд.2, доп. URSS. 2012.

[3] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. — 2-е изд., доп. — М.: МЦНМО, 2006.

[4] Виноградов И.М. Основы теории чисел. — М.: Наука, 1972.

[5] Гашков С.Б., Применко Э.А., Черепнев М.А. Криптографические методы защиты информации. — М.: Академия Москва, 2010.

[6] Грушо А.А, Применко Э.А, Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. — Йошкар-Ола: МОСУ, 2001.

[7] Грушо А.А., Применко Э.А., Тимонина Е.Е. Криптографические протоколы. — Йошкар-Ола: МОСУ, 2001.

[8] Минеев М.П., Чубариков В.Н. Лекции по арифметическим вопросам криптографии. — М.: Научно-издательский центр Луч, 2014. — 224 с.

[9] Применко Э.А. Алгебраические основы криптографии. — , М.: Книжный дом Либроком. — 2013. — 288 с.

[10] Применко Э.А. Конечные группы подстановок. — , М.: МИЭМ. — 1982.

[11] Коблиц Н. Курс теории чисел и криптографии. — М: Научное изд-во ТВП. 2001.

[12] Кострикин А.И. Введение в алгебру. — М.: Наука, 1977.

[13] Холл М. Теория групп. — М.: ИЛ. 1962.

[14] Цирлер Н. Линейные возвратные последовательности // Кибернетический сборник. — М.: ИЛ, 1963. — Вып. 6. — С.55-79.