

# ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ



По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со стеклянными стенами и охраняется сторожевым керуулом, однако и в этом случае сомнения не оставят меня.

Ю. Слаффорд

Э. А. ПРИМЕНКО

# АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ



Э. А. Применко

# АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Допущено УМО  
по классическому университетскому образованию  
в качестве учебного пособия  
для студентов высших учебных заведений,  
обучающихся по направлениям ВПО 010400  
«Прикладная математика и информатика»  
и 010300 «Фундаментальная информатика  
и информационные технологии»



URSS

МОСКВА



ББК 22.145 22.18 32.811 32.97

3БТ  
7-764**67073880****Применко Эдуард Андреевич****Алгебраические основы криптографии: Учебное пособие.**

М.: Книжный дом «ЛИБРОКОМ», 2013. — 288 с.

(Основы защиты информации.)

В основу настоящего пособия положены лекции, читаемые автором на факультете вычислительной математики и кибернетики МГУ. Курс «Математические основы криптологии» входит как обязательный в учебные планы магистратуры факультета ВМК по программе «Математическое и программное обеспечение защиты информации», а также в учебные планы студентов третьего курса, обучающихся по аналогичной специализации. Этот курс является базовым для других обязательных дисциплин и спецкурсов. Материал, излагаемый в настоящем курсе, разбросан по различным монографиям, статьям и учебникам, что затрудняет его изучение. Предлагаемое пособие призвано помочь студентам в изучении данного курса. В пособии рассматриваются такие основные алгебраические структуры, как конечные поля, группы подстановок, а также их теоретико-числовая реализация; в частности, изучаются группы точек эллиптических кривых над конечным полем.

**Рецензенты:**

д-р физ.-мат. наук, проф. С. Б. Гашков;  
 д-р физ.-мат. наук, проф. В. М. Максимов

*Редактор серии М. А. Борисов*

**НАУЧНАЯ  
БИБЛИОТЕКА 7  
МГУ**

Издательство «Книжный дом «ЛИБРОКОМ».  
 117335, Москва, Нахимовский пр-т, 56.  
 Формат 60×90/16. Печ. л. 18. Зак. № ВС-20.

Отпечатано в ООО «ЛЕНАНД».  
 117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

**ISBN 978-5-382-01455-5****© Книжный дом «ЛИБРОКОМ», 2013**

13588 ID 169492



9 785382 014555



Все права защищены. Никакая часть настоящей книги не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, а также размещение в Интернете, если на то нет письменного разрешения владельца.

# Оглавление

<b>Предисловие</b>	<b>7</b>
<b>1 Введение. Математическая модель шифров</b>	<b>8</b>
1.1 Примеры шифров . . . . .	9
<b>2 Основы теории конечных групп</b>	<b>13</b>
2.1 Элементарные свойства групп подстановок . . . . .	15
2.2 Смежные классы . . . . .	21
2.3 Циклические группы . . . . .	26
2.4 Прямое произведение конечных групп . . . . .	29
<b>3 Введение в элементарную теорию чисел</b>	<b>32</b>
3.1 Делимость и ее свойства . . . . .	32
3.2 Сравнения и их свойства . . . . .	37
3.3 Кольца, поля . . . . .	39
3.4 Функции Эйлера и Мебиуса . . . . .	45
<b>4 Квадратичные вычеты</b>	<b>55</b>
4.1 Определение и свойства . . . . .	55
4.2 Символ Лежандра . . . . .	57
4.3 Символ Якоби . . . . .	61
4.4 Алгоритмы решения квадратичного сравнения по простому модулю . . . . .	64
4.5 Алгоритмы решения сравнения второй степени по примарному модулю . . . . .	71
4.6 Решения сравнений по модулю $2^n$ . . . . .	77

<b>5 Порождение больших простых чисел</b>	<b>84</b>
5.1 Алгоритмы порождения простых чисел . . . . .	84
<b>6 Вероятностные тесты на простоту</b>	<b>89</b>
6.1 Обоснование тестов . . . . .	89
6.2 Тест Соловея—Штрассена . . . . .	90
6.3 Тест Миллера—Рабина . . . . .	91
<b>7 Конечные поля</b>	<b>98</b>
7.1 Общие определения . . . . .	98
7.2 Построение конечных полей . . . . .	100
7.3 Минимальные многочлены и их свойства . . . . .	101
7.4 Группа автоморфизмов конечных полей . . . . .	110
<b>8 Детерминированные алгоритмы дискретного логарифмирования</b>	<b>112</b>
8.1 Алгоритм согласования . . . . .	113
8.2 Алгоритм Полига—Хеллмана . . . . .	115
8.3 $\rho$ -алгоритм Полларда . . . . .	120
8.4 Алгоритм вычисления индексов . . . . .	123
8.4.1 Алгоритм вычисления индексов в $\mathbb{Z}_p^*$ . . . . .	125
8.4.2 Алгоритм вычисления индексов в $\mathbb{F}_{2^m}^*$ . . . . .	126
<b>9 Рекуррентные последовательности над конечными полями</b>	<b>129</b>
<b>10 Автономные автоматы</b>	<b>140</b>
10.1 Определения. Регистры сдвига . . . . .	140
10.2 Критерий регулярности автономных автоматов .	146
<b>11 Линейный конгруэнтный метод</b>	<b>156</b>
<b>12 Строение конечных групп</b>	<b>163</b>
12.1 Конечные абелевы группы . . . . .	163
12.2 Сопряжённые классы и элементы.	
Теорема Коши . . . . .	169
12.3 Двойные классы смежности. Теоремы Силова .	173

---

<b>13 Конечные группы подстановок</b>	<b>179</b>
13.1 Орбиты, стабилизаторы и их свойства.	
Лемма Бернсайда . . . . .	179
13.2 Регулярные и полурегулярные группы . . . . .	185
13.3 Блоки и импримитивные группы . . . . .	187
13.4 Примитивные группы.	
Кратная транзитивность . . . . .	191
13.5 Группы подстановок с регулярным	
нормальным делителем . . . . .	198
13.6 Базисы симметрической	
и знакопеременной групп . . . . .	205
<b>14 Эллиптические кривые</b>	<b>224</b>
14.1 Общие понятия и канонические уравнения . . . . .	224
14.2 Дискриминант эллиптической кривой	
над полем характеристики $p > 3$ . . . . .	227
14.3 Группа точек эллиптической кривой	
над полем характеристики $p > 3$ . . . . .	231
14.4 Порядок группы $\mathcal{E}_p(a, b)$ с нулевым	
дискриминантом . . . . .	235
14.5 Элементарные верхние и нижние оценки	
порядка группы $\mathcal{E}_p(a, b)$ . . . . .	237
14.6 Элементарное доказательство теоремы Хассе .	239
14.7 Эллиптические кривые над полем	
характеристики 3 . . . . .	256
14.8 Эллиптические кривые над полем	
характеристики 2 . . . . .	261
14.8.1 Группа точек суперсингулярной кривой .	261
14.8.2 Суперсингулярные кривые над полем	
нечетной степени . . . . .	266
14.8.3 Группа точек несуперсингулярной	
кривой . . . . .	271
14.8.4 Аномальные несуперсингулярные	
эллиптические кривые . . . . .	277
<b>Литература</b>	<b>282</b>

# Предисловие

Учебное пособие написано на основе лекций, читаемых автором на факультете ВМК МГУ имени М. В. Ломоносова для бакалавров, студентов и магистров, обучающихся по направлению «Математическое и программное обеспечение информационной безопасности». Курс является базовым для других дисциплин и спецкурсов. К ним относятся такие курсы, как «Криптографические протоколы», «Криптографические хэш-функции», «Криптоанализ потоковых и блочных шифров» и др.

Материал, излагаемый в курсе, разбросан по различным монографиям, учебным пособиям и статьям, что затрудняет его изучение. Данное учебное пособие в определенной степени восполняет этот пробел.

Особое внимание в учебном пособии уделено конечным группам подстановок, теоретико-числовым алгоритмам, применяемым в криптографии, вычислениям в группе точек эллиптической кривой над конечным полем. Излагаемый теоретический материал подкрепляется многочисленными примерами, задачами и упражнениями.

Автор признателен рецензентам профессорам Гашкову С. Б. и Максимову В. М. за ценные замечания.

# Глава 1

## Введение. Математическая модель шифров

Криптография как основа для построения систем защиты информации возникла одновременно с письменностью. И первая задача, которую решала криптография — это обеспечение конфиденциальности (секретности) при передачи информации по открытым каналам связи. Как наука она сформировалась в конце 40-х годов прошлого века. Большинство результатов научных исследований в области криптографии остаются недоступными, так как криптографические методы являются основой для построения систем, обеспечивающих информационную безопасность государства. С другой стороны, повсеместное использование информационных технологий сделало весьма актуальной задачу обеспечения целостности информации. Целостность информации означает, что она получена из достоверного источника в неискаженном виде и в определенное время. Первая задача — обеспечение конфиденциальности — решается, как правило, при помощи симметрической криптографии (ключ зашифрования и расшифрования практически один и тот же). Обеспечение целостности решают при помо-

щи асимметрической криптографии (ключи зашифрования и расшифрования различны).

Третья из основных задач криптографии — это обеспечение неотслеживаемости (анонимности), то есть невозможность противником получить сведения о действиях участников информационного взаимодействия. Особенно актуальна эта задача для банковских технологий (система электронных платежей).

Неформально, суть зашифрования заключается в таком целенаправленном преобразовании информации, открытого текста, передаваемой по открытому каналу связи, при котором злоумышленник, не обладающий секретным ключом, не сможет дешифровать, то есть получить исходный открытый текст.

Формально модель шифра (криптосистемы, криптографического алгоритма) описывается следующим образом:

пусть  $\mathcal{X}$  — множество открытых текстов,  $\mathcal{Y}$  — множество шифрованных текстов,  $\mathcal{K} = \mathcal{K}_e \times \mathcal{K}_d$  — множество ключей ( $\mathcal{K}_e$  — ключи зашифрования,  $\mathcal{K}_d$  — ключи расшифрования),  $\mathcal{E} = \{E_{k_e} \mid k_e \in \mathcal{K}_e\}$  — множество функций зашифрования,  $\mathcal{D} = \{D_{k_d} \mid k_d \in \mathcal{K}_d\}$  — множество функций расшифрования.

**Определение 1.1.** Система  $(\mathcal{X}, \mathcal{Y}, \mathcal{K} = \mathcal{K}_e \times \mathcal{K}_d, \mathcal{E}, \mathcal{D})$  называется *алгебраическим шифром*, если выполнены условия:

$$\forall x \in \mathcal{X}, \forall (k_e, k_d) \in \mathcal{K}, D_{k_d}(E_{k_e}(x)) = x \quad (1.1)$$

$$\mathcal{Y} = \bigcup_{k_e \in \mathcal{K}_e} E_{k_e}(\mathcal{X}) \quad (1.2)$$

Условие (1.1) обеспечивает однозначность расшифрования, а условие (1.2) означает, что любой шифртекст получают зашифрованием на некотором ключе некоторого открытого текста.

## 1.1 Примеры шифров

- Шифр простой замены. Пусть  $A = \{a_1, \dots, a_n\}$ ,  $A^*$  — множество слов конечной длины над  $A$ , тогда шифр

простой замены определяется следующим образом:

$$\mathcal{X} = \mathcal{Y} = A^*,$$

$$\mathcal{K} = \{(\pi, \pi^{-1}) \mid \pi \in G < S_n^A\},$$

$$E_{k_e}(x) = \pi(b_1) \dots \pi(b_t), \quad x = b_1 \dots b_t, \quad b_i \in A,$$

$$D_{k_d}(y) = \pi^{-1}(c_1) \dots \pi^{-1}(c_t), \quad y = c_1 \dots c_t, \quad c_i \in A.$$

## 2. Шифр перестановки.

$$\mathcal{X} = \mathcal{Y} = (\underbrace{A \times \dots \times A}_m)^*,$$

$$\mathcal{K} = \{(\pi, \pi^{-1}) \mid \pi \in G < S_n\},$$

$$E_{k_e}(x) = E_{k_e}(x_{11} \dots x_{1m} \dots x_{t1} \dots x_{tm}) =$$

$$= x_{1\pi(1)} \dots x_{1\pi(m)} \dots x_{t\pi(1)} \dots x_{t\pi(m)}, \quad x_{ij} \in A,$$

$$D_{k_d}(y) = D_{k_d}(y_{11} \dots y_{1m} \dots y_{t1} \dots y_{tm}) =$$

$$= y_{1\pi^{-1}(1)} \dots y_{1\pi^{-1}(m)} \dots y_{t\pi^{-1}(1)} \dots y_{t\pi^{-1}(m)}, \quad y_{ij} \in A.$$

## 3. Шифр модульного гаммирования.

$$\mathcal{X} = \mathcal{Y} = (\mathbb{Z}_n)^*,$$

$$\mathcal{K} \subset (\mathbb{Z}_n)^* \times (\mathbb{Z}_n)^*,$$

$$E_{k_e}(x) = x_1 \boxplus \gamma_1 \dots x_t \boxplus \gamma_t, \quad x_i, \gamma_i \in \mathbb{Z}_n, \quad k_e = \gamma_1 \dots \gamma_t,$$

$$D_{k_d}(y) = y_1 \boxplus \beta_1 \dots y_t \boxplus \beta_t, \quad y_i, \gamma_i \in \mathbb{Z}_n, \quad k_d = \beta_1 \dots \beta_t,$$

где  $\beta_i = n - \gamma_i, i = \overline{1, t}$ ,  $\boxplus$  — операция сложения по модулю  $n$ .

**Замечание 1.1.** Особенно просто шифр гаммирования реализуется в случае  $n = 2$ . В этом случае  $k_e = k_d$ .

**Замечание 1.2.** Приведенные шифры являются *симметрическими шифрами* — ключ расшифрования вычислительно простиран с ключом шифрования. Шифры простой замены и

перестановки являются не стойкими при небольших значениях  $t$  и  $n$ . При большом количестве текстов, шифрованных на одном ключе, возможно дешифрование шифртекста (без знания ключа) на основе естественной статистики языка. Шифр гаммирования при случайном выборе ключа (последовательности) и при условии, что длина ключа не меньше длины открытого текста, является абсолютно стойким.

#### 4. Шифр RSA (Rivest, Shamir, Adleman).

$$\begin{aligned} \mathcal{X} = \mathcal{Y} &= \mathbb{Z}_n, \quad n = p \cdot q, \quad p, q \text{ — простые,} \\ \mathcal{K} &= \{(\{e, n\}, \{d(p, q)\}) \mid e \cdot d \equiv 1 \pmod{(p-1)(q-1)}\}, \\ \{e, n\} &\text{ — открытый ключ, } \{d(p, q)\} \text{ — секретный ключ,} \\ E_{k_e}(x) &\equiv x^e \pmod{n}, \\ D_{k_d}(y) &\equiv y^d \pmod{n}. \end{aligned}$$

#### 5. Криптосистема Эль-Гамала (ElGamal).

$$\begin{aligned} \mathcal{X} = \mathcal{Y} &= F_q^*, \quad F_q \text{ — конечное поле из } q\text{-элементов,} \\ g &\text{ — примитивный элемент } F_q, \quad \langle g \rangle = F_q^*, \\ \mathcal{K} &= \{(\mathbb{Z}_{q-1} \times F_q^*, \mathbb{Z}_{q-1} \times F_q^*)\} = \\ &= \{(s, g^s), (t, g^t) \mid s, t \in \mathbb{Z}_{q-1}\}, \\ s, t &\text{ — секретные, } g^s, g^t \text{ — открытые ключи,} \\ E_{k_e}(x) &= x(g^t)^s = xg^{ts} \pmod{(q-1)}, \\ D_{k_d}(y) &= y(g^s)^{-t} \pmod{(q-1)}. \end{aligned}$$

**Замечание 1.3.** В криптосистеме Эль-Гамала вместо группы  $F_q^*$  можно взять любую группу  $G$  большего порядка, а в качестве  $g$ -элемент большего порядка. Естественно, что групповая операция в этой группе должна допускать простую реализацию. Так, например, в современных протоколах ЭЦП в качестве  $G$  выбирается группа точек эллиптической кривой.

**Замечание 1.4.** Шифры 4 и 5 дают примеры *асимметрических шифров*. Стойкость криптосистемы RSA основывается на сложности задачи факторизации, то есть задачи разложения числа на простые множители. Стойкость криптосистемы Эль-Гамала обосновывается сложностью задачи дискретного логарифмирования в конечной группе.

Уже из приведенных примеров видно, что для реализации шифров используют такие алгебраические структуры как группы, кольца, поля. При этом нужно уметь эффективно проводить вычисления в этих структурах. Например, нужно знать свойства группы подстановок, используемых при реализации шифров простой замены и перестановки. Для реализации шифров гаммирования необходимо уметь строить случайные и псевдослучайные последовательности большого периода. При реализации шифра RSA необходимо уметь порождать простые числа большого размера с определенными свойствами. При реализации криптосистемы Эль-Гамала необходимо уметь строить конечные группы, содержащие элементы большого порядка, при этом находить примитивные элементы в конечных полях, эффективно вычислять обратный элемент и возводить в степень. Таким образом, основные алгебраические структуры, на основе которых строятся современные шифры, — это конечные группы, кольца вычетов и конечные поля и их теоретико-числовая реализация.

## Глава 2

# Основы теории конечных групп

В этом разделе мы напомним основные понятия и свойства конечных групп.

**Определение 2.1.** Множество  $G \neq \emptyset$  с бинарной операцией « $\circ$ », называется *группой*, если выполнены условия:

1.  $\forall a, b \in G \quad a \circ b \in G;$
2.  $\forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c;$
3.  $\exists e \in G: \forall a \in G \quad e \circ a = a \circ e; \quad \begin{matrix} \text{Элемент } e \\ \text{называется единицей} \end{matrix}$
4.  $\forall a \exists b: a \circ b = b \circ a = e. \quad \begin{matrix} \text{Элемент } b \\ \text{называется обратным к элементу } a \end{matrix}$

Если выполнено условие  $\forall a, b \in G \quad a \circ b = b \circ a$ , то группа  $G$  называется *коммутативной* или *абелевой* группой.

Если групповая операция « $\circ$ » — умножение, то группа называется *мультипликативной*. В этом случае элемент  $e$  — это единица группы, а элемент  $b$  для элемента  $a$  в условии 4 называется обратным.

В случае, когда операция « $\circ$ » — сложение, то группа называется *аддитивной*, элемент  $e$  — нуль группы, а элемент  $b$  для элемента  $a$  в условии 4 называется противоположным.

Приведём некоторые примеры групп.

1. Множество  $\mathbb{Z}$  целых чисел с операцией сложения.
2. Множество  $\mathbb{Z}_2 = \{0, 1\}$  с операцией сложения по модулю 2, операцию сложения по модулю 2 принято обозначать символом « $\oplus$ ».
3. Множество  $G_n$  всех комплексных корней  $n$ -ой степени из 1 с операцией умножения.
4. Множество  $M_n$  невырожденных квадратных матриц над  $\mathbb{R}$  размера  $n \times n$  относительно операции умножения матриц.
5. Множество  $S^\Omega$  всех подстановок на множестве  $\Omega$ . Если  $\Omega = \{1, \dots, n\}$ , то  $S^\Omega = S_n$  — симметрическая группа степени  $n$ . Операцией « $\circ$ » является суперпозиция взаимнооднозначных отображений из  $S$  в  $S$ .
6. Множество  $C_2 = \{1, -1\}$  с операцией умножения.

Группа называется *конечной*, если  $|G| < \infty$  ( $\#G < \infty$ ).

Непустое подмножество  $H \subseteq G$  называется *подгруппой группы*  $G$  (запись  $H < G$ ), если  $H$  — группа относительно данной групповой операции. Например,  $G_2 < G_{2k}$  при любом  $k \geq 1$ , множество всех четных чисел  $2\mathbb{Z} < \mathbb{Z}$ .

**Определение 2.2.** Отображение  $\varphi: G \rightarrow G'$  называется *гомоморфизмом группы*  $G$  в группу  $G'$ , если

$$\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$$

для любых  $a, b \in G$ . Если  $\varphi$  является взаимнооднозначным отображением, то гомоморфизм  $\varphi$  называется *изоморфизмом*.

**Пример 2.1.** Пусть  $G = \{e^{\frac{i\pi k}{6}} \mid k = \overline{0, 5}\}$  — мультипликативная группа корней шестой степени из единицы,  $G' = \{1, -1\}$ .

Определим отображение  $\varphi$  следующим образом:  $\varphi(a) = a^3$  для любого  $a \in G$ . Тогда отсюда следует, что

$$\varphi(e^{\frac{i\pi k}{3}}) = e^{i\pi k} = \begin{cases} 1, & \text{если } k \text{ — четное;} \\ -1, & \text{если } k \text{ — нечетное.} \end{cases}$$

Таким образом,  $\varphi(g) \in G'$  и

$$\varphi(ab) = (ab)^3 = a^3b^3 = \varphi(a)\varphi(b).$$

Следовательно,  $\varphi$  — гомоморфизм.

## 2.1 Элементарные свойства групп подстановок

Особую роль в теории конечных групп играет  $S^\Omega$  — группа подстановок на множестве  $\Omega$ .

Пусть  $\Omega = \{1, \dots, n\}$ , тогда  $S^\Omega = S_n = \left\{ \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix} \right\}$  — симметрическая группа подстановок,  $|S_n| = n!$ .

Если  $\alpha \in \Omega, g \in S^\Omega$ , то  $g(\alpha) = \alpha^g \in \Omega$ .

Если  $g_1, g_2 \in S^\Omega$ , то полагаем  $g_1 \circ g_2 = g$  по следующему правилу:

$$\alpha^g = (\alpha^{g_1})^{g_2} = \alpha^{g_1 g_2}, \forall \alpha \in \Omega.$$

Очевидно, что  $g \in S^\Omega$ .

Относительно введенной операции  $S_n$  является группой, в частности

$$e = \begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix},$$

и если

$$g = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}, \text{ то } g^{-1} = \begin{pmatrix} i_1 & \dots & i_n \\ 1 & \dots & n \end{pmatrix}.$$

Как уже отмечалось выше, конечные группы подстановок играют исключительную роль в теории конечных групп. Этот факт подтверждает следующая теорема.

**Теорема 2.1 (Кэли).** *Произвольная конечная группа  $G$  изоморфна некоторой группе  $G'$  подстановок на множестве  $G$ , то есть существует  $G' < S^G$  такая, что  $G$  и  $G'$  изоморфны.*

*Доказательство.* Для любого  $g \in G$  определим  $\varphi_g \in S^G$  следующим образом:  $a^{\varphi_g} = ag$  для любого  $a \in G$ . Очевидно, что  $\varphi_g \in S^G$ , то есть  $\varphi_g$  взаимнооднозначное отображение  $G$  в  $G$ . Это следует из того, что  $\{ag \mid a \in G\} = G$

Пусть  $G' = \{\varphi_g \mid g \in G\}$ . Поскольку  $a^{\varphi_g} = g$ , то  $\varphi_{g_1} \neq \varphi_{g_2}$ , если  $g_1 \neq g_2$ . Следовательно,  $|G'| = |G|$ . Далее, положим  $\varphi_a \circ \varphi_b = \varphi_{ab}$ , то есть  $c^{\varphi_a \circ \varphi_b} = (c^{\varphi_a})^{\varphi_b}$ , для любого  $c \in G$ . Легко показать, что относительно введенной операции  $G'$  является группой. Например, единицей  $e'$  группы  $G'$  является подстановка  $\varphi_e$ , а  $(\varphi_g)^{-1} = \varphi_{g^{-1}}$ .

Отображение  $\psi: G \rightarrow G'$ , определенное по правилу

$$\psi(g) = \varphi_g$$

является изоморфизмом, так как  $|G'| = |G|$  и из определения  $\psi$  имеем:

$$\psi(g_1g_2) = \varphi_{g_1g_2} = \varphi_{g_1} \circ \varphi_{g_2} = \psi(g_1) \circ \psi(g_2).$$

□

**Определение 2.3.** Подстановка  $g$  есть цикл длины  $m$ , или просто  $m$ -цикл, если для некоторого  $I = \{i_1, \dots, i_m\} \subseteq \Omega$  выполняются условия:

$$i_k^g = i_{k+1}, \quad k = \overline{1, m-1}, \quad i_m^g = i_1,$$

$$\alpha^g = \alpha \text{ для любого } \alpha \in \Omega \setminus I.$$

Записывается цикл следующим образом:  $g = (i_1 \ i_2 \ \dots \ i_m)$ . Например, если  $n = 7$ , то

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 2 & 6 & 7 \end{pmatrix} = (2 \ 3 \ 5)$$

является 3-циклом.

Заметим, что любой  $m$ -цикл допускает  $m$  эквивалентных записей, то есть, если  $\pi = (i_1 \ \dots \ i_m)$  —  $m$ -цикл, то

$$\pi = (i_1 \ i_2 \ \dots \ i_m) = (i_2 \ \dots \ i_m \ i_1) =$$

$$= (i_2 \ \dots \ i_m \ i_1 \ i_2) = \dots = (i_m \ i_1 \ i_2 \ \dots \ i_{m-1})$$



Так, например,  $(2\ 3\ 5) = (3\ 5\ 2) = (5\ 2\ 3)$ . Очевидно также, что если  $\pi = (i_1\ i_2 \dots i_m)$  —  $m$ -цикль, то  $\pi^{-1} = (i_1\ i_m \dots i_2)$ . Например,  $(\alpha\ \beta\ \gamma)^{-1} = (\alpha\ \gamma\ \beta)$ .

Циклы  $g = (i_1\ i_2 \dots i_m)$  и  $h = (j_1\ j_2 \dots j_k)$  называются *независимыми*, если  $\{i_1, \dots, i_m\} \cap \{j_1, \dots, j_k\} = \emptyset$ .

**Утверждение 2.1.** Любой подстановке  $g \in S^\Omega$  может быть представлена в виде произведения независимых циклов. Это представление определено с точностью до порядка следования циклов.

*Доказательство.* Пусть  $\alpha \in \Omega$ ,  $g \in S^\Omega$ .

Рассмотрим последовательность элементов из  $\Omega$  следующего вида

$$\alpha, \alpha^g, \alpha^{g^2}, \dots, \alpha^{g^t}, \dots$$

Из конечности  $\Omega$  следует, что найдутся  $r$  и  $s$ ,  $s > r$  такие, что

$$\alpha^{g^r} = \alpha^{g^s} \Leftrightarrow \alpha^{g^{s-r}} = \alpha.$$

Таким образом, найдется  $k \in \mathbb{N}$  такое, что  $\alpha^{g^k} = \alpha$ .

Пусть  $k$  — минимальное число, удовлетворяющее последнему условию. Тогда  $\pi(\alpha) = (\alpha\ \alpha^g \dots \alpha^{g^{k-1}})$  — цикл длины  $k$ , порождённый подстановкой  $g$ . Очевидно, что  $\alpha^{g^i} \neq \alpha^{g^j}$  при  $1 \leq i < j \leq k$ . Справедливость этого условия вытекает из минимальности  $k$ . Далее, если  $k \neq n = |\Omega|$ , то выбираем  $\beta \in \Omega \setminus \{\alpha, \alpha^g, \dots, \alpha^{g^{k-1}}\}$  и аналогичным образом построим цикл  $\pi(\beta) = (\beta\ \beta^g \dots \beta^{g^{l-1}})$ . Очевидно, что  $\pi(\alpha)$  и  $\pi(\beta)$  — независимые циклы. Если  $l + k = n$ , то процесс разложения на циклы закончен. В противном случае выбираем

$$\gamma \in \Omega \setminus \left( \{\alpha, \alpha^g, \dots, \alpha^{g^{k-1}}\} \cup \{\beta, \beta^g, \dots, \beta^{g^{l-1}}\} \right)$$

и аналогичным образом строим цикл  $\pi(\gamma)$ . В силу конечности  $\Omega$  этот процесс через некоторое число шагов закончится, и мы получим требуемое представление подстановки в виде произведения независимых циклов.  $\square$

**Пример 2.2.** Пусть  $n = 12$ ,

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 5 & 2 & 4 & 6 & 3 & 9 & 10 & 7 & 8 & 12 & 1 \end{pmatrix}.$$

В это случае  $w$  представима в виде произведения циклов следующим образом:

$$w = (1 \ 11 \ 12)(2 \ 5 \ 6 \ 3)(4)(7 \ 9)(8 \ 10).$$

**Определение 2.4.** Если  $g \in S^\Omega$ ,  $|\Omega| = n$ , то последовательность  $c(g) = (l_1, \dots, l_n)$  называется *циклической структурой подстановки*, если  $l_i$  — число циклов длины  $i$  в представлении  $g$  в виде произведения независимых циклов.

Для предыдущего примера в частности

$$c(w) = (1, 2, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0).$$

Очевидно, что  $\sum_{i=1}^n i \cdot l_i = n$ .

Цикл длины 2 называется *транспозицией*.

**Утверждение 2.2.** Любой  $g \in S^\Omega$  можно представить в виде произведения транспозиций.

**Доказательство.** Для доказательства справедливости утверждения достаточно доказать, что любой цикл можно представить в виде произведения транспозиций. Покажем это. Во-первых, любой цикл длины один ( $\alpha$ ) является произведением транспозиций  $(\alpha \beta)(\alpha \beta)$ ,  $\beta \neq \alpha$ .

Пусть  $g = (\alpha_1 \dots \alpha_k)$  — цикл длины  $k$ ,  $k \geq 3$ . Тогда непосредственной проверкой легко убедиться, что  $g = (\alpha_1 \alpha_k)(\alpha_2 \dots \alpha_k)$ . Из этого соотношения, математической индукцией устанавливается справедливость утверждения.  $\square$

Например,  $(1 \ 3 \ 5 \ 7) = (1 \ 7)(3 \ 5 \ 7) = (1 \ 7)(3 \ 7)(5 \ 7)$ .

Представление подстановки в виде произведения транспозиций неоднозначно. Так подстановка  $(1 \ 3 \ 5 \ 7)$  допускает и другие представления в виде произведения транспозиций.

$$(1 \ 3 \ 5 \ 7) = (3 \ 5 \ 7 \ 1) = (3 \ 1)(5 \ 1)(7 \ 1)$$

$$(1 \ 3 \ 5 \ 7) = (5 \ 7 \ 1 \ 3) = (5 \ 3)(7 \ 3)(1 \ 3)$$

$$(1 \ 3 \ 5 \ 7) = (7 \ 1 \ 3 \ 5) = (7 \ 5)(1 \ 5)(3 \ 5)$$

С другой стороны, покажем, что для любой  $\pi \in S_n$  инвариантом является чётность числа транспозиций в ее представлении в виде произведения транспозиций.

Пусть  $f(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$  и  $\pi \in S_n$ . Положим

$$f^\pi(x_1, \dots, x_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)}) = \prod_{1 \leq i < j \leq n} (x_{\pi(i)} - x_{\pi(j)})$$

и

$$\begin{aligned} f^{\pi_1 \pi_2}(x_1 \dots x_n) &= (f^{\pi_1})^{\pi_2}(x_1 \dots x_n) = \\ &= f(x_{\pi_2(\pi_1(1))}, \dots, x_{\pi_2(\pi_1(n))}). \end{aligned}$$

Из определения  $f^\pi(x_1, \dots, x_n)$  следует, что

$$f^\pi(x_1, \dots, x_n) = \pm f(x_1, \dots, x_n).$$

**Определение 2.5.** Подстановку  $\pi \in S_n$  назовем *чётной* (*нечётной*), если  $f^\pi(x_1, \dots, x_n) = f(x_1, \dots, x_n)$  (соответственно  $f^\pi(x_1, \dots, x_n) = -f(x_1, \dots, x_n)$ ).

**Утверждение 2.3.** Подстановка  $\pi \in S_n$  является чётной тогда и только тогда, когда число транспозиций в любом ее представлении в виде транспозиций является чётным числом.

**Доказательство.** Для доказательства достаточно установить, что если  $\pi = (i \ j)$  — транспозиция ( $i < j$ ), то

$$f^\pi(x_1, \dots, x_n) = -f(x_1, \dots, x_n).$$

Действительно, если мы установим этот факт, то тогда  $f^\pi(x_1, \dots, x_n) = (-1)^N f(x_1, \dots, x_n)$ , где  $N$  — число транспозиций в некотором ее представлении в виде независимых циклов.

Поэтому из определения чётности подстановки вытекает, что  $(-1)^N$  не зависит от выбранного представления.

Представим  $f(x_1, \dots, x_n)$  в виде

$$\begin{aligned} f(x_1, \dots, x_n) &= \\ &= f_1(x_1, \dots, x_n) f_2(x_2, \dots, x_n) \cdots f_{n-1}(x_{n-1}, x_n), \end{aligned}$$

где  $f_k(x_k, \dots, x_n) = \prod_{k < r \leq n} (x_k - x_r)$ ,  $k = \overline{1, n-1}$ .

Очевидно, что у функции  $f^\pi$  в этом представлении множители  $f_k^\pi$  будут совпадать с  $f_k$ , если  $k < i$  или  $k \geq j$ . Таким образом, нам нужно подсчитать число сомножителей у функции  $f_k^\pi(x_k, \dots, x_n)$ , ( $k = \overline{i, j-1}$ ), которые поменяли знак на противоположный при действии на функцию  $f(x_1, \dots, x_n)$  транспозиции  $\pi = (i\ j)$ . Выпишем эти функции:

$$\begin{aligned} f_i^\pi(x_i, \dots, x_n) &= (x_j - x_{i+1}) \cdots \\ &\cdots (x_j - x_{j-1})(x_j - x_i)(x_j - x_{j+1}) \cdots (x_j - x_n), \end{aligned}$$

$$\begin{aligned} f_{i+1}^\pi(x_{i+1}, \dots, x_n) &= (x_{i+1} - x_{i+2}) \cdots \\ &\cdots (x_{i+1} - x_{j-1})(x_{i+1} - x_i)(x_{i+1} - x_{j+1}) \cdots (x_{i+1} - x_n), \end{aligned}$$

.....

$$f_{j-1}^\pi(x_{j-1}, \dots, x_n) = (x_{j-1} - x_i) \cdots (x_{j-1} - x_{j+1}) \cdots (x_{j-1} - x_n).$$

Из этих соотношений следует, что число сомножителей вида  $(x_s - x_t)$ , где  $s > t$  у функции  $f_i^\pi$  равно  $j - (i + 1) + 1 = j - i$ , а у каждой из функций  $f_r^\pi$  при  $r = \overline{i+1, j-1}$  это число равно 1. Таким образом, общее число таких сомножителей будет равно

$$N = j - i + j - 1 - (i + 1) + 1 = 2(j - i) - 1.$$

Следовательно,

$$\begin{aligned} f^\pi(x_1, x_2, \dots, x_n) &= (-1)^{2(j-i)-1} f(x_1, x_2, \dots, x_n) = \\ &= -f(x_1, x_2, \dots, x_n). \end{aligned}$$



Множество всех четных подстановок образует подгруппу  $A_n$  симметрической группы  $S_n$ . Эта подгруппа называется *знакоизменной*. Покажем, что

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Пусть  $T_n$  – множество всех нечетных подстановок из  $S_n$ . Тогда  $|T_n| + |A_n| = |S_n| = n!$ . Если  $g$  – нечетная, то  $gT_n \subset T_n$ . Следовательно,  $|gA_n| = |A_n| \leq |T_n|$ . С другой стороны,  $gT_n \subset A_n$  и поэтому  $|gT_n| = |T_n| \leq |A_n|$ . Таким образом,  $|T_n| = |A_n| = n!/2$ .

**Пример 2.3.**

$$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\},$$

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}.$$

## 2.2 Смежные классы

Пусть  $H < G$ ,  $a$  – некоторый элемент группы  $G$ . Множество  $aH = \{ah \mid h \in H\}$  называется *левым смежным классом группы  $G$  по подгруппе  $H$ , порожденным элементом  $a$* , а множество  $Ha$  – *правым смежным классом*. Из определения вытекают следующие свойства:

1.  $a \in aH$ ,  $a \in Ha$ , так как подгруппа  $H$  содержит единицу.
2. Смежный класс состоит из элементов группы, причем любой элемент группы входит в какой-нибудь смежный класс.
3. Подгруппа  $H$  является одним из смежных классов (как левых, так и правых), поскольку  $H = eH = He$ .
4. В абелевой группе  $aH = Ha$ , для всех  $a \in G$ .

**Пример 2.4.** Пусть  $G = S_n$ ,  $H = A_n$ ,  $g$  – нечетная подстановка. Тогда  $S_n = A_n + gA_n$ .

**Теорема 2.2.** Смежный класс порождается любым своим элементом.

**Доказательство.** Надо показать, что если  $g \in aH$ , то верно равенство  $aH = gH$ . Пусть  $g = ah_1$ ,  $h_1 \in H$ . Тогда для любого элемента  $h \in H$  имеем  $ah = (ah_1)(h_1^{-1}h) = gh_2$ , где  $h_2 = h_1^{-1}h \in H$  в силу определения подгруппы. Значит  $aH \subset gH$ . В то же время  $gh = a(h_1h) = ah_3$ , где  $h_3 = h_1h \in H$ . Следовательно,  $gH \subset aH$ , и с учетом вложения в другую сторону получаем требуемое равенство.  $\square$

**Теорема 2.3.** Любые два левых (правых) смежных класса либо совпадают, либо не пересекаются.

**Доказательство.** Утверждение теоремы вытекает из предыдущей теоремы, так как если два смежных класса  $aH$  и  $bH$  имеют общий элемент  $g$ , то  $aH = bH = gH$ .  $\square$

Итак, вся группа разбивается на непересекающиеся левые (правые) смежные классы по подгруппе  $H$ . Это разбиение называется **левосторонним** (соответственно **правосторонним**) **разложением** группы  $G$  по подгруппе  $H$ .

**Пример 2.5.** Пусть  $G_8 = \{e^{\frac{\pi k i}{4}} \mid k = \overline{0, 7}\}$ ,  $H = \{1, -1\}$ . Тогда

$$G_8 = \{1, -1\} + \{e^{\frac{\pi i}{4}}, e^{\frac{5\pi i}{4}}\} + \{i, -i\} + \{e^{\frac{3\pi i}{4}}, e^{\frac{7\pi i}{4}}\}.$$

**Теорема 2.4.** Если  $H$  — конечная подгруппа группы  $G$ , то каждый (левый или правый) смежный класс группы  $G$  по подгруппе  $H$  содержит столько же элементов, сколько  $H$ .

**Доказательство.** Рассмотрим случай левых смежных классов. Предположим противное, то есть, что существует  $a \in G$  такой, что  $|aH| < |H|$ . (Так как  $H$  — конечная подгруппа, то смежный класс  $aH$ , у которого число элементов не совпадает с числом элементов в подгруппе  $H$ , имеет меньшее число элементов чем  $H$ .) Тогда существуют  $h_1, h_2 \in H$  такие, что из

$ah_1 = ah_2$  следует  $h_1 = h_2$ , так как  $a \in G$ . Пришли к противоречию. Поэтому все левые смежные классы по подгруппе  $H$  имеют число элементов, равное числу элементов в  $H$ .

Аналогично доказывается для правых смежных классов.

□

**Определение 2.6.** Если подгруппа  $H$  группы  $G$  такова, что множество смежных классов  $G$  по  $H$  конечно, то число этих смежных классов называется *индексом подгруппы  $H$  в группе  $G$*  и обозначается  $[G : H]$ .

Так как левые смежные классы группы  $G$  по подгруппе  $H$  образуют разбиение этой группы, то из Теоремы 2.4 вытекает следующий важный результат.

**Теорема 2.5** (Лагранж). *Порядок конечной группы  $G$  равен произведению порядка любой ее подгруппы  $H$  на индекс  $[G : H]$  этой подгруппы в  $G$ . В частности, порядок любой подгруппы  $H$  группы  $G$  и ее индекс в  $G$  делят порядок группы  $G$ .*

**Определение 2.7.** Подгруппа  $H$  группы  $G$  называется *нормальной подгруппой* (или *нормальным делителем*) этой группы, если  $ghg^{-1} \in H$  для всех  $g \in G$  и  $h \in H$ . Обозначение:  $H \triangleleft G$ .

Ясно, что каждая подгруппа абелевой группы нормальна, поскольку в этом случае  $ghg^{-1} = gg^{-1}h = eh = h$ .

**Упражнение 2.1.** Пусть  $G = A_4$ . Показать, что

$$K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \triangleleft A_4.$$

Выписать все смежные классы группы  $A_4$  по подгруппе  $K$ .

**Пример 2.6.** Любая подгруппа  $H$  группы  $G$  индекса 2 является нормальной в  $G$ . Это следует из того, что

$$G = H + gH = H + Hg,$$

то есть  $gH = Hg$ , для всех  $g \in G$ , то есть  $H \triangleleft G$ , в частности,  $A_n \triangleleft S_n$ .

**Теорема 2.6.** Если  $H$  – нормальная подгруппа группы  $G$ , то множество смежных классов группы  $G$  по подгруппе  $H$  образует группу относительно операции

$$(aH) \cdot (bH) = (ab)H.$$

**Доказательство.** Установим, во-первых, корректность введенной на смежных классах бинарной операции. Для этого нужно показать, что результат этой операции не зависит от выбора представителей смежных классов. Итак, пусть  $ah_1 \in aH$  и  $bh_2 \in bH$ . Убедимся, что  $c = (ah_1)(bh_2) \in abH$  для всех  $h_1, h_2 \in H$ .

Так как  $H \triangleleft G$ , то существует  $h'_1 \in H$  такой, что  $h_1b = bh'_1$ . Следовательно,  $c = (ah_1)(bh_2) = a(h_1b)h_2 = (ab)(h'_1h_2) = ab \cdot h'' \in abH$ . Таким образом, корректность бинарной операции умножения смежных классов установлена.

Далее, если  $G' = \{H, a_2H, \dots, a_mH\}$  – множество всех смежных классов группы  $G$  по  $H$ , то из определения бинарной операции следует, что

$$\begin{aligned} (aH)(bH \cdot cH) &= aH(bcH) = (abc)H = (aH \cdot bH)(cH), \\ (aH) \cdot H &= H \cdot (aH) = aH, \\ (a^{-1}H)(aH) &= (aH)(a^{-1}H) = (aa^{-1})H = H. \end{aligned}$$

Следовательно,  $G'$  – группа и  $e' = H, (aH)^{-1} = a^{-1}H$  □

**Определение 2.8.** Пусть  $H$  – нормальная подгруппа группы  $G$ . Тогда группа, образованная смежными классами группы  $G$  по подгруппе  $H$  с операцией, введенной в Теореме 2.6, называется *фактор-группой группы  $G$  по подгруппе  $H$*  и обозначается  $G/H$ .

Если фактор-группа  $G/H$  конечна, то ее порядок совпадает с индексом  $[G : H]$  подгруппы  $H$  в  $G$ . Таким образом, из Теоремы 2.5 получаем, что для конечной группы  $G$

$$|G/H| = [G : H] = |G|/|H|.$$

**Пример 2.7.** Пусть  $G = S_3$ ,  $H = A_3$ . Тогда

$$G/H = \{A_3, (1\ 2)A_3\} = \{A_3, (1\ 3)A_3\} = \{A_3, (2\ 3)A_3\},$$

$$[G : H] = \frac{|G|}{|H|} = \frac{|G|}{|3|} = 2.$$

**Упражнение 2.2.** Доказать, что если  $|G| < \infty$  и  $K < H < G$ , то  $[G : K] = [G : H][H : K]$ .

Пусть  $\varphi$  — сюръективный гомоморфизм группы  $G$  на  $G'$ , то есть для каждого  $g' \in G'$ , существует  $g \in G$  такой, что  $\varphi(g) = g'$ . Множество  $\ker \varphi = \{g \in G \mid \varphi(g) = e'\}$  называется ядром гомоморфизма  $\varphi$ .

**Упражнение 2.3.** Показать, что  $\ker \varphi \triangleleft G$ .

**Теорема 2.7** (о гомоморфизме). *Если  $\varphi$  — сюръективный гомоморфизм группы  $G$  на  $G'$ ,  $\ker \varphi = T$ , то группа  $G/T$  изоморфна группе  $G'$ .*

*Доказательство.* Пусть  $\{T, g_2T, \dots, g_mT\} = G/T$ ,  $a, b \in G$ ,  $\varphi(a) = \varphi(b)$ . Тогда из определения гомоморфизма следует, что  $\varphi(ab^{-1}) = e'$ . Следовательно,  $ab^{-1} \in T$ , то есть  $a \in Tb = bT$ , так как  $T \triangleleft G$ . С другой стороны, если  $a \in bT$ , то

$$\varphi(a) = \varphi(bt) = \varphi(b)\varphi(t) = \varphi(b)e' = \varphi(b) = g'.$$

Поэтому для любого  $g' \in G'$  существует  $g_i \in G$  такой, что  $\varphi(g_it) = \varphi(g'_i) = g'$  для всех  $t \in T$  и, следовательно,  $|G/T| = |G'|$ .

Определим  $\psi: G/T \rightarrow G'$  следующим образом:

$$\psi(g_iT) = \varphi(g_i).$$

Из выше сказанного следует, что  $\psi$  — взаимнооднозначное отображение и

$$\begin{aligned} \psi(g_iTg_jT) &= \psi(g_ig_jT) = \varphi(g_ig_j) = \\ &= \varphi(g_i)\varphi(g_j) = \psi(g_iT)\psi(g_jT). \end{aligned}$$

Следовательно,  $\psi$  — изоморфизм. □

### 2.3 Циклические группы

**Определение 2.9.** Мультиликативная группа  $G$  называется *циклической*, если в ней имеется такой элемент  $a$ , что каждый элемент  $b \in G$  является степенью элемента  $a$ , то есть существует целое число  $k$  такое, что  $b = a^k$ . Этот элемент  $a$  называется *образующим* группы  $G$ . Для циклической группы  $G$  применяют обозначение  $G = \langle a \rangle$ .

**Определение 2.10.** Порядком элемента  $g$  группы  $G$  называют наименьшее из чисел  $n \in \mathbb{N}$  со свойством  $g^n = e$ , если такие  $n$  существуют, и бесконечность — в противном случае. Порядок  $g$  обозначают через  $\text{ord}(g)$ .

Порядок  $\text{ord}(g)$  элемента  $g$  конечной группы  $G$  — это порядок циклической группы порожденной этим элементом, то есть

$$\text{ord}(g) = |\langle g \rangle|$$

Из теоремы Лагранжа и определения порядка элемента получаем

**Следствие 2.1.** Если  $|G| < \infty$ , то для любого  $g \in G$  его порядок  $\text{ord}(g)$  делит  $|G|$ .

**Замечание 2.1.** Обратное утверждение, вообще говоря, неверно. Например,  $G = \{\{0, 1\}^n, \oplus\}$  —  $n$ -мерный булев куб является абелевой группой, любой элемент которой (кроме нулевого набора) имеет порядок 2. Поэтому, если  $n \geq 3$ , то  $|G| = 2^n$  и  $4 \mid 2^n$ , но элементов порядка 4 в этой группе нет.

#### Утверждение 2.4.

Если порядок любого элемента конечной абелевой группы  $G$  есть степень простого числа  $p$ , то  $|G| = p^n$ ,  $n \in \mathbb{N}$ .

**Доказательство.**

Так как порядок любого элемента группы  $G$  есть делитель  $|G|$ , то  $|G| = p^n \cdot s$ ,  $(s, p) = 1$ . Далее доказательство будем вести индукцией по  $n$ . Пусть  $n = 1$ , порядок группы  $|G| = p \cdot s$ ,

элемент  $a$  группы  $G$  имеет порядок  $\text{ord}(a) = p$ , и  $H$  — группа, образованная элементом  $a$ , то есть  $H = \langle a \rangle$ . Так как  $G$  — абелева, то  $\bar{G} = G/H$  — абелева,  $|\bar{G}| = s$ . Из условия утверждения следует, что  $\text{ord}(\bar{g}) = p$  для любого элемента группы  $\bar{G}$ , отличного от единицы. Следовательно,  $\text{ord}(\bar{g}) = 1$  или  $\text{ord}(\bar{g}) = p$  для любого  $\bar{g} \in G/H$ . Поскольку  $\text{ord}(\bar{g})|s$ , то  $s = 1$ . Таким образом, база индукции установлена.

Допустим, что мы доказали утверждение для любой абелевой группы порядка  $p^k s$ ,  $(s, p) = 1$ ,  $k \geq 1$ , и пусть  $G$  — группа порядка  $p^{k+1}s$ . Выберем в группе  $G$  элемент  $a$  максимального порядка  $p^r$ ,  $r \geq 1$  и рассмотрим фактор-группу  $\bar{G} = G/\langle a \rangle$ .

Группа  $\bar{G}$  будет также удовлетворять условиям утверждения и  $|\bar{G}| = p^{k+1-r}s$ . Из индуктивного предположения следует, что  $s = 1$  и, следовательно,  $|G| = p^{k+1}$ .  $\square$

**Утверждение 2.5** (основное свойство порядка). *Если  $g \in G$ ,  $g^k = e$ , то  $\text{ord}(g)|k$ .*

**Доказательство.** Пусть  $\text{ord}(g) = m$ . Разделим  $k$  на  $m$  с остатком:  $k = qm + r$ ,  $0 \leq r < m$ . Тогда  $g^k = (g^m)^q \cdot g^r$ , и так как  $r < m = \text{ord}(g)$ , то

$$g^k = e \Leftrightarrow g^r = e \Leftrightarrow r = 0 \Rightarrow m|k.$$

$\square$

**Упражнение 2.4.** Доказать, что порядок любой подстановки из  $S_n$  равен наименьшему общему кратному длин ее циклов (в представлении подстановки в виде произведения независимых циклов).

**Лемма 2.1** (о порядке произведения двух перестановочных элементов конечной группы). *Если  $a, b \in G$ ,  $|G| < \infty$ ,  $ab = ba$ ,  $\text{ord}(a) = m$ ,  $\text{ord}(b) = n$  и  $\text{НОД}(m, n) = 1$ , то  $\text{ord}(ab) = mn$ .*

**Доказательство.** Пусть  $\text{ord}(ab) = N$ . Из условия леммы следует, что  $(ab)^{mn} = (a^m)^n(b^n)^m = e$ . Следовательно, согласно утверждению 2.5,  $N|mn$ . С другой стороны,

$$(ab)^{mn} = (a^m)^N b^{mn} = b^{mn} = e$$

и

$$(ab)^{nN} = a^{nN}(b^n)^N = a^{nN} = e.$$

Поэтому, из утверждения 2.5 вытекает, что  $n|mN$  и  $m|nN$ . Так как  $\text{НОД}(m, n) = 1$ , то это означает, что  $mn|N$ . Учитывая, что  $N|mn$ , получим  $N = mn$ .  $\square$

**Утверждение 2.6.** Пусть  $G = \langle a \rangle$  циклическая группа порядка  $n = dt$ . Тогда  $H = \langle a^t \rangle$  — единственная циклическая подгруппа группы  $G$  порядка  $d$  и любой  $b \in G$ , имеющий порядок  $d$ , представим в виде  $b = a^{ts}$ ,  $\text{НОД}(s, d) = 1$ .

**Доказательство.** Очевидно, что  $\text{ord}(a^t) = d$ . Иначе порядок элемента  $a$  был бы меньше  $n$ . Пусть  $H' = \langle a^u \rangle$  и  $\text{ord}(a^u) = d$ , то есть  $a^{ud_1} \neq e$  при  $d_1 < d$ . Покажем, что  $u = ts$  и  $\text{НОД}(s, d) = 1$ . Из условия  $a^{ud} = e$  следует, что  $n|ud$ , при этом  $n = td$ . Тогда  $ud = ns = tds$ , то есть  $u = ts$ . Допустим, что  $\text{НОД}(s, d) = d' > 1$ . Тогда  $d = d'd_1$ ,  $s = d's_1$  и  $u = td's_1$ . Отсюда получаем:

$$(a^u)^{d_1} = a^{td'd_1s_1} = \left(a^{td'd_1}\right)^{s_1} = (a^n)^{-1} = e, d_1 < d.$$

Пришли к противоречию с определением порядка.  $\square$

**Следствие 2.2.** Если  $|G| < \infty$  и  $G$  не содержит собственных подгрупп, то  $G$  — циклическая группа простого порядка.

**Теорема 2.8** (критерий образующего циклической группы). Пусть  $G$  — циклическая группа,  $|G| = n$ . Тогда элемент  $b \in G$  является образующим группы тогда и только тогда, когда выполняется условие

$$b^{\frac{n}{p}} \neq e \quad (2.1)$$

для всех простых  $p|n$ .

**Доказательство.** Необходимость очевидна, поскольку, если  $\langle b \rangle = G$ , то  $\text{ord}(b) = n$ .

Пусть (2.1) выполнено. Допустим, что  $\langle b \rangle \neq G$ . Это значит, что  $b^m = e$  и  $n = mt$ ,  $t > 1$ . Если  $p$  — некоторый простой делитель  $t$ , то  $t = pk$ ,  $k \geq 1$ , тогда  $n = mpk$ , и, следовательно,

$$b^{\frac{n}{p}} = b^{mk} = (b^m)^k = e.$$

Пришли к противоречию с условием (2.1).  $\square$

## 2.4 Прямое произведение конечных групп

Рассмотрим некоторую группу  $G$  и две её подгруппы  $A$  и  $B$ . Построим по этим подгруппам новую группу  $\langle A, B \rangle$ , которая состоит из всех возможных произведений элементов групп  $A$  и  $B$ , то есть

$$\langle A, B \rangle = \{h \mid h = u_1 \dots u_s, s \in \mathbb{N}, u_i \in A \cup B, 1 \leq i \leq s\}.$$

**Упражнение 2.5.** Доказать, что если одна из подгрупп  $A$  или  $B$  нормальна в  $G$ , то

$$\langle A, B \rangle = \{ab \mid a \in A, b \in B\}.$$

**Определение 2.11.** Прямым произведением групп  $A_1, \dots, A_k$  называется группа

$$G = A_1 \times \dots \times A_k = \{(a_1, \dots, a_k) \mid a_i \in A_i\},$$

в которой групповая операция определяется следующим образом:

$$(a_{11}, \dots, a_{1k}) \cdot (a_{21}, \dots, a_{2k}) = (a_{11}a_{21}, \dots, a_{1k}a_{2k}).$$

**Пример 2.8.** Рассмотрим группы  $A_1 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$  и  $A_2 = \{-1, 1\}$ . Тогда

$$\begin{aligned} A_1 \times A_2 &= \{e = (e, 1), g_1 = (e, -1), g_2 = ((1\ 2\ 3), 1), \\ &\quad g_3 = ((1\ 2\ 3), -1), g_4 = ((1\ 3\ 2), 1), g_5 = ((1\ 3\ 2), -1)\}. \end{aligned}$$

И, например,  $g_1 \cdot g_4 = ((1\ 3\ 2), -1) = g_5$ .

**Теорема 2.9.** Если  $H_1$  и  $H_2$  — такие нормальные делители группы  $G$ , что  $H_1 \cap H_2 = \{e\}$ ,  $\langle H_1, H_2 \rangle = G$ , то  $G \cong H_1 \times H_2$ .

**Доказательство.** Из условия теоремы и упражнения 2.5 следует, что  $G = \langle H_1, H_2 \rangle = \{ab \mid a \in H_1, b \in H_2\}$ . Тем самым любой элемент группы  $G$  представим в виде произведения элементов групп  $H_1$  и  $H_2$ , то есть для каждого  $g \in G$  существуют такие элементы  $h_1 \in H_1$ ,  $h_2 \in H_2$ , что  $g = h_1 h_2$ . Докажем, что такое представление единственное. Действительно, пусть  $g = h_1 h_2 = h'_1 h'_2$ . Тогда  $(h'_1)^{-1} h_1 = h'_2 (h_2)^{-1}$ . Элемент  $h'_2 (h_2)^{-1}$  является элементом группы  $H_2$ , значит  $(h'_1)^{-1} h_1$  тоже элемент группы  $H_2$ , но этот элемент лежит также и в  $H_1$ , так как  $h'_1$  и  $h_1$  из  $H_1$ . Но группы  $H_1$  и  $H_2$  пересекаются только по единичному элементу, значит  $(h'_1)^{-1} h_1 = e$  и  $h'_1 = h_1$ . Аналогично доказывается, что  $h'_2 = h_2$ . Итак, представление любого элемента  $g$  группы  $G$  в виде  $g = h_1 h_2$  единствено.

Определим отображение  $\varphi: G \rightarrow H_1 \times H_2$  следующим образом:

$$\varphi(g) = (h_1, h_2), h_1 \in H_1, h_2 \in H_2, g = h_1 h_2.$$

Из однозначности представления любого элемента группы  $G$  в виде произведения элементов групп  $H_1$  и  $H_2$  следует, что  $\varphi$  — взаимно однозначное отображение. Для доказательства теоремы достаточно показать, что для любых элементов  $g_1, g_2$  группы  $G$  выполняется

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2).$$

Действительно, пусть  $g_1 = h_1 h_2$  и  $g_2 = f_1 f_2$ . Тогда  $\varphi(g_1 g_2) = \varphi((h_1 h_2)(f_1 f_2))$ . В силу нормальности подгрупп  $H_1$  и  $H_2$  справедливо соотношение  $a_1 a_2 = a_2 a_1$  для любого  $a_1 \in H_1$ ,  $a_2 \in H_2$ .

Следовательно,  $(h_1 h_2)(f_1 f_2) = (h_1 f_1)(h_2 f_2)$  и поэтому

$$\begin{aligned}\varphi(g_1 g_2) &= \varphi((h_1 f_1)(h_2 f_2)) = (h_1 f_1, h_2 f_2) = \\ &= (h_1, h_2) \times (f_1, f_2) = \varphi(g_1) \varphi(g_2).\end{aligned}$$

Что и требовалось доказать. □

Доказанная теорема допускает обобщение.

**Теорема 2.10.** *Если  $H_1, \dots, H_s$  такие нормальные делители группы  $G$ , что*

$$H_i \cap \langle H_1, \dots, H_{i-1}, H_{i+1}, \dots, H_s \rangle = \langle e \rangle,$$

для всех  $i = \overline{1, s}$  и  $\langle H_1, \dots, H_s \rangle = G$ , то

$$G \cong H_1 \times \cdots \times H_s.$$

*Доказательство.* Проведём доказательство индукцией по  $s$ . Для  $s = 2$  теорема уже доказана. Пусть теорема верна для некоторого  $s \geq 2$ . Докажем, что она верна для  $s+1$ . Рассмотрим  $s+1$  подгрупп  $H_1, \dots, H_{s+1}$  группы  $G$ , удовлетворяющих условию теоремы. Положим  $G' = \langle H_1, \dots, H_s \rangle$ . Очевидно, что  $H_i$ ,  $i = \overline{1, s}$  — нормальные подгруппы группы  $G'$ . Легко проверить, что для  $G', H_1, \dots, H_s$  выполнены все условия теоремы. Поэтому, по индуктивному предположению,  $G' \cong H_1 \times \cdots \times H_s$ . Осталось заметить, что для подгрупп  $G'$  и  $H_{s+1}$  группы  $G$  выполнены условия предыдущей теоремы. В силу этого  $G \cong G' \times H_{s+1}$ . Учитывая разложение группы  $G'$ , окончательно получаем

$$G \cong G' \times H_{s+1} \cong H_1 \times \cdots \times H_{s+1}.$$

□

## Глава 3

# Введение в элементарную теорию чисел

### 3.1 Делимость и ее свойства

Рассмотрим множество  $\mathbb{Z}$  и установим сперва основное свойство делимости в множестве целых чисел, а именно возможность деления с остатком.

**Теорема 3.1** (о делении с остатком). *Пусть  $a > 0$  и  $b > 0$  – целые числа. Тогда  $a$  представимо единственным образом в виде*

$$a = bq + r, \quad 0 \leq r < b.$$

*Доказательство.* Такое представление числа  $a$  можно получить, если взять  $q$  равным наибольшему числу среди всех чисел, для которых  $bq \leq a$ .

Допустив же существование представления числа  $a$  еще одним равенством того же вида:  $a = bq_1 + r_1$ ,  $0 \leq r_1 < b$ ,  $r_1 \leq r$  и вычитая почленно это последнее равенство из предыдущего, получим  $0 = b(q - q_1) + r - r_1$ . Отсюда получаем, что  $r - r_1 = bs$ ,  $s \in \mathbb{Z}$ ,  $r - r_1 < b$ , то есть  $r - r_1 = 0$  и  $q - q_1 = 0$ .  $\square$

Число  $q$  называется *неполным частным*, а число  $r$  – *остатком* от деления  $a$  на  $b$ .



Если  $r = 0$ , то говорят, что  $b$  делит  $a$ , пишут  $b \mid a$ . Очевидно, что если  $b \mid a$  и  $b \mid c$ , то  $b \mid (a \pm c)$ .

**Определение 3.1.** Число  $\text{НОД}(a, b)$  называется *наибольшим общим делителем* двух чисел  $a, b$  если:

1.  $\text{НОД}(a, b)$  делит оба числа  $a$  и  $b$ ;
2.  $\text{НОД}(a, b)$  является наибольшим общим делителем чисел  $a$  и  $b$ , то есть если  $d' \mid a$  и  $d' \mid b$ , то  $d' \mid \text{НОД}(a, b)$  (или, что то же самое,  $d' \leq \text{НОД}(a, b)$ ).

**Теорема 3.2** (алгоритм Евклида). Для любых целых чисел  $a$  и  $b$  существует наибольший общий делитель  $\text{НОД}(a, b)$ .

**Доказательство.** Чтобы найти  $\text{НОД}(a, b)$ , где  $a \geq b$ , сначала делят  $a = r_0$  на  $b = r_1$  и записывают частное  $q_1$  и остаток  $r_2 : r_0 = q_1 r_1 + r_2$ . Затем производят второе деление,  $r_1$  делят на  $r_2 : r_1 = q_2 r_2 + r_3$ . Затем делят  $r_2$  на  $r_3$  и так далее. Когда получается остаток, который является делителем предыдущего остатка, то этот последний ненулевой остаток и есть  $\text{НОД}(a, b)$ .

То есть:

$$\left\{ \begin{array}{ll} r_0 = r_1 q_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 = r_2 q_2 + r_3, & 0 \leq r_3 < r_2, \\ \dots & \dots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} = r_n q_n, & r_{n+1} = 0. \end{array} \right. \quad (3.1)$$

Покажем, что  $r_n = \text{НОД}(a, b)$ . Так как, рассматривая равенства (3.1), идя сверху вниз, убеждаемся, что общие делители чисел  $r_0$  и  $r_1$  одинаковы с общими делителями чисел  $r_1$  и  $r_2$ , далее одинаковы с общими делителями чисел  $r_2$  и  $r_3$ , чисел  $r_3$  и  $r_4, \dots$ , чисел  $r_{n-1}$  и  $r_n$ , наконец, с делителями одного числа  $r_n$ , являющегося последним не равным нулю остатком алгоритмом Евклида. Одновременно с этим имеем

$$\text{НОД}(r_0, r_1) = \text{НОД}(r_1, r_2) = \dots = \text{НОД}(r_{n-1}, r_n) = r_n.$$



**Определение 3.2.** Числа  $a$  и  $b$  называются *взаимно простыми*, если  $\text{НОД}(a, b) = 1$ .

**Теорема 3.3** (критерий взаимной простоты). Числа  $a$  и  $b$  взаимно просты, если и только если найдутся такие целые числа  $u$  и  $v$ , что  $au + bv = 1$ .

*Доказательство.* Если существуют такие  $u$ ,  $v$ , что  $au + bv = 1$ , то справедливость  $\text{НОД}(a, b) = 1$  очевидна.

Пусть  $\text{НОД}(a, b) = 1$ ,  $r_0 = a$ ,  $r_1 = b$ . Из (3.1) получаем следующую систему равенств:

$$\left\{ \begin{array}{l} a = bq_1 + r_2 \Rightarrow \frac{a}{b} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{r_1/r_2} \\ \frac{r_1}{r_2} = q_2 + \frac{1}{r_2/r_3} \Rightarrow \frac{a}{b} = q_1 + q_2 + \frac{1}{q_2 + r_2/r_3} \\ \dots \\ \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}}, \quad \frac{r_{n-1}}{r_n} = q_n \end{array} \right. \quad (3.2)$$

На основе системы (3.2) выпишем представление дроби  $a/b$  в виде цепной дроби:

$$\frac{r_0}{r_1} = \frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{1}{q_{n-2} + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

Определим подходящую дробь  $k$ -й глубины,  $k = \overline{1, n}$ , следую-

шим образом:

$$\begin{aligned} \frac{q_1}{1} &= \frac{P_1}{Q_1}, \\ q_1 + \frac{1}{q_2} &= \frac{q_1 q_2 + 1}{q_2} = \frac{P_2}{Q_2}, \\ q_1 + \frac{1}{q_2 + \frac{1}{q_3}} &= \frac{q_1 q_2 q_3 + q_1 + q_3}{q_2 q_3 + 1} = \frac{P_3}{Q_3}, \\ \dots \\ \frac{P_k}{Q_k} &= q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_{n-2} + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}, \end{aligned}$$

в частности,  $P_n/Q_n = a/b$ .

Докажем следующее рекуррентное соотношение методом математической индукции:

$$\frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}.$$

Положим  $P_0 = 1$ ,  $Q_0 = 0$ ,  $P_1 = q_1$ ,  $Q_1 = 1$ .

База индукции,  $k = 2$ :

$$\frac{P_2}{Q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0}.$$

Шаг индукции:  $P_{k+1}/Q_{k+1} = P'_k/Q'_k$ ,  $q'_i = q_i$ ,  $q'_k = q_k + 1/q_{k+1}$ ,  $i = \overline{1, k-1}$ . Далее, используя индуктивное предположение, бу-

дем иметь:

$$\begin{aligned} \frac{P'_k}{Q'_k} &= \frac{q'_k P'_{k-1} + P'_{k-2}}{q'_k Q'_{k-1} + Q'_{k-2}} = \frac{q'_k P_{k-1} + P_{k-2}}{q'_k Q_{k-1} + Q_{k-2}} = \\ &= \frac{(q_k + 1/q_{k+1}) P_{k-1} + P_{k-2}}{(q_k + 1/q_{k+1}) Q_{k-1} + Q_{k-2}} = \frac{P_k + P_{k-1}/q_{k+1}}{Q_k + Q_{k-1}/q_{k+1}} = \\ &= \frac{P_k q_{k+1} + P_{k-1}}{Q_k q_{k+1} + Q_{k-1}}. \end{aligned}$$

Таким образом, для числителя и знаменателя  $i$ -ой подходящей дроби справедливы следующие рекуррентные соотношения:

$$\left\{ \begin{array}{l} P_0 = 1, Q_0 = 0, \\ P_1 = q_1, Q_1 = 1, \\ Q_k = q_k Q_{k-1} + Q_{k-2}, \\ P_k = q_k P_{k-1} + P_{k-2}, \quad k = \overline{2, n-1} \\ P_n = a, Q_n = b. \end{array} \right. \quad (3.3)$$

Далее рассмотрим разность

$$\sigma_k = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_{k-1} Q_k} = \frac{\Delta_k}{Q_{k-1} Q_k}.$$

Заметим, что из (3.3) следует:

$$\begin{aligned} \Delta_1 &= P_1 Q_0 - Q_1 P_0 = -1, \\ \Delta_{k+1} &= P_{k+1} Q_k - Q_{k+1} P_k = \\ &= (q_{k+1} P_k + P_{k-1}) Q_k - (q_{k+1} Q_k + Q_{k-1}) P_k = \\ &= P_{k-1} Q_k - P_k Q_{k-1} = -(P_k Q_{k-1} - Q_k P_{k-1}) = -\Delta_k. \end{aligned}$$

Таким образом,  $\Delta_k = (-1)^k$ . В частности,

$$\Delta_n = P_n Q_{n-1} - Q_n P_{n-1} = a Q_{n-1} - b P_{n-1} = (-1)^n.$$

Следовательно,

$$1 = a(-1)^n Q_{n-1} + b(-1)^{n+1} P_{n-1}. \quad (3.4)$$

Отсюда получаем  $u = (-1)^n Q_{n-1}$ ,  $v = (-1)^{n+1} P_{n-1}$ . Теорема доказана.  $\square$

**Следствие 3.1.** Если  $d = \text{НОД}(a, b)$ , то существуют такие целые числа  $u, v$ , что  $d = au + bv$ .

*Доказательство.* Пусть  $a = a_1d$ ,  $b = b_1d$  и  $\text{НОД}(a_1, b_1) = 1$ . Из Теоремы 3.2 следует, что существуют такие целые числа  $u, v$ , что  $a_1u + b_1v = 1$ . Умножив обе части этого равенства на  $d$ , получим требуемый результат.  $\square$

## 3.2 Сравнения и их свойства

**Определение 3.3.** Пусть  $m > 1$ . Говорят, что  $a$  сравнимо с  $b$  по модулю  $m$  и пишут  $a \equiv b \pmod{m}$ , если  $m \mid (a - b)$  ( $a = b + tm$ ).

**Утверждение 3.1.** Если  $a \equiv b \pmod{m}$  и  $c \equiv d \pmod{m}$ , то  $a \pm c \equiv b \pm d \pmod{m}$  и  $ac \equiv bd \pmod{m}$ .

*Доказательство.*

$$\begin{aligned} a &= b + tm \\ c &= d + km \end{aligned} \Rightarrow ac = bd + Tm \Rightarrow ac \equiv bd \pmod{m}$$

$\square$

**Утверждение 3.2.**  $a \equiv b \pmod{m}$  тогда и только тогда, когда  $r_a = r_b$  (остатки от деления  $a$  и  $b$  на  $m$ ).

Доказать самостоятельно.

Легко проверить, что сравнение является отношением эквивалентности, то есть для неё выполняются свойства:

1.  $a \equiv a \pmod{m}$ ,
2. если  $a \equiv b \pmod{m}$ , то  $b \equiv a \pmod{m}$ ,
3. если  $a \equiv b \pmod{m}$  и  $b \equiv c \pmod{m}$ , то  $a \equiv c \pmod{m}$ .

*Классы эквивалентности:*

$$\mathbb{Z} = m\mathbb{Z} + \{1 + m\mathbb{Z}\} + \dots + \{m - 1 + m\mathbb{Z}\}.$$

*Фактор-множество:*

$$\mathbb{Z}/(m) = \{m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m - 1) + m\mathbb{Z}\}.$$

$\mathbb{Z}_m = \{0, 1, \dots, m - 1\}$  — кольцо вычетов по модулю  $m$  — полная система вычетов. Во множестве  $\mathbb{Z}_m$  операции сложения и умножения выполняются по следующему правилу

$$x + y = \begin{cases} x + y, & \text{если } x + y < m; \\ (x + y) - m, & \text{если } x + y \geq m. \end{cases}$$

$$xy = \begin{cases} xy, & \text{если } xy < m; \\ r_{xy}, & \text{если } xy \geq m, \end{cases}$$

где  $r_{xy}$  — остаток от деления  $xy$  на  $m$ .

**Определение 3.4.** Элемент  $a \in \mathbb{Z}_m$ ,  $a \neq 0$  обратим по модулю  $m$ , если существует такой элемент  $b$ , что  $ab \equiv 1 \pmod{m}$ . Элемент  $b$  в этом случае называется обратным к элементу  $a$  по модулю  $m$ . Обозначение:  $b \equiv a^{-1} \pmod{m}$ .

**Теорема 3.4** (критерий обратимости). Элемент  $a \in \mathbb{Z}_m$  обратим тогда и только тогда, когда  $\text{НОД}(a, m) = 1$ .

*Доказательство.* Необходимость следует из определения обратимости и Теоремы 3.3.

Достаточность — из формулы (3.4), а именно, если в (3.4) положить  $a = m$ , то

$$b^{-1} \pmod{m} = (-1)^{n+1} P_{n-1}.$$

Вычисление  $P_{n-1}$  производится по рекуррентным формулам (3.2):

$$P_k = q_k P_{k-1} + P_{k-2}, k = \overline{2, n-1}, P_0 = 1, P_1 = q_1,$$

где  $n$  — число шагов в алгоритме Евклида при нахождении НОД( $b, m$ ).  $\square$

**Пример 3.1.** Найти  $301^{-1} \pmod{800}$ .

Находим НОД(301, 800) по алгоритму Евклида:

$$\begin{aligned} 800 &= 301 \cdot 2 + 198 \\ 301 &= 198 \cdot 1 + 103 \\ 198 &= 103 \cdot 1 + 95 \\ 103 &= 95 \cdot 1 + 8 \\ 95 &= 8 \cdot 11 + 7 \\ 8 &= 7 \cdot 1 + 1 \\ 7 &= 1 \cdot 7. \end{aligned}$$

Таким образом,  $q_1 = 2$ ,  $q_2 = 1$ ,  $q_3 = 1$ ,  $q_4 = 1$ ,  $q_5 = 11$ ,  $q_6 = 1$ ,  $q_7 = 7$ ,  $n = 7$ .

Последовательно вычисляем  $P_2, \dots, P_7$  по формуле (3.2). Вычисления удобно производить в следующей таблице:

	$q_1 = 2$	$q_2 = 1$	$q_3 = 1$	$q_4 = 1$	$q_5 = 11$	$q_6 = 1$	$q_7 = 7$
1	2	3	5	8	93	101	800
$p_0$	$p_1$	$p_2$	$p_3$	$p_4$	$p_5$	$p_6$	$p_7$

Таким образом,  $301^{-1} \pmod{800} = (-1)^{7+1} \cdot 101 = 101$ .

### 3.3 Кольца, поля

**Определение 3.5.** Множество  $K$  называется *кольцом*, если в  $K$  определены две операции «+» (сложение) и «·» (умножение) и выполняются следующие условия (для любых  $a, b, c \in K$ ):

1.  $a + b \in K$ ,  $a \cdot b \in K$ ;
2.  $a + (b + c) = (a + b) + c$ ,  $a(bc) = (ab)c$ ;
3.  $a + b = b + a$ ;
4.  $(a + b)c = ac + bc$ ;
5. существует элемент  $0 \in K$  такой, что  $a + 0 = a$ .

6\*. Если существует такой элемент  $e \in K$ , что  $ae = ea = a$ , то  $K$  называется *кольцом с единицей «e»*.

7\*. Если  $ab = ba$ , то  $K$  называется *коммутативным кольцом*.

**Определение 3.6.** Коммутативное кольцо с единицей такое, что любой элемент, отличный от 0, имеет обратный элемент, называется *полем*.

**Примеры:**

- $\mathbb{Z}$  — коммутативное кольцо;
- $\mathbb{R}$  — поле;
- $\mathbb{Z}_2 = \{0, 1\}$  — поле;
- $F[x]$  — множество многочленов над полем — кольцо;
- $\mathcal{L}_n(F)$  — множество квадратных матриц размера  $n \times n$  над полем  $F$  — кольцо;
- $\mathbb{Z}_n$  — кольцо вычетов по модулю  $n$  — коммутативное кольцо с единицей.

**Определение 3.7.** Элемент  $d$  из кольца  $K$  называется *делителем нуля*, если существует такой элемент  $b \in K$ ,  $b \neq 0$ , что  $bd = 0$ .

Например, если  $K = \mathbb{Z}_{10} = \{0, 1, \dots, 9\}$ , то 2, 4, 5, 6, 8 — делители нуля:

$$\begin{aligned} 2 \cdot 5 &\equiv 0 \pmod{10}, \\ 4 \cdot 5 &\equiv 0 \pmod{10}, \\ 5 \cdot 6 &\equiv 0 \pmod{10}, \\ 5 \cdot 8 &\equiv 0 \pmod{10}. \end{aligned}$$

Если

$$L_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\},$$

то матрицы  $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$  и  $\begin{pmatrix} 0 & 0 \\ d & c \end{pmatrix}$  являются делителями нуля.

**Утверждение 3.3.** Конечное коммутативное кольцо с единицей и без делителей нуля является полем.

*Доказательство.* Для установления истинности утверждения достаточно показать, что любой элемент, отличный от 0, имеет обратный.

Пусть  $a \in K$ ,  $a \neq 0$ ,  $K = \{e, a_2, \dots, a_n\}$ .

Рассмотрим множество  $aK = \{a, aa_2, \dots, aa_n\}$ . Очевидно, что  $aK \subseteq K$ . Покажем, что  $aK = K$ , то есть  $aa_i \neq aa_j$  при  $i \neq j$ . Действительно, из  $aa_i = aa_j$  следует, что  $a(a_i - a_j) = 0$ . Так как  $a \neq 0$  и в кольце  $K$  нет делителей нуля, то  $a_i - a_j = 0$ , то есть  $a_i = a_j$ . Таким образом  $aK = K$ , поэтому найдётся  $i \in \{1, \dots, n\}$  такой, что  $aa_i = e$ . Это означает, что элемент  $a$  обратим,  $a^{-1} = a_i$ .  $\square$

**Утверждение 3.4.** Для любого  $f(x)$  и любого  $g(x) \neq 0$  из  $F[x]$  найдутся  $q(x)$  и  $r(x)$  такие, что

$$f(x) = g(x)q(x) + r(x), \quad 0 \leq \deg r(x) < \deg g(x). \quad (3.5)$$

*Доказательство.* Если  $\deg f(x) < \deg g(x)$ , то в (3.5) можно положить  $q(x) = 0$ ,  $r(x) = f(x)$ .

Пусть  $\deg f(x) \geq \deg g(x)$ ,

$$\begin{aligned} f(x) &= a_n x^n + \dots + a_1 x + a_0, \quad a_n \neq 0, \\ g(x) &= b_m x^m + \dots + b_1 x + b_0, \quad b_m \neq 0. \end{aligned}$$

Далее будем «делением столбиком» определять  $q(x)$ ,  $r(x)$ . Вычислим

$$\begin{aligned} r_1(x) &= f(x) - b_m^{-1} a_n x^{n-m} g(x) = \\ &= a_{n_1} x^{n_1} + a_{n_1-1} x^{n_1-1} + \dots + a_{11} x + a_{10}. \end{aligned}$$

Очевидно, что  $n_1 = \deg r_1(x) \leq n - 1$ . Далее, если  $n_1 < m$ , то

$$r_1(x) = r(x), \quad q(x) = b_m^{-1} a_n x^{n-m}.$$

В случае, когда  $n_1 \geq m$  вычисляем

$$\begin{aligned} r_2(x) &= b_m^{-1} a_{1n_1} x^{n_1-m} g(x) - r_1(x) = \\ &= a_{2n_2} x^{n_2} + \dots + a_{21} x + a_{20}, \quad n_2 < n_1. \end{aligned}$$

Если  $n_2 < m$ , то

$$\begin{aligned} f(x) &= (b_m^{-1} a_n x^{n-m} + b_m^{-1} a_{1n_1} x^{n_1-m}) g(x) + r_2(x) = \\ &= q(x)g(x) + r(x). \end{aligned}$$

Если  $n_2 \geq m$ , то вычислим

$$r_3(x) = b_m^{-1} a_{2n_2} x^{n_2-m} g(x) - r_2(x), \deg r_3(x) < \deg r_2(x).$$

Продолжим этот процесс, до тех пор, пока не будет выполняться неравенство  $\deg r_k(x) < m$ . В результате получим:

$$\begin{aligned} f(x) &= g(x) (b_m^{-1} a_n x^{n-m} + b_m^{-1} a_{1n_1} x^{n_1-m} + \dots + \\ &\quad + b_m^{-1} a_{kn_k} x^{n_{k-1}-m}) + r_k(x) = \\ &= g(x)q(x) + r(x), \quad r(x) = r_k(x). \end{aligned}$$

□

**Теорема 3.5 (Безу).** Если  $f(x) \in F[x]$ ,  $a \in F$  и  $f(a) = 0$ , то

$$f(x) = (x - a)q(x), \quad \deg q(x) = \deg f(x) - 1.$$

**Доказательство.** Разделим  $f(x)$  на  $(x - a)$ . Согласно предыдущему утверждению будем иметь  $f(x) = (x - a)q(x) + r(x)$ . Так как  $\deg r(x) < 1$ , то  $r(x) = c \in F$ .

По условию  $f(a) = 0$ . Поэтому,  $c = 0$  и мы получаем требуемый результат. □

**Следствие 3.2.** Многочлен  $f(x) \in F[x]$  степени  $n$  имеет в поле  $F$  не более  $n$  корней.

**Определение 3.8.** Множество элементов  $J$  кольца  $K$  называется левосторонним (правосторонним) идеалом, если

1. для любых элементов  $a, b \in J$  разность  $a - b \in J$ ;
2. для любого элемента  $a \in J$  и любого  $k \in K$  элемент  $ak$  ( $ka$ ) принадлежит  $J$ .

Если идеал одновременно является и левосторонним и правосторонним, то он называется *двусторонним идеалом* или просто *идеалом*.

Из определения следует, что любой идеал содержит хотя бы 0, то есть идеал — заведомо непустое подмножество кольца  $K$ . Рассмотрим несколько примеров идеалов.

- Нулевой идеал  $\Theta$  — идеал, содержащий только 0;
- единичный идеал  $J$  — идеал содержащий всё кольцо  $K$ , то есть  $J = K$ ;
- в кольце целых чисел идеалом является множество

$$J = m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\};$$

- другим примером идеала кольца целых чисел является идеал

$$J = \langle a, b \rangle = \{ma + nb \mid m, n \in \mathbb{Z}\},$$

где  $a, b$  — некоторые фиксированные целые числа.

**Определение 3.9.** Идеал  $J$  называется *главным*, если существует такой элемент  $a \in J$ , что для любого другого элемента  $b \in J$  найдётся элемент кольца  $k$  такой, что  $b = ak$ .

**Теорема 3.6.** В кольце многочленов  $F[x]$  над полем  $F$  и в кольце  $\mathbb{Z}$  целых чисел любой идеал главный.

*Доказательство.* Проведём доказательство для кольца  $F[x]$  (для  $\mathbb{Z}$  схема доказательства аналогична). Пусть  $J$  — ненулевой идеал в  $F[x]$ . Возьмём среди всех ненулевых многочленов из идеала  $J$  многочлен  $g$  минимальной степени. Докажем, что

$J = \langle g \rangle = \{gh \mid h \in F[x]\}$ . Пусть  $f$  — любой элемент идеала  $J$ . Разделим  $f$  на  $g$  с остатком:

$$f = gh + r, \deg r < \deg g.$$

Элемент  $gh$  принадлежит идеалу в силу определения идеала. Рассмотрим разность  $f - gh = r$ . Она также принадлежит идеалу. А значит и  $r \in J$ . Но  $r$  в силу выбора  $g$  может равняться только нулю, что и требовалось доказать.  $\square$

**Теорема 3.7** (о примитивном элементе). *Мультипликативная группа отличных от нуля элементов конечного поля циклическая.*

*Доказательство.* Пусть  $F = F_q$  — конечное поле из  $q$  элементов и  $F_q^* = F_q \setminus \{0\}$ . Очевидно, что  $F_q^*$  — группа и  $|F_q^*| = q - 1$ . Пусть  $q - 1 = p_1^{s_1} \cdots p_t^{s_t}$  — каноническое разложение числа  $q - 1$  на простые множители, где  $s_i \geq 1$ ,  $i = \overline{1, t}$ , и  $b$  — элемент из  $F_q^*$  максимального порядка. Из теоремы Лагранжа следует, что

$$m = \text{ord}(b) = p_1^{k_1} \cdots p_t^{k_t}, \quad 0 \leq k_i \leq s_i.$$

Если  $a \in F_q^*$ , то  $n = \text{ord}(a) \leq \text{ord}(b) = m$  и  $\text{ord}(a) = p_1^{r_1} \cdots p_t^{r_t}$ ,  $0 \leq r_i \leq s_i$ .

Пусть  $p^r \in \{p_1^{r_1}, \dots, p_t^{r_t}\}$ ,  $p^k \in \{p_1^{k_1}, \dots, p_t^{k_t}\}$  и

$$m = p^k w, \quad n = p^r u, \quad \text{НОД}(w, p) = \text{НОД}(u, p) = 1.$$

Рассмотрим элементы  $c = b^{p^k}$  и  $d = a^u$ . Очевидно, что  $\text{ord}(c) = w$ ,  $\text{ord}(d) = p^r$ . Учитывая, что  $cd = dc$ , применим лемму о порядке произведения двух элементов группы и получим:

$$\text{ord}(cd) = p^r w \leq p^k w,$$

откуда  $r_i \leq k_i$ ,  $i = \overline{1, t}$ .

Таким образом, мы установили, что для любого  $a \in F_q^*$   $\text{ord}(a) \mid m$ , то есть любой элемент  $a \in F_q^*$  является корнем уравнения  $f(x) = x^m - 1$ . Следовательно,  $m \geq q - 1$ . Но поскольку  $m \mid q - 1$ , то  $m = q - 1$ , то есть  $G$  — циклическая группа.  $\square$

### 3.4 Функции Эйлера и Мебиуса

Вернемся теперь к свойству делимости в кольце  $\mathbb{Z}$  и кольце вычетов по модулю  $n$ . Докажем следующую очень важную теорему.

**Теорема 3.8** (китайская теорема об остатках). *Пусть дана система взаимно простых чисел  $m_1, \dots, m_n$ , то есть*

$$\text{НОД}(m_i, m_j) = 1, \quad i, j = \overline{1, n}, \quad i \neq j.$$

*Пусть также  $M = m_1 \cdots m_n$ . Тогда система*

$$\{x = a_i \pmod{m_i}, i = \overline{1, n}\} \quad (3.6)$$

*имеет единственное решение по модулю  $M$  и это решение имеет вид*

$$X = \sum_{i=1}^n a_i M_i N_i \pmod{M}, \quad (3.7)$$

где  $M_i = M/m_i$ ,  $N_i = M_i^{-1} \pmod{m_i}$ ,  $i = \overline{1, n}$ .

**Доказательство.** Докажем сначала единственность решения по модулю  $M$ . Пусть  $X_1$  и  $X_2$  являются решениями системы (3.6) и  $X_0 = X_1 - X_2$ . Из (3.6) следует, что  $m_i \mid X_0$ ,  $i = \overline{1, n}$ . Из условия  $\text{НОД}(m_i, m_j) = 1$ ,  $i \neq j$  следует, что  $M \mid X_0$ . Следовательно  $X_1 = X_2 + kM$ , то есть  $X_1 \equiv X_2 \pmod{M}$ .

Далее, поскольку  $M_i N_i = 1 + t_i m_i$  и  $m_i \mid M_j$  при  $i \neq j$ , то из (3.7) получаем, что  $X \equiv a_i \pmod{m_i}$ ,  $i = \overline{1, n}$ . Таким образом,  $X$  — решение (3.6).  $\square$

**Следствие 3.3.** *Если  $m_1, \dots, m_k$  попарно простые, то равенство*

$$f(x) \equiv 0 \pmod{m_1 \cdots m_k} \quad (3.8)$$

*равносильно системе*

$$\begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ f(x) \equiv 0 \pmod{m_2}, \\ \dots \\ f(x) \equiv 0 \pmod{m_k}. \end{cases}$$

При этом, обозначив через  $T_1, \dots, T_k$  числа решений отдельных сравнений этой системы по соответствующим модулям и через  $T$  число решений сравнения (3.8), будем иметь

$$T = T_1 \cdots T_k.$$

Обозначим через  $\mathbb{Z}_n^* = \{a \in \mathbb{Z} \mid \text{НОД}(a, n) = 1\}$ . Таким образом,  $\mathbb{Z}_n^*$  — это множество элементов кольца  $\mathbb{Z}_n$ , обратимых по модулю  $n$ . Число элементов в  $\mathbb{Z}_n^*$ ,  $n \in \mathbb{Z}$  называют *функцией Эйлера* и обозначают через  $\varphi(n)$ , то есть  $\varphi(n) = |\mathbb{Z}_n^*|$ .

**Утверждение 3.5.** Множество  $\mathbb{Z}_n^*$  с операцией умножения по модулю  $n$  является мультипликативной абелевой группой.

*Доказательство.* Пусть  $a, b \in \mathbb{Z}_n^*$ . Это значит, что

$$\text{НОД}(a, n) = \text{НОД}(b, n) = 1.$$

Из критерия взаимной простоты следует, что существуют  $u_1, v_1$  и  $u_2, v_2$  такие, что

$$au_1 + v_1n = 1, \quad bu_2 + v_2n = 1.$$

Перемножим левые и правые части этих соотношений, получим

$$ab(u_1u_2) + (au_1v_2 + v_1u_2b + v_1v_2n)n = 1.$$

Следовательно,  $ab \in \mathbb{Z}_n^*$ . Справедливость ассоциативного закона сложения из его справедливости в кольце  $\mathbb{Z}_n$ . Очевидно, что  $1 \in \mathbb{Z}_n^*$  и, так как  $\text{НОД}(a^{-1}, n) = 1$ , то  $a^{-1} \in \mathbb{Z}_n^*$ .  $\square$

**Теорема 3.9 (Эйлер).** Если  $a \in \mathbb{Z}$  и  $\text{НОД}(a, n) = 1$ , то

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

*Доказательство.* Если  $\text{НОД}(a, n) = 1$ , то существует такое число  $a_0 \in \mathbb{Z}_n^*$ , что  $a_0 \equiv a \pmod{n}$  и  $\text{НОД}(a_0, n) = 1$ . Далее, так как  $a_0 \in \mathbb{Z}_n^*$ , и порядок любого элемента конечной группы есть делитель порядка группы, то  $a_0^{\varphi(n)} \equiv 1 \pmod{n}$ . Из свойств сравнений следует, что  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .  $\square$

**Утверждение 3.6** (теорема Ферма). *Если  $p$  простое и число  $a$  взаимно просто с  $p$ , то есть  $\text{НОД}(a, p) = 1$ , то*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Доказательство.* Справедливость следует из теоремы Эйлера и равенства  $\varphi(p) = p - 1$ .  $\square$

**Теорема 3.10** (свойство мультипликативности функции Эйлера). *Если  $\text{НОД}(m, n) = 1$ , то*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

*Доказательство.* По определению значение  $\varphi(mn)$  равно количеству чисел из  $\mathbb{Z}_{mn}$  взаимно простых с  $mn$ . Пусть  $j$  — произвольный элемент из  $\mathbb{Z}_{mn}$  и

$$\begin{aligned} j_1 &\equiv j \pmod{m}, j_1 \in \mathbb{Z}_m, \\ j_2 &\equiv j \pmod{n}, j_2 \in \mathbb{Z}_n. \end{aligned}$$

Из китайской теоремы об остатках следует, что пара  $(j_1, j_2)$  взаимнооднозначно соответствует  $j \in \mathbb{Z}_{mn}$ .

Далее заметим, что  $\text{НОД}(j, mn) = 1$  тогда и только тогда, когда  $\text{НОД}(j_1, m) = \text{НОД}(j_2, n) = 1$ . Действительно, из критерия взаимной простоты имеем, что если  $uj + vtn = 1$  и  $j = j_1 + mt$ , то  $j_1u + m(tu + vn) = 1$ . Таким образом,  $\text{НОД}(j_1, m) = 1$ . Аналогично устанавливается, что

$$\text{НОД}(j_2, n) = 1.$$

Пусть теперь  $\text{НОД}(j_1, m) = \text{НОД}(j_2, n) = 1$ . Покажем, что  $\text{НОД}(j, mn) = 1$ . Из  $\text{НОД}(m, n) = 1$ , следует, что достаточно установить, что  $\text{НОД}(j, m) = \text{НОД}(j, n) = 1$ . Так как  $j = j_1 + tm$ ,  $j = j_2 + sn$ , то из  $d | j$  и  $d | m$  будет следовать, что  $d | j_1$ . Но  $\text{НОД}(m, j_1) = 1$ , следовательно  $d = 1$ . Аналогично получаем, что из  $d | j$  и  $d | n$  следует, что  $d = 1$ . Из вышеизложенного следует, что

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\{(j_1, j_2) \mid j_1 \in \mathbb{Z}_m^*, j_2 \in \mathbb{Z}_n^*\}| = \\ = |\mathbb{Z}_m^*| |\mathbb{Z}_n^*| = \varphi(m)\varphi(n).$$

□

**Утверждение 3.7.** Если  $n = p_1^{k_1} \cdots p_t^{k_t}$  — каноническое разложение числа  $n$  в произведение степеней простых чисел, то

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

*Доказательство.* Покажем сначала, что для простого  $p$  и  $k > 1$

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Рассмотрим последовательность

$$1, 2, \dots, p, p+1, \dots, p^2-1, p^2, \dots, p^k-1.$$

Любое число из этой последовательности может быть однозначно записано в  $p$ -ичной системе счисления:

$$a = \alpha_0 + \alpha_1 p + \dots + \alpha_{k-1} p^{k-1}, \quad \alpha_i \in \mathbb{Z}_p, \quad i = \overline{0, k-1}.$$

Очевидно, что  $\text{НОД}(a, p) = \text{НОД}(a, p^k) \neq 1, a \neq 0$  тогда и только тогда, когда  $\alpha_0 = 0, \alpha_1, \alpha_2, \dots, \alpha_{k-1}$  одновременно не равны нулю. Количество таких чисел равно  $p^{k-1} - 1$ . Оставшиеся числа и только они, очевидно, взаимно прости с  $p^k$ . Поэтому

$$\varphi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Отсюда и свойства мультипликативности функции Эйлера следует справедливость доказываемого утверждения. □

**Теорема 3.11** (криптографическая теорема). Если  $n = pq$ ,  $p \neq q$ ,  $p, q$  простые, то для любого  $x \in \mathbb{Z}_n$  и любого  $k \in \mathbb{Z}$  справедливо сравнение

$$x^{k\varphi(n)+1} \equiv x \pmod{n}.$$



*Доказательство.* Рассмотрим случай, когда  $x$  и  $n$  взаимно просты, то есть  $\text{НОД}(x, n) = 1$ . Тогда по теореме Эйлера  $x^{\varphi(n)} \equiv 1 \pmod{n}$ . Отсюда и из свойств сравнений имеем  $x^{k\varphi(n)} \equiv 1 \pmod{n}$  при любом  $k \in \mathbb{Z}$ . Умножив теперь обе части получившегося равенства на  $x$ , будем иметь требуемое

$$x^{k\varphi(n)+1} \equiv x \pmod{n}.$$

Рассмотрим теперь второй случай  $\text{НОД}(x, n) > 1$ ,  $x \in \mathbb{Z}_n$ . Это означает, что либо  $p | x$  и  $q \nmid x$ , либо  $p \nmid x$  и  $q | x$ . Если  $p | x$  и  $q \nmid x$  (второй случай рассматривается аналогично) то по теореме Ферма получим  $x^{q-1} \equiv 1 \pmod{q}$ . Из свойств сравнений следует, что для любого  $k \in \mathbb{Z}$

$$x^{k(q-1)(p-1)} \equiv 1 \pmod{q}, \text{ то есть } x^{k(q-1)(p-1)} = 1 + qt.$$

Так как  $p | x$ , то  $x = ps$ . Поэтому, если умножить обе части последнего равенства на  $x$ , то получим

$$x^{k(p-1)(q-1)+1} = x + pqst, \text{ то есть } x^{k(p-1)(q-1)} \equiv x \pmod{n}.$$

□

**Замечание 3.1.** Доказанная теорема математически обосновывает корректность алгоритмов шифрования и расшифрования крипtosистемы с открытым ключом RSA.

**Определение 3.10.** Функция  $f(n)$  натурального аргумента называется *мультипликативной*, если  $f(n) \neq 0$  и для любых взаимно простых  $m$  и  $n$  выполнено соотношение

$$f(mn) = f(m)f(n).$$

Примерами мультипликативных функций являются функция Эйлера и  $f(n) = n^s$  ( $s \geq 0$ ).

В дальнейшем будем считать, что  $f(1) = 1$  и  $n$  имеет следующее каноническое разложение на простые множители

$$n = p_1^{k_1} \cdots p_t^{k_t}.$$

**Определение 3.11.** Функция  $\mu(n)$ , определяемая соотношением

$$\mu(n) = \begin{cases} 1, & \text{если } n=1; \\ (-1)^t, & \text{если } n \text{ свободно от квадратов;} \\ 0, & \text{иначе,} \end{cases}$$

называется *функцией Мёбиуса*.

**Упражнение 3.1.** Доказать, что функция Мёбиуса мультипликативна.

**Утверждение 3.8.** Если  $f(n)$  мультипликативная функция, то

$$\sum_{d|n} f(d) = \prod_{i=1}^t \left( \sum_{j=0}^{k_i} f(p_i^j) \right) \quad (3.9)$$

**Доказательство.** Раскроем скобки в правой части выражения (3.9). В результате получим, что она будет состоять из попарно различных выражений вида

$$A_{(r_1, \dots, r_t)} = f(p_1^{r_1}) \cdots f(p_t^{r_t}), \quad 0 \leq r_i \leq k_i.$$

Из мультипликативности функции  $f$  следует, что

$$A_{(r_1, \dots, r_t)} = f(p_1^{r_1} \cdots p_t^{r_t}).$$

Очевидно, что  $d = p_1^{r_1} \cdots p_t^{r_t}$  пробегает множество всех делителей числа  $n$ .  $\square$

**Следствие 3.4.** Если в (3.9) положить  $f(n) = n^s$ , то получим

$$\sum_{d|n} d^s = \begin{cases} \prod_{i=1}^t \frac{p_i^{s(k_i+1)} - 1}{p_i^s - 1}, & \text{если } s \geq 1; \\ \prod_{i=1}^t (k_i + 1), & \text{если } s = 0. \end{cases} \quad (3.10)$$

При  $s = 1$  из (3.10) получим формулу для суммы всех делителей числа  $n$ :

$$\sum_{d|n} d = \prod_{i=1}^t \frac{p_i^{k_i+1} - 1}{p_i - 1}. \quad (3.11)$$

При  $s = 0$  формула (3.10) даёт нам выражение для количества делителей числа  $n$ .

**Утверждение 3.9.** Если  $f(n)$  – мультипликативная функция, то

$$\sum_{d|n} \mu(d)f(d) = \prod_{i=1}^t (1 - f(p_i)). \quad (3.12)$$

*Доказательство.* Функция  $g(n) = \mu(n)f(n)$  мультипликативная и  $g(p_i) = \mu(p_i)f(p_i) = -f(p_i)$ ,  $g(p_i^j) = 0$ , если  $j \geq 2$ . Отсюда и из (3.9) получаем

$$\sum_{d|n} g(d) = \sum_{d|n} \mu(d)f(d) = \prod_{i=1}^t \left( \sum_{j=0}^1 g(p_i^j) \right) = \prod_{i=1}^t (1 - f(p_i)).$$

□

**Следствие 3.5.** Для любого натурального числа  $n$  справедливо тождество

$$\sum_{d|n} \mu(d) = \begin{cases} 0, & \text{если } n > 1; \\ 1, & \text{если } n = 1. \end{cases} \quad (3.13)$$

*Доказательство.* Справедливость утверждения прямо следует из соотношения (3.12) при  $f(n) = 1$ . □

**Следствие 3.6.** Для любого натурального числа  $n$  справедливо тождество

$$\sum_{d|n} \frac{\mu(d)}{d} = \begin{cases} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right), & \text{если } n > 1; \\ 1, & \text{если } n = 1. \end{cases}$$

*Доказательство.* Справедливость утверждения прямо следует из соотношения (3.12) при  $f(n) = 1/n$ .  $\square$

**Теорема 3.12** (формула обращения Мёбиуса). *Если для некоторых функций  $F$  и  $G$  соотношение*

$$G(n) = \sum_{d|n} F(d)$$

*справедливо для любого натурального  $n$ , то*

$$F(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right).$$

*Доказательство.* Представим  $n$  в виде  $n = p_1^{k_1} \cdots p_t^{k_t}$ . Тогда условие теоремы примет вид

$$G\left(\prod_{i=1}^t p_i^{k_i}\right) = \sum_{i_1=0}^{k_1} \cdots \sum_{i_t=0}^{k_t} F\left(\prod_{j=1}^t p_j^{i_j}\right).$$

Это соотношение должно быть справедливо для любого  $n$ , значит

$$G\left(p_1^{k_1-1} \prod_{i=2}^t p_i^{k_i}\right) = \sum_{i_1=0}^{k_1-1} \cdots \sum_{i_t=0}^{k_t} F\left(\prod_{j=1}^t p_j^{i_j}\right).$$

Откуда

$$\begin{aligned} G\left(\prod_{i=1}^t p_i^{k_i}\right) - G\left(p_1^{k_1-1} \prod_{i=2}^t p_i^{k_i}\right) &= \\ &= \sum_{i_2=0}^{k_2} \cdots \sum_{i_t=0}^{k_t} F\left(p_1^{k_1} \prod_{j=2}^t p_j^{i_j}\right). \end{aligned}$$

Последнее соотношение можно переписать в эквивалентном виде

$$\sum_{r_1=0}^1 (-1)^{r_1} G\left(p_1^{k_1-r_1} \prod_{i=2}^t p_i^{k_i}\right) = \sum_{i_2=0}^{k_2} \cdots \sum_{i_t=0}^{k_t} F\left(p_1^{k_1} \prod_{j=2}^t p_j^{i_j}\right).$$

Это соотношение выполняется для любого  $n$ , поэтому в нём можно заменить  $p_2^{k_2}$  на  $p_2^{k_2-1}$  и оно останется истинным. Следовательно,

$$\begin{aligned} \sum_{r_1=0}^1 (-1)^{r_1} \left[ G \left( p_1^{k_1-r_1} p_2^{k_2} \prod_{i=3}^t p_i^{k_i} \right) - \right. \\ \left. - G \left( p_1^{k_1-r_1} p_2^{k_2-1} \prod_{i=3}^t p_i^{k_i} \right) \right] = \\ = \sum_{i_3=0}^{k_3} \cdots \sum_{i_t=0}^{k_t} F \left( p_1^{k_1} p_2^{k_2} \prod_{j=3}^t p_j^{k_j} \right). \end{aligned}$$

А это эквивалентно соотношению

$$\begin{aligned} \sum_{r_1=0}^1 \sum_{r_2=0}^1 (-1)^{r_1+r_2} G \left( p_1^{k_1-r_1} p_2^{k_2-r_2} \prod_{i=3}^t p_i^{k_i} \right) = \\ = \sum_{i_3=0}^{k_3} \cdots \sum_{i_t=0}^{k_t} F \left( p_1^{k_1} p_2^{k_2} \prod_{j=3}^t p_j^{i_j} \right). \end{aligned}$$

Индуктивно продолжая эту процедуру, получим соотношение

$$\begin{aligned} F(p_1^{k_1} \cdots p_t^{k_t}) = \\ = \sum_{r_1=0}^1 \cdots \sum_{r_t=0}^1 (-1)^{r_1+\cdots+r_t} G(p_1^{k_1-r_1} \cdots p_t^{k_t-r_t}). \end{aligned}$$

Далее, заметим, что  $(-1)^{r_1+\cdots+r_t} = \mu(p_1^{r_1} \cdots p_t^{r_t})$  и  $\mu(d) = 0$ , если  $d$  несвободно от квадратов, то есть если  $p_i^2 \mid d$  для некоторого  $i$ . В силу этого полученное соотношение можно записать в виде

$$\begin{aligned} F(n) = \sum_{r_1=0}^{k_1} \cdots \sum_{r_t=0}^{k_t} \mu(p_1^{r_1} \cdots p_t^{r_t}) G \left( \frac{p_1^{k_1} \cdots p_t^{k_t}}{p_1^{r_1} \cdots p_t^{r_t}} \right) = \\ = \sum_{d \mid n} \mu(d) G \left( \frac{n}{d} \right). \end{aligned}$$

Что и требовалось доказать.  $\square$

**Следствие 3.7.** Для любого натурального  $n$  справедливо равенство

$$\varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right). \quad (3.14)$$

*Доказательство.* Несложно установить, что для любого натурального  $n$  справедливо тождество

$$n = \sum_{d|n} \varphi(d).$$

Положим  $G(n) = n$  и  $F(n) = \varphi(n)$ . Тогда из теоремы 3.12 получаем

$$\varphi(n) = \sum_{d'|n} \mu(d') \frac{n}{d'},$$

произведя замену  $\frac{n}{d'} = d$ ,  $d' = \frac{n}{d}$ , получим соотношение (3.14).  $\square$

**Упражнение 3.2.** Доказать, что для любого натурального  $n$  справедливо равенство

$$n = \sum_{d|n} \varphi(d).$$



## Глава 4

# Квадратичные вычеты

### 4.1 Определение и свойства

Пусть  $m \in \mathbb{Z}$ ,  $m > 1$ . Рассмотрим сравнение

$$x^2 \equiv a \pmod{m}. \quad (4.1)$$

**Определение 4.1.** Число  $a \in \mathbb{Z}_m$  называется *квадратичным вычетом (квадратичным невычетом) по модулю  $m$* , если сравнение (4.1) имеет (соответственно, не имеет) решений.

Например, если  $m = 6$ , то  $1, 3, 4$  — это вычеты по модулю 6, а  $2, 5$  — невычеты.

**Утверждение 4.1.** Если  $p$  простое,  $p \geq 3$ , то число квадратичных вычетов (и невычетов) по модулю  $p$  равно  $\frac{p-1}{2}$  и квадратичный вычет — это суть элемент множества:

$$1, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p}.$$

*Доказательство.* Действительно, так как

$$\mathbb{Z}_p^* = \left\{ -\frac{p-1}{2}, -\frac{p-1}{2} + 1, \dots, -1, 2, \dots, \frac{p-1}{2} \right\},$$

то множество

$$(\mathbb{Z}_p^*)^2 = \left\{ 1, 2^2, \dots, \left( \frac{p-1}{2} \right)^2 \right\}$$

есть множество всех вычетов по модулю  $p$ . Остальные элементы из  $\mathbb{Z}_p^*$  являются невычетами.  $\square$

**Теорема 4.1.** Пусть  $p$  простое,  $p \geq 3$  и  $a \in \mathbb{Z}_p^*$ . Тогда

$$a^{\frac{p-1}{2}} \pmod{p} = \begin{cases} 1, & \text{если } a \text{ — вычет;} \\ -1, & \text{если } a \text{ — невычет.} \end{cases}$$

*Доказательство.* По теореме Ферма для  $a \in \mathbb{Z}_p^*$  выполняется сравнение

$$a^{p-1} \equiv 1 \pmod{p}.$$

Учитывая, что  $p-1$  — четное число, получим:

$$\left( a^{\frac{p-1}{2}} - 1 \right) \left( a^{\frac{p-1}{2}} + 1 \right) \equiv 0 \pmod{p}. \quad (4.2)$$

Теперь пусть  $a$  — квадратичный вычет. Это значит, что найдется  $x_0 \in \mathbb{Z}_p^*$  такое, что  $x_0^2 \equiv a \pmod{p}$ . Отсюда, с учетом теоремы Ферма, будем иметь:

$$a^{\frac{p-1}{2}} - 1 \equiv x_0^{p-1} - 1 \equiv 0 \pmod{p}.$$

Таким образом, в (4.2) множитель  $a^{\frac{p-1}{2}} - 1$  для любого вычета  $a$  обращается в 0 ( $\pmod{p}$ ). Это означает, что любой вычет  $a \in \mathbb{Z}_p^*$  является корнем многочлена  $f(x) = x^{\frac{p-1}{2}} - 1$ . Так как  $\mathbb{Z}_p$  — поле, а число вычетов по модулю  $p$  равно  $(p-1)/2$ , то только для квадратичных вычетов  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .

Если  $a$  — квадратичный невычет, то  $a^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}$ . Тогда, учитывая, что в поле  $\mathbb{Z}_p$  нет делителей нуля, из (4.2) получим, что для любого невычета  $a \in \mathbb{Z}_p^*$ ,  $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ .



Следовательно, любой невычет есть корень многочлена  $g(x) = x^{\frac{p-1}{2}} + 1$ . Поскольку число невычетов совпадает со степенью многочлена, то тем самым мы установим, что для любого квадратичного невычета  $a \in \mathbb{Z}_p^*$  выполняется условие  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .  $\square$

## 4.2 Символ Лежандра

**Определение 4.2.** Символом Лежандра целого числа  $a$  относительно простого числа  $p$  называется число

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } p \mid a; \\ 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p. \end{cases}$$

### Свойства символа Лежандра

1.  $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$ .

Если  $p \mid a$ , то по определению символа Лежандра равенство верно. В случае  $\text{НОД}(a, p) = 1$ , справедливость следует из Теоремы 4.1.

2. Если  $a \equiv a_1 \pmod{p}$ , то  $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$ .

Справедливость следует из того, что сравнения  $x^2 \equiv a \pmod{p}$  и  $x^2 \equiv a_1 \pmod{p}$ , при условии, что  $a \equiv a_1 \pmod{p}$  либо разрешимы, либо неразрешимы.

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

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

Справедливость 3 и 4 следует из определения символа Лежандра и Теоремы 4.1.

5. Для любых  $a_1, \dots, a_k \in \mathbb{Z}$

$$\left( \frac{a_1 \cdots a_k}{p} \right) = \left( \frac{a_1}{p} \right) \cdots \left( \frac{a_k}{p} \right).$$

Справедливость следует из теоремы 4.1 и свойств сравнений.

6. Из свойства 5 в качестве следствия получаем, что для любых  $a, b \in \mathbb{Z}$

$$\left( \frac{ab^2}{p} \right) = \left( \frac{a}{p} \right).$$

Пусть  $p_1 = \frac{p-1}{2}$ ,  $\mathcal{Z}_{p_1} = \{1, \dots, p_1\}$ ,  $a \in \mathbb{Z}_p^*$ . Тогда для любого  $i \in \mathcal{Z}_{p_1}$ ,  $ai \equiv \pm r_i = \varepsilon_i r_i \pmod{p}$ , где  $r_i \in \mathcal{Z}_{p_1}$ ,  $r_i \neq r_j$  при  $i \neq j$ ,  $\varepsilon_i = \pm 1$  и поэтому

$$\prod_{i=1}^{p_1} a \cdot i = a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdots p_1 \equiv \varepsilon_1 \cdots \varepsilon_{p_1} \cdot r_1 \cdots r_{p_1} \pmod{p}.$$

Откуда, учитывая, что  $\mathcal{Z}_{p_1} = \{r_1, \dots, r_{p_1}\}$ , после сокращения получим

$$\left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p} = \varepsilon_1 \cdots \varepsilon_{p_1}. \quad (4.3)$$

**Лемма 4.1.** Для любого  $a \in \mathbb{Z}_p^*$

$$\left( \frac{a}{p} \right) = (-1)^{\sum_{i=1}^{p_1} \left[ \frac{2ai}{p} \right]}. \quad (4.4)$$

*Доказательство.* Пусть  $i \in \mathcal{Z}_{p_1}$ ,  $a \in \mathbb{Z}_p^*$ ,  $ai/p = k + \delta$ , где  $k = [ai/p]$ ,  $0 \leq \delta < 1$ . Тогда  $2ai/p = 2k + 2\delta$ . Отсюда следует, что

$$\left[ \frac{2ai}{p} \right] = 2 \left[ \frac{ai}{p} \right] + [2\delta].$$

Если  $\delta > 1/2$ , т.е.  $ai > p/2$ , то  $\varepsilon_i = -1$  и  $[2ai/p]$  — нечётное число. Если  $\delta < 1/2$ , т.е.  $ai < p/2$ , то  $\varepsilon_i = +1$  и  $[2ai/p]$  — чётное число.

Таким образом, мы установили, что  $\varepsilon_i = (-1)^{[2ai/p]}$ ,  $i \in \mathbb{Z}_{p_1}$ . Отсюда и из (4.3) получаем (4.4).  $\square$

**Лемма 4.2.** *Если  $a$  нечётное,  $\text{НОД}(a, p) = 1$ ,  $p$  простое,  $p \geq 3$ , то*

$$\left(\frac{2a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right] + \frac{p^2-1}{8}}. \quad (4.5)$$

*Доказательство.* Справедливость (4.5) вытекает из доказанных свойств символа Лежандра и Леммы 4.1:

$$\begin{aligned} \left(\frac{2a}{p}\right) &= \left(\frac{2a+2p}{p}\right) = \left(\frac{4\left(\frac{a+p}{2}\right)}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = \\ &= (-1)^{\sum_{i=1}^{p_1} \left[\frac{(a+p)i}{p}\right]} = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p} + i\right]} = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right] + \sum_{i=1}^{p_1} i} = \\ &= (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right] + \frac{p^2-1}{8}} \end{aligned}$$

 $\square$ 

Если в (4.5) положить  $a = 1$ , то получим

$$7. \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

**Следствие 4.1.** *Если  $a$  нечётное, то*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right]}.$$

**Теорема 4.2.** *Пусть  $p$  и  $q$  — различные нечетные простые числа. Тогда*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

*Доказательство.* Пусть  $p_1 = \frac{p-1}{2}$ ,  $q_1 = \frac{q-1}{2}$  и

$$\Omega = \{(qi, pj) | i = \overline{1, p_1}, j = \overline{1, q_1}\}.$$

Очевидно, что  $|\Omega| = p_1 q_1$ . Заметим, что  $qi \neq pj$ . Это следует из того, что  $i < (p-1)/2$ ,  $j < (q-1)/2$  и  $p \nmid (qi)$  и  $q \nmid (pj)$ .

Рассмотрим следующие множества:

$$\Omega_1 = \bigcup_{j=1}^{q_1} \Omega_{1j},$$

$$\text{где } \Omega_{1j} = \begin{cases} \emptyset, & \text{если } \left[ \frac{pj}{q} \right] = 0 \\ \{(qi, pj) | 1 \leq i \leq \left[ \frac{pj}{q} \right]\} & \text{иначе} \end{cases}$$

$$\Omega_2 = \bigcup_{i=1}^{p_1} \Omega_{2i},$$

$$\text{где } \Omega_{2i} = \begin{cases} \emptyset, & \text{если } \left[ \frac{qi}{p} \right] = 0 \\ \{(qi, pj) | 1 \leq j \leq \left[ \frac{qi}{p} \right]\} & \text{иначе} \end{cases}$$

Нетрудно видеть, что  $\Omega_1 \cap \Omega_2 = \emptyset$  и  $\Omega_1 \cup \Omega_2 = \Omega$ . Из определения  $\Omega_1$  и  $\Omega_2$  следует, что

$$|\Omega_1| = \sum_{j=1}^{q_1} \left[ \frac{pj}{q} \right], \quad |\Omega_2| = \sum_{i=1}^{p_1} \left[ \frac{qi}{p} \right].$$

Отсюда, учитывая следствие 4.1, получаем:

$$\left( \frac{p}{q} \right) = (-1)^{|\Omega_1|}, \quad \left( \frac{q}{p} \right) = (-1)^{|\Omega_2|}.$$

Перемножив левые и правые части последних равенств, получим:

$$\left( \frac{q}{p} \right) \left( \frac{p}{q} \right) = (-1)^{|\Omega_1|+|\Omega_2|} = (-1)^{|\Omega|} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$



Следовательно,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

### 4.3 Символ Якоби

Обобщением символа Лежандра является символ Якоби.

**Определение 4.3.** Пусть  $P$  нечётное, больше единицы, и  $P = p_1 \cdots p_r$  — его разложение на простые множители (среди них могут быть и равные). Тогда *символ Якоби*  $\left(\frac{a}{P}\right)$  определяется равенством:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

Исходя из известных свойств символа Лежандра можно получить аналогичные свойства для символа Якоби.

#### Свойства символа Якоби

- Если  $a \equiv a_1 \pmod{P}$ , то

$$\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right).$$

Действительно,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) = \left(\frac{a_1}{p_1}\right) \cdots \left(\frac{a_1}{p_r}\right) = \left(\frac{a_1}{P}\right),$$

потому что  $a$ , будучи сравнимо с  $a_1$  по модулю  $P$ , будет сравнимо с  $a_1$  и по модулям  $p_1, \dots, p_r$ , которые являются делителями  $P$ .

$$2. \left(\frac{1}{P}\right) = 1.$$

В самом деле,

$$\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right) \cdots \left(\frac{1}{p_r}\right) = 1.$$

$$3. \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

По определению имеем:

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2}}.$$

С другой стороны

$$\begin{aligned} \frac{P-1}{2} &= \frac{p_1 \cdots p_r - 1}{2} = \\ &= \frac{\left(1 + 2^{\frac{p_1-1}{2}}\right) \cdots \left(1 + 2^{\frac{p_r-1}{2}}\right) - 1}{2} = \\ &= \frac{p_1 - 1}{2} + \cdots + \frac{p_r - 1}{2} + 2N. \end{aligned}$$

Следовательно,

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

$$4. \left(\frac{ab \dots l}{P}\right) = \left(\frac{a}{P}\right) \left(\frac{b}{P}\right) \cdots \left(\frac{l}{P}\right).$$

Действительно,

$$\begin{aligned} \left(\frac{ab \dots l}{P}\right) &= \left(\frac{ab \dots l}{p_1}\right) \cdots \left(\frac{ab \dots l}{p_r}\right) = \\ &= \left(\frac{a}{p_1}\right) \left(\frac{b}{p_1}\right) \cdots \left(\frac{l}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) \left(\frac{b}{p_r}\right) \cdots \left(\frac{l}{p_r}\right). \end{aligned}$$

Собирая символы с одинаковыми числителями, мы и получим утверждаемое свойство.

Отсюда получаем следствие:

$$5. \left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right).$$

$$6. \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Действительно,

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_r}\right) = (-1)^{\frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8}},$$

но

$$\begin{aligned} \frac{P^2 - 1}{8} &= \frac{p_1^2 \cdots p_r^2 - 1}{8} = \\ &= \frac{\left(1 + 8\frac{p_1^2-1}{8}\right) \cdots \left(1 + 8\frac{p_r^2-1}{8}\right) - 1}{8} = \\ &= \frac{p_1^2 - 1}{8} + \cdots + \frac{p_r^2 - 1}{8} + 2N. \end{aligned}$$

Следовательно,

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

7. Если  $P$  и  $Q$  положительные нечётные взаимно простые, то

$$\left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right) (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

Пусть  $Q = q_1 \cdots q_s$  и  $P = p_1 \cdots p_r$ , тогда

$$\begin{aligned} \left(\frac{Q}{P}\right) &= \left(\frac{Q}{p_1}\right) \cdots \left(\frac{Q}{p_r}\right) = \prod_{\alpha=1}^r \prod_{\beta=1}^s \left(\frac{q_\beta}{p_\alpha}\right) = \\ &= (-1)^{\sum_{\alpha=1}^r \sum_{\beta=1}^s \frac{p_\alpha-1}{2} \cdot \frac{q_\beta-1}{2}} \prod_{\alpha=1}^r \prod_{\beta=1}^s \left(\frac{p_\alpha}{q_\beta}\right) = \\ &= (-1)^{\left(\sum_{\alpha=1}^r \frac{p_\alpha-1}{2}\right) \left(\sum_{\beta=1}^s \frac{q_\beta-1}{2}\right)} \left(\frac{P}{Q}\right). \end{aligned}$$

Но, как было показано при доказательстве свойства 3,

$$\frac{P-1}{2} = \sum_{\alpha=1}^r \frac{p_\alpha - 1}{2} + 2N,$$

$$\frac{Q-1}{2} = \sum_{\beta=1}^s \frac{q_\beta - 1}{2} + 2N_1,$$

поэтому

$$\left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right) (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

#### 4.4 Алгоритмы решения квадратичного сравнения по простому модулю

**Утверждение 4.2.** Если  $p = 8m + 5$ ,  $p$  простое и  $\left(\frac{a}{p}\right) = 1$ , то сравнение

$$x^2 \equiv a \pmod{p}$$

имеет решение

$$x = \pm a^{m+1} \cdot 2^{(2m+1)\sigma(a)} \pmod{p}, \quad \sigma(a) \in \{0, 1\}.$$

*Доказательство.* Из условия утверждения имеем:

$$\left(\frac{a}{p}\right) = a^{4m+2} = (a^{2m+1})^2 \equiv 1 \pmod{p}.$$

Отсюда следует, что  $a^{2m+1} = \pm 1$ .

Если  $a^{2m+1} \equiv 1 \pmod{p}$ , то  $a^{2m+2} \equiv a \pmod{p}$  и, следовательно,  $x = \pm a^{m+1}$ . При этом  $\sigma(a) = 0$ .

Пусть  $a^{2m+1} \equiv -1 \pmod{p}$ . Заметим, что

$$\begin{aligned} \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}} = (-1)^{(2m+1)(4m+3)} = -1 \equiv \\ &\equiv 2^{\frac{p-1}{2}} \equiv (2^{2m+1})^2 \pmod{p}. \end{aligned}$$

Поэтому, из  $a^{2m+1} \equiv -1 \pmod{p}$  следует, что

$$(2^{2m+1})^2 (a^{m+1})^2 \equiv a \pmod{p}.$$

Таким образом, в этом случае  $x = \pm a^{m+1} \cdot 2^{2m+1}$  и  $\sigma(a) = 1$ .  $\square$

**Утверждение 4.3.** При  $p = 4m + 3$ ,  $(\frac{a}{p}) = 1$ , решение сравнения  $x^2 \equiv a \pmod{p}$  имеет вид  $x = \pm a^{m+1}$ .

*Доказательство.* Так как  $a$  — квадратичный вычет, то

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

По условию  $p = 4m + 3$ , следовательно,  $a^{2m+1} \equiv 1 \pmod{p}$ , где  $\text{НОД}(a, p) = 1$ . Домножим обе части последнего сравнения на  $a$ . Получим

$$a^{2m+2} = (a^{m+1})^2 \equiv a \pmod{p}.$$

Следовательно,  $x = \pm a^{m+1}$ . Исходное сравнение имеет степень 2. Поэтому мы нашли все его решения.  $\square$

Дадим обоснование алгоритма решения сравнений  $x^2 \equiv a \pmod{p}$  ( $p \geq 3$ ) при условии, что  $(\frac{a}{p}) = 1$  и дан элемент  $b \in \mathbb{Z}_p$  такой, что  $(\frac{b}{p}) = -1$ .

1. Представляем  $p - 1$  в виде  $p - 1 = 2^m \cdot s$ ,  $\text{НОД}(s, 2) = 1$ .

Если  $m = 1$ , то  $p \equiv 3 \pmod{4}$  и в этом случае применяем Утверждение 2.5.

Если  $m \geq 2$ , то переходим к следующему шагу.

2. Вычислим  $c = b^s \pmod{p}$ , тогда  $(\frac{c}{p}) = (\frac{b}{p})^s = -1$ .

3. Вычислим  $r = a^{\frac{s+1}{2}} \pmod{p}$ ,  $m \geq 2$ . Элемент  $r$  удовлетворяет сравнению

$$\left(\frac{r^2}{a}\right)^{2^{m-1}} = a^{s \cdot 2^{m-1}} = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = 1 \pmod{p}. \quad (4.6)$$

4. Покажем, что  $v = \text{ord}(c) = 2^m \pmod{p}$ . В самом деле,

$$c^{2^m} = b^{s \cdot 2^m} = b^{p-1} \equiv 1 \pmod{p}.$$

Таким образом,  $v \mid 2^m$ , то есть  $v = 2^n$ ,  $n \leq m$ . Допустим, что  $n < m$ . Тогда, если  $\mathbb{Z}_p^* = \langle g \rangle$ ,  $\text{ord}(g) = p - 1$ , то согласно, согласно свойству подгруппы циклической группы,  $c \in \langle g^{2^{m-n}s} \rangle$ , то есть  $c = g^{2^{m-n} \cdot sw} = g^{2N}$ , откуда  $(\frac{c}{p}) = (\frac{g}{p})^{2N} = 1$ . Пришли к противоречию с условием  $(\frac{c}{p}) = -1$ . Поэтому  $m = n$  и  $\langle c \rangle = \langle g^s \rangle$ , то есть  $g^s \equiv c^u \pmod{p}$  для некоторого  $u \in \mathbb{N}$ .

Из (4.6) следует, что  $\text{ord}(a^{-1}r^2) \mid 2^{m-1}$ ,  $m \geq 2$ , то есть  $\text{ord}(a^{-1}r^2) = 2^l$ ,  $l < m$ . Поэтому  $a^{-1}r^2 \in \langle g^{2^{m-l}s} \rangle = \langle c^{2^{m-l} \cdot u} \rangle$ , следовательно,  $a^{-1}r^2 = c^{2i} \in \langle c \rangle$ , где  $i = 2^{m-l-1}u$ . Поэтому

$$r^2 c^{-2i} \equiv a \pmod{p}$$

что эквивалентно

$$r^2 c^{2j} \equiv a \pmod{p}$$

откуда

$$(rc^j)^2 \equiv a \pmod{p}$$

Таким образом,  $x = \pm rc^j$ , где  $j = \overline{1, 2^m - 1}$ .

5. Будем искать  $j$  в виде двоичного представления:

$$j = j_0 + j_1 \cdot 2 + \cdots + j_{m-1} \cdot 2^{m-1}.$$

Заметим, что если  $j_{m-1} = 1$ , то, учитывая, что  $c^{2^{m-1}} \equiv -1 \pmod{p}$ , будем иметь  $c^j r = -c^{j'} r$ , где

$$j' = j_0 + j_1 \cdot 2 + \cdots + j_{m-2} \cdot 2^{m-2}.$$

Поэтому, не ограничивая общности рассуждений, можно считать, что  $j_{m-1} = 0$ .

Итак, решение сравнения  $x^2 \equiv a \pmod{p}$  будем искать в виде:

$$x = \pm c^{j_0 + j_1 \cdot 2 + \cdots + j_{m-2} \cdot 2^{m-2}} \cdot r$$



Откуда следует, что

$$c^{2 \cdot j_0 + 2^2 \cdot j_1 + \dots + 2^{m-1} \cdot j_{m-2}} \cdot \left(\frac{r^2}{a}\right) \equiv 1 \pmod{p}. \quad (4.7)$$

Так как  $\left(\frac{r^2}{a}\right)^{2^{m-1}} = 1$ , (см (4.6)) то  $\left(\frac{r^2}{a}\right)^{2^{m-2}} = \varepsilon_0$ ,  $\varepsilon_0 = \pm 1$ . Возведем обе части (4.7) в степень  $2^{m-2}$ . Учитывая, что  $c^{2^m} \equiv 1$ ,  $c^{2^{m-1}} \equiv -1 \pmod{p}$ , получим

$$c^{2^{m-1}j_0} \cdot \varepsilon_0 \equiv 1 \pmod{p},$$

$$c^{2^{m-1}j_0} \cdot \left(\frac{r^2}{a}\right)^{2^{m-2}} = \left(c^{2j_0} \cdot \frac{r^2}{a}\right)^{2^{m-2}} \equiv 1 \pmod{p}.$$

Следовательно,

$$j_0 = \frac{1 - \varepsilon_0}{2} = \begin{cases} 0, & \text{если } \varepsilon_0 = 1 \\ 1, & \text{если } \varepsilon_0 = -1 \end{cases}$$

и

$$c^{2^{m-2}j_0} \left(\frac{r^2}{a}\right)^{2^{m-3}} = \varepsilon_1 = \pm 1 \quad (4.8)$$

Для вычисления  $j_1$  возведем обе части (4.7) в степень  $2^{m-3}$ . С учетом (4.8) получим:

$$\begin{aligned} c^{2^{m-2} \cdot j_0 + 2^{m-1} \cdot j_1} \cdot \left(\frac{r^2}{a}\right)^{2^{m-3}} &= c^{2^{m-1} \cdot j_1} c^{2^{m-2} \cdot j_0} \cdot \left(\frac{r^2}{a}\right)^{2^{m-3}} = \\ &= c^{2^{m-1} \cdot j_1} \varepsilon_1 = 1, \end{aligned}$$

то есть  $j_1 = \frac{1 - \varepsilon_1}{2}$  и  $c^{2^{m-3} \cdot j_0 + 2^{m-2} \cdot j_1} \left(\frac{r^2}{a}\right)^{2^{m-4}} = \varepsilon_2$ .

Пусть мы уже вычислили  $j_0, \dots, j_{t-1}$ ,  $t \geq 1$ . Тогда формула для  $\varepsilon_t$  имеет вид:

$$\varepsilon_t = \left(\frac{r^2}{a}\right)^{2^{m-2-t}} c^{j_0 \cdot 2^{m-t-1} + j_1 \cdot 2^{m-t} + \dots + j_{t-1} \cdot 2^{m-2}}, \varepsilon_t = \pm 1, t \geq 1. \quad (4.9)$$

Возведем обе части сравнения (4.7) в степень  $2^{m-t-2}$ , получим

$$\left(\frac{r^2}{a}\right)^{2^{m-2-t}} c^{j_0 \cdot 2^{m-t-1} + j_1 \cdot 2^{m-t} + \dots + j_{t-1} \cdot 2^{m-2} + j_t \cdot 2^{m-1}} \equiv 1 \pmod{p}.$$

Из этого сравнения и (4.9) получаем:

$$\epsilon_t \cdot c^{j_t 2^{m-1}} \equiv 1 \pmod{p}, \text{ т.е. } j_t = \frac{1 - \epsilon_t}{2}.$$

Применяя описанную выше процедуру, мы через  $m - 1$  шагов вычислим решение исходного сравнения.

На основе изложенного приведем формальное описание алгоритма вычисления решения сравнения  $x^2 \equiv a \pmod{p}$ .

#### Описание алгоритма решения сравнения

$$x^2 \equiv a \pmod{p = 2^m \cdot s + 1}$$

Вход алгоритма: простое  $p$ ,  $a$  — квадратичный вычет по модулю  $p$ ,  $b$  — квадратичный невычет.

Выход:  $x = \pm\sqrt{a}$ .

**Шаг 1.** Выполняем вычисления первых трех пунктов обоснования алгоритма.

Если  $m = 1$ , то  $x = \pm a^{\frac{s+1}{2}} \pmod{p}$  — искомое решение.

Если  $m > 1$ , то вычисляем 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 имеет вид

$$x \equiv \pm c^j r \pmod{p},$$

$$j = j_0 + j_1 \cdot 2 + \dots + j_{m-2} \cdot 2^{m-2}, j_k \in \{0, 1\}.$$

**Шаг 2.** Для определения  $j_0, \dots, j_{m-2}$  последовательно проводим следующие вычисления:

- Вычисляем  $\varepsilon_0 = h^{2^{m-2}} \pmod{p}$ ,  $\varepsilon_0 = \pm 1$ . Находим  $j_0$  по формуле

$$j_0 = \frac{1 - \varepsilon_0}{2}.$$

- Вычисляем  $\varepsilon_1 = h^{2^{m-3}} \cdot c^{2^{m-2}j_0}$ ,  $\varepsilon_1 = \pm 1$ . Находим  $j_1$  по формуле

$$j_1 = \frac{1 - \varepsilon_1}{2}.$$

...

- Вычисляем  $\varepsilon_t = h^{2^{m-2-t}} c^{j_0 \cdot 2^{m-t-1} + j_1 \cdot 2^{m-t} + \dots + j_{t-1} \cdot 2^1}$ , как и раньше,  $\varepsilon_t = \pm 1$ . Находим  $j_t$  по формуле

$$j_t = \frac{1 - \varepsilon_t}{2}.$$

...

- Вычисляем  $\varepsilon_{m-2} = h c^{j_0 \cdot 2 + \dots + j_{m-3} \cdot 2^{m-2}}$ ,  $\varepsilon_{m-2} = \pm 1$ . Находим

$$j_{m-2} = \frac{1 - \varepsilon_{m-2}}{2}.$$

**Шаг 3.** Вычисляем  $j = \sum_{i=0}^{m-2} j_i \cdot 2^i$  и определяем  $x = \pm c^j r$ .

**Пример 4.1.**  $p = 241$ ,  $a = 30$ ,  $b = 13$ .

1.  $p - 1 = 240 = 2^4 \cdot 15$ , то есть  $m = 4$ ,  $s = 15$ .

Проверим, что  $a$  — квадратичный вычет, а  $b$  — квадратичный невычет. Для этого вычислим символы Лежандра для каждого из этих чисел:

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{30}{241}\right) = \left(\frac{2}{241}\right) \left(\frac{3}{241}\right) \left(\frac{5}{241}\right) = \\ &= (-1)^{\frac{(241-1)(241+1)}{8}} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{241-1}{2}} \left(\frac{1}{3}\right) \times \\ &\quad \times (-1)^{\frac{5-1}{2} \cdot \frac{241-1}{2}} \left(\frac{1}{5}\right) = 1, \end{aligned}$$

$$\begin{aligned} \left(\frac{b}{p}\right) &= \left(\frac{13}{241}\right) = (-1)^{\frac{13-1}{2} \cdot \frac{241-1}{2}} \left(\frac{241}{13}\right) = \\ &= \left(\frac{7}{13}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{13-1}{2}} \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1. \end{aligned}$$

Находим

$$c = 13^{15} = 13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1 \equiv 76 \pmod{241},$$

$$r = a^{\frac{s+1}{2}} = a^8 = 30^8 \equiv 1 \pmod{241},$$

$$a^{-1} = 30^{-1} = -8 \equiv 233 \pmod{241},$$

$$h = r^2 \cdot a^{-1} = a^{-1} \equiv -8 \pmod{241}.$$

2. (0) Определяем  $\varepsilon_0 \equiv h^2 \equiv 8^4 \equiv -1 \pmod{241}$ .

$$\text{Следовательно, } j_0 = \frac{1 - \varepsilon_0}{2} = 1.$$

- (1) Определяем  $\varepsilon_1 \equiv h^2 c^4 = 64 \cdot (76)^4 \equiv -1 \pmod{241}$ .

$$\text{Следовательно, } j_1 = \frac{1 - \varepsilon_1}{2} = 1.$$

- (2) Определим  $\varepsilon_2 \equiv c^6 h$

$$\varepsilon_2 = (76)^6 \cdot (-8) = (76)^2 \cdot (76)^4 \times (-8) \equiv -1 \pmod{241}.$$

$$\text{Следовательно, } j_2 = \frac{1 - \varepsilon_2}{2} = 1.$$

3. Вычисляем  $j = 1 + 2 + 4 = 7$  и находим искомое решение

$$x = \pm c^7 \cdot r = \pm 76^7 \equiv \pm 111 \pmod{241}.$$

**Пример 4.2.**  $p = 449$ ,  $a = 178$ ,  $b = 3$ .

1.  $p - 1 = 2^6 \cdot 7$ , то есть  $m = 6$ ,  $s = 7$ .

Отсюда получаем

$$c = 3^7 = 3^6 \cdot 3 \equiv 729 \cdot 3 \equiv 280 \cdot 3 \equiv 391 \equiv -58 \pmod{449}$$

$$r = a^{\frac{s+1}{2}} = a^4 = (178)^4 = 309, \pmod{449}$$

$$h = r^2 \cdot a^{-1} = 322, \pmod{449}$$

$$a^{-1} = 169 \equiv 280 \pmod{449}.$$

$$2. \quad (0) \quad \varepsilon_0 = h^{2^4} \equiv -1 \pmod{449}, \quad j_0 = \frac{1 - \varepsilon_0}{2} = 1.$$

$$(1) \quad \varepsilon_1 = h^8 \cdot c^{2^4} \equiv -1 \pmod{449}, \quad j_1 = 1.$$

$$(2) \quad \varepsilon_2 = h^4 \cdot c^{2^3+2^4} \equiv 1 \pmod{449}, \quad j_2 = 0.$$

$$(3) \quad \varepsilon_3 = h^2 \cdot c^{2^2+2^3} \equiv 1 \pmod{449}, \quad j_3 = 0.$$

$$(4) \quad \varepsilon_4 = h \cdot c^{2+4} \equiv 1 \pmod{449}, \quad j_4 = 0.$$

$$3. \quad j = 1 + 2 = 3, \quad x = \pm c^3 \cdot r \equiv \pm 133 \pmod{449}.$$

Итак,  $x \equiv \pm 133 \pmod{449}$ .

## 4.5 Алгоритмы решения сравнения второй степени по примарному модулю

**Теорема 4.3.** Если  $p$  простое,  $p \geq 3$  и  $(\frac{a}{p}) = 1$ , то для любого  $k \geq 2$  сравнение

$$x^2 \equiv a \pmod{p^k} \tag{4.10}$$

имеет ровно 2 решения.

**Доказательство.** Необходимость следует из того, что если  $x_0^2 \equiv a \pmod{p^k}$ , то  $x_0^2 \equiv a \pmod{p}$ , и, следовательно,  $(\frac{a}{p}) = 1$ . Для доказательства достаточности представим искомое решение  $x$  в виде:

$$x = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \dots + \lambda_{k-1} p^{k-1}, \quad \lambda_i \in \mathbb{Z}_p$$

Так как  $(\frac{a}{p}) = 1$ , то  $x^2 \equiv \lambda_0^2 \equiv a \pmod{p}$ .

Таким образом, в качестве  $\lambda_0$  можно взять любые решения сравнения  $x^2 \equiv a \pmod{p}$ .

Далее, пусть  $x_i = \lambda_0 + \lambda_1 p + \dots + \lambda_i p^i$ ,  $i = \overline{1, k-1}$ . Если  $i < n-1$ , то  $x = x_i + A p^{i+1}$ , поэтому

$$x^2 \equiv x_i^2 \pmod{p^{i+1}} \equiv a \pmod{p^{i+1}} \tag{4.11}$$

Далее, последовательно будем вычислять  $x_i$  при  $i = \overline{1, k-1}$ .  
 Ясно, что  $x_{k-1} = x$  — искомое решение. Из (4.11) следует, что  
 существует  $t_{i+1}$  такое, что

$$x_i^2 = a + t_{i+1}p^{i+1}, \quad i = \overline{1, k-1} \quad (4.12)$$

С другой стороны,  $x_{i+1} = x_i + \lambda_{i+1}p^{i+1}$ ,  $i = \overline{0, k-2}$

Из (4.11) следует, что  $x_{i+1}^2 = x_i^2 + 2\lambda_{i+1}(\lambda_0 + \lambda_1 p + \dots + \lambda_i p^i)p^{i+1} \equiv a \pmod{p^{i+2}}$ , т.е  $x_i^2 + 2\lambda_{i+1}\lambda_0 p^{i+1} \equiv a \pmod{p^{i+2}}$

Учитывая (4.12) получаем:  $(t_{i+1} + 2\lambda_{i+1}\lambda_0)p^{i+1} \equiv 0 \pmod{p^{i+2}}$ .

Отсюда следует  $t_{i+1} + 2\lambda_{i+1}\lambda_0 \equiv 0 \pmod{p}$ .

Из последнего сравнения находим:

$$\lambda_{i+1} = (-2\lambda_0)^{-1}t_{i+1} \pmod{p}, i = \overline{0, k-2} \quad (4.13)$$

Таким образом, на основании (4.12) и (4.13) мы последовательно определим  $\lambda_{i+1}$ , а значит и  $x_{i+1}$ . При  $i = k-1$  получим искомое решение. Теорема полностью доказана.

На основании этой теоремы опишем алгоритм решения сравнения (4.10).  $\square$

### Описание алгоритма

Вход алгоритма: простое  $p$ ,  $p \geq 3$ ,  $a$  — квадратичный вычет по модулю  $p^k$ ,  $k \geq 2$ ,  $\left(\frac{a}{p}\right) = 1$ .

Выход:  $x = \pm\sqrt{a} \pmod{p^k}$ .

**Шаг 1.** Находим любое из двух решений  $\lambda_0 \in \mathbb{Z}$  сравнения

$$x^2 \equiv a \pmod{p}$$

и полагаем  $x_0 = \lambda_0$ .

**Шаг 2.** Вычисляем величину  $\delta_0 = (-2\lambda_0)^{-1} \pmod{p}$ .

**Шаг 3.** Производим следующие вычисления для  $i = \overline{0, k-2}$ :



- (0) Вычисляем  $x_i^2 = (\lambda_0 + \lambda_1 p + \dots + \lambda_i p^i)^2$ .
- (1) Находим  $t_{i+1} \pmod{p}$  такое, что  $x_i^2 = a + t_{i+1} p^{i+1}$ .
- (2) Вычисляем  $\lambda_{i+1} \equiv \delta_0 \cdot t_{i+1} \pmod{p}$ .
- (3) Находим  $x_{i+1} = \lambda_0 + \lambda_1 p + \dots + \lambda_{i+1} p^{i+1}$ .

**Шаг 4.** Искомое решение:  $x = \pm x_{k-1} \pmod{p^k}$ .

**Пример 4.3.**  $x^2 \equiv 136 \pmod{625}$ .

1.  $x^2 \equiv 1 \pmod{5}$ ,  $\lambda_0 = \pm 1$ . Положим  $x_0 = 1$ .
2.  $\delta_0 = (-2)^{-1} \equiv 2 \pmod{5}$ .
3. Проводим вычисления для  $i = 0, 1, 2$ :

- ( $i = 0$ )
  - 0)  $x_0^2 = 1$ ,
  - 1)  $1 = 136 - 27 \cdot 5, t_1 = -27 \equiv 3 \pmod{5}$ ,
  - 2)  $\lambda_1 = 2 \cdot 3 \equiv 1 \pmod{5}$ .
  - 3)  $x_1 = 1 + 1 \cdot 5 = 6$ ,
- ( $i = 1$ )
  - 0)  $x_1^2 = 36 = 136 - 4 \cdot 25$ ,
  - 1)  $t_2 = -4 \equiv 1 \pmod{5}$ ,
  - 2)  $\lambda_2 = 2 \cdot 1 = 2$ ,
  - 3)  $x_2 = 1 + 1 \cdot 5 + 2 \cdot 25 = 56$ .
- ( $i = 3$ )
  - 0)  $x_2^2 = 3136 = 136 + 24 \cdot 125$ ,
  - 1)  $t_3 = 24 \equiv 4 \pmod{5}$ ,
  - 2)  $\lambda_3 = 2 \cdot 4 \equiv 3 \pmod{5}$ ,
  - 3)  $x_3 = \pm(1 + 1 \cdot 5 + 2 \cdot 25 + 3 \cdot 125) = \pm 194 \pmod{625}$ .
4.  $x = \pm 194 \pmod{625}$ .

**Теорема 4.4.** Для любого натурального  $k > 1$  и простого  $p$  ( $p \geq 3$ ) группа  $\mathbb{Z}_{p^k}^*$  циклическая.

*Доказательство.* Докажем это утверждение конструктивно: далее будет указан алгоритм вычисления элемента  $h \in \mathbb{Z}_{p^k}^*$ , имеющий порядок  $(p-1)p^{k-1}$  по модулю  $p^k$ .

Так как  $\mathbb{Z}_p$  — поле, то  $\mathbb{Z}_p^*$  — циклическая группа. Пусть  $g$  — примитивный элемент поля, тогда  $ord(g) = p - 1$ .

По теореме Ферма  $g^{p-1} \equiv 1 \pmod{p}$ , следовательно, для некоторого  $v \in \mathbb{Z}$  выполнено равенство:

$$g^{p-1} = 1 + vp. \quad (4.14)$$

Пусть  $t$  — произвольный целочисленный параметр, тогда из (4.14) и бинома Ньютона следует, что

$$\begin{aligned} (g + pt)^{p-1} &= 1 + vp + (p-1)g^{p-2}pt + \\ &+ \sum_{i=2}^{p-1} \binom{p-1}{i} (pt)^i g^{p-1-i} = \\ &= 1 + p(v - tg^{p-2} + pT_1) = 1 + pu_1 \end{aligned} \quad (4.15)$$

Выберем теперь  $t = t_0$  так, чтобы  $u_1 \not\equiv 0 \pmod{p}$ . Для выполнения этого условия необходимо и достаточно, чтобы  $v \not\equiv t_0 g^{p-2} \pmod{p}$ . Поскольку,  $g^{p-2} \equiv g^{-1} \pmod{p}$ , то  $u_1 \not\equiv 0 \pmod{p}$  при  $t_0 \not\equiv vg \pmod{p}$ .

Из (4.15) следует, что

$$\begin{aligned} (g + pt_0)^{p(p-1)} &= (1 + pu_1)^p = 1 + p^2 u_1 + \sum_{i=2}^p \binom{p}{i} (pu_1)^i = \\ &= 1 + p^2(u_1 + pT_2) = 1 + p^2 u_2, \quad p \nmid u_2. \end{aligned}$$

Индукцией по  $k$  можно установить, что при любом  $k \geq 1$  справедливо соотношение:

$$(g + pt_0)^{p^k(p-1)} = 1 + p^{k+1} u_{k+1}, \quad p \nmid u_{k+1} \quad (4.16)$$

Действительно, если предположить, что (4.16) верно при данном значении  $k \geq 1$ , то

$$\begin{aligned} (g + pt_0)^{p^{k+1}(p-1)} &= (1 + p^{k+1}u_{k+1})^p = \\ &= 1 + p^{k+2}u_{k+1} + \sum_{i=2}^p (p^{k+1}u_{k+1})^i \binom{p}{i} = \\ &= 1 + p^{k+2}u_{k+2}, \quad p \nmid u_{k+2}. \end{aligned}$$

Тем самым мы установили справедливость (4.16) при любом натуральном  $k$ .

Покажем, что порядок элемента  $h = g + pt_0$  по модулю  $p^k$  равен  $(p-1)p^{k-1}$ .

Пусть  $m = \text{ord}(h)$  по модулю  $p^k$ ,  $k > 1$ . Тогда

$$(g + pt_0)^m \equiv 1 \pmod{p^k} \quad (4.17)$$

Из (4.17) следует, что  $(g + pt_0)^m \equiv 1 \pmod{p}$ . Так как  $\text{ord}(g + pt_0)$  по модулю  $p$  равен  $p-1$ , то по основному свойству порядка:

$$(p-1) \mid m, \quad \text{т.е. } m = (p-1)s. \quad (4.18)$$

С другой стороны, из теоремы Лагранжа имеем:

$$m \mid (p-1)p^{k-1} = |\mathbb{Z}_{p^k}^*| \Leftrightarrow mQ = (p-1)p^{k-1}. \quad (4.19)$$

Из (4.18) и (4.19) вытекает, что

$$m = (p-1)p^{r-1}, \quad r \leq k. \quad (4.20)$$

Отсюда, учитывая (4.16) и (4.17), получаем

$$(g + pt_0)^{(p-1)p^{r-1}} = 1 + p^r u_r \equiv 1 \pmod{p^k}, \quad p \nmid u_r.$$

то есть  $p^r u_r = lp^k$ . Но, поскольку  $p \nmid u_r$ , то  $r \geq k$ . Так как в силу (4.20)  $r \leq k$ , то получаем, что  $r = k$  и

$$m = \text{ord}(g + pt_0) = (p-1)p^{k-1} = |\mathbb{Z}_{p^k}^*|.$$

□

**Утверждение 4.4.** Пусть  $k \geq 1$  и  $\mathbb{Z}_{p^k}^* = \langle g \rangle$ ,  $p \geq 3$ ,  $p$  простое. Тогда

$$\mathbb{Z}_{2p^k}^* = \begin{cases} \langle g \rangle, & \text{если } g \text{ нечётное,} \\ \langle g + p^k \rangle, & \text{если } g \text{ четное.} \end{cases}$$

*Доказательство.* Заметим, что

$$|\mathbb{Z}_{2p^k}^*| = |\mathbb{Z}_{p^k}^*| = (p-1)p^{k-1} = \text{ord}(g) = m.$$

Поэтому, если  $g$  — нечетное число, то  $g^m - 1$  чётное. Следовательно,  $2p^k \mid (g^m - 1)$ . А это означает, что

$$\text{ord}(g) = m \pmod{2p^k}.$$

Если  $g$  чётное, то  $g + p^k = g_1$  нечётное и

$$\text{ord}(g_1) = \text{ord}(g) = m \pmod{p^k}.$$

Но  $2 \mid (g_1^m - 1)$ . Поэтому  $\text{ord}(g_1) = m \pmod{2p^k}$ . □

**Утверждение 4.5.** Порядок любого элемента группы  $\mathbb{Z}_{2^n}^*$  при  $n \geq 3$  является делителем  $2^{n-2}$  и, следовательно, эта группа не является циклической.

*Доказательство.* Пусть  $x \in \mathbb{Z}_{2^n}^*$ . Тогда  $x = 2t + 1$ , следовательно,

$$x^{2^1} = 1 + 4t^2 + 4t = 1 + 4t(t+1) = 1 + 8t_1 = 1 + 2^3 t_1,$$

$$x^{2^2} = 1 + 16t_1 + 64t_1^2 = 1 + 2^4 t_2.$$

Далее, если мы уже установили, что

$$x^{2^{k-1}} = 1 + 2^{k+1} t_{k-1},$$

то отсюда следует, что

$$(x^{2^{k-1}})^2 = x^{2^k} = 1 + 2^{k+2} t_k. \quad (4.21)$$

Положим в (4.21)  $k = n - 2$ . В результате получим

$$x^{2^{n-2}} = 1 + 2^n t_{n-2} \equiv 1 \pmod{2^n}.$$

Тем самым установлена справедливость утверждения. □

**Утверждение 4.6.** Если  $n \geq 3$ , то  $\text{ord}(5) = 2^{n-2} \pmod{2^n}$ .

*Доказательство.* Для доказательства справедливости утверждения установим, что при любом  $k \geq 0$

$$5^{2^k} = 1 + 2^{k+2} + 2^{k+3}t_k. \quad (4.22)$$

Действительно, при  $k = 0$  и  $k = 1$  (4.22) справедливо:

$$5^{2^0} = 5 = 1 + 2^2 + 2^3 \cdot 0,$$

$$5^{2^1} = 1 + 2^3 + 2^4 \cdot 1.$$

Допустим, что

$$5^{2^{k-1}} = 1 + 2^{k+1} + 2^{k+2}t_{k-1}.$$

Тогда

$$\begin{aligned} 5^{2^k} &= \left(1 + 2^{k+1} + 2^{k+2}t_{k-1}\right)^2 = \\ &= 1 + 2^{2k+2} + 2^{2k+4}t_{k-1}^2 + 2^{k+2} + 2^{k+3}t_{k-1} + 2^{2k+4}t_{k-1} = \\ &= 1 + 2^{k+2} + 2^{k+3} \left(2^{k-1} + 2^{k+1}t_{k-1}^2 + 2^{k+1}t_{k-1} + t_{k-1}\right) = \\ &= 1 + 2^{k+2} + 2^{k+3}t_k. \end{aligned}$$

Из (4.22) следует, что  $5^{2^{n-2}} = 1 + 2^n + 2^{n+1}t_k \equiv 1 \pmod{2^n}$  и при  $k < n - 2$  выполнено соотношение  $5^{2^k} \not\equiv 1 \pmod{2}$ . Следовательно,  $\text{ord}(5) = 2^{n-2}$ .  $\square$

**Упражнение 4.1.** Подсчитать число элементов порядка  $2^{n-2}$  в группе  $\mathbb{Z}_{2^n}^*$  ( $n \geq 3$ ). Для  $n = 5$  найти все элементы  $\mathbb{Z}_{32}^*$  порядка 8.

## 4.6 Решения сравнений по модулю $2^n$

Рассмотрим сравнение

$$x^2 \equiv a \pmod{2^n}, \quad \text{НОД}(a, 2) = 1, \quad n \in \mathbb{N} \quad (4.23)$$

- Если  $n = 1$ , то (4.23), очевидно, имеет одно решение  $x \equiv 1 \pmod{2}$ .
- Если  $n = 2$ , то (4.23) имеет два решения, если  $a \equiv 1 \pmod{4}$  и не имеет решений, если  $a \equiv -1 \pmod{4}$ .
- Пусть  $n \geq 3$ ,  $x = 2t + 1$  — решение (4.23), тогда

$$x^2 = 1 + 4t(t+1) \equiv a \pmod{2^n}. \quad (4.24)$$

Так как  $t(t+1)$  — чётное число, то из (4.24) следует, что

$$a \equiv 1 \pmod{8}. \quad (4.25)$$

Условие (4.25) является необходимым для решения сравнения (4.23) при  $n \geq 3$ . При  $n = 3$  сравнение (4.23) будет иметь 4 решения:

$$x = \pm 1, \pm 3 \pmod{8}.$$

**Теорема 4.5.** Если  $n \geq 4$ ,  $a \equiv 1 \pmod{8}$ , то сравнение (4.23) разрешимо и имеет 4 решения.

*Доказательство.* Заметим, что все нечетные числа можно представить в виде  $x = \pm(1 + 4k)$ , так как

$$\begin{aligned} 1 + 4k &\equiv 1 \pmod{4}, \\ -1 - 4k &\equiv -1 \equiv 3 \pmod{4}. \end{aligned}$$

Поэтому, если  $x_1 = 1 + 4k$  решение (4.23), то  $x_2 = -1 - 4k$ , также решение (4.23).

Далее решение  $x_1$  будем искать в виде

$$x = 1 + \lambda_2 2^2 + \cdots + \lambda_{n-2} 2^{n-2} + \lambda_{n-1} 2^{n-1},$$

где  $\lambda_2, \dots, \lambda_{n-1}$  — неизвестные двоичные коэффициенты.

Заметим, что если  $x_0$  — решение (4.23), то  $x_0 + 2^{n-1}$  также решение (4.23). Поэтому одно из искомых решений будет иметь вид:

$$b = 1 + \lambda_2 2^2 + \cdots + \lambda_{n-2} 2^{n-2}.$$

Пусть,

$$\begin{aligned} b_0 &= 1, \\ b_2 &= 1 + \lambda_2 2^2, \\ b_3 &= b_2 + \lambda_3 2^3, \\ \dots &\dots \end{aligned}$$

$$b_{n-2} = b = b_{n-3} + \lambda_{n-2} 2^{n-2}, \quad n \geq 4.$$

Из

$$(1 + \lambda_2 2^2 + \dots + \lambda_{n-2} 2^{n-2})^2 \equiv a \pmod{2^n}, \quad n \geq 4 \quad (4.26)$$

следует

$$(1 + \lambda_2 2^2)^2 \equiv a \pmod{2^4}. \quad (4.27)$$

Из (4.27) следует, что  $1 + \lambda_2 2^3 \equiv a \pmod{16}$ . Откуда, учитывая (4.25), получим  $\lambda_2 = \frac{a-1}{8} \pmod{2}$ . Таким образом, мы определим  $b_2$ .

Допустим, что мы уже вычислили  $b_2, \dots, b_{i-1}$ , то есть определили  $\lambda_2, \dots, \lambda_{i-1}$ ,  $i > 2$ . Из (4.26) вытекает

$$(b_{i-1} + \lambda_i 2^i)^2 \equiv a \pmod{2^{i+2}}.$$

После раскрытия скобок получим:

$$b_{i-1}^2 + \lambda_i 2^{i+1} \equiv a \pmod{2^{i+2}}.$$

Таким образом,

$$\lambda_i \equiv \frac{a - b_{i-1}^2}{2^{i+1}} \pmod{2} \quad (4.28)$$

Формула (4.28) позволяет индуктивным образом определить все коэффициенты  $\lambda_2, \dots, \lambda_{n-2}$  искомого решения  $x_1 = b$  сравнения (4.23). Остальные три решения суть следующие:

$$x_2 = -x_1, \quad x_3 = x_1 + 2^{n-1}, \quad x_4 = -x_1 - 2^{n-1} \pmod{2^n}. \quad (4.29)$$

□

### Описание алгоритма

$$x^2 \equiv a \pmod{2^n}, (a, 2) = 1, n \geq 4.$$

**Шаг 1.** Если  $a \not\equiv 1 \pmod{8}$ , то решений нет. В противном случае переходим к шагу 2.

**Шаг 2.** Вычисляем  $\lambda_2 = \frac{a-1}{8} \pmod{2}$  и  $b_2 = 1 + 4\lambda_2$ .

**Шаг 3.** Последовательно для  $i = 3, \dots, n-2$  вычисляем

$$\lambda_i = \frac{a - b_{i-1}^2}{2^{i+1}}, \quad b_i = b_{i-1} + \lambda_i 2^i.$$

При  $i = n-2$  получим  $b_{n-2} = x_1$ .

**Шаг 4.** Вычисляем все 4 решения исходного сравнения:

$$x_1,$$

$$x_2 = -x_1 = 2^n - x_1,$$

$$x_3 = x_1 + 2^{n-1},$$

$$x_4 = -x_1 - 2^{n-1} = 2^{n-1} - x_1.$$

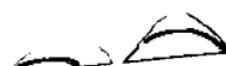
**Пример 4.4.**  $x^2 \equiv 209 \pmod{256}$ ,  $n = 8$ ,  $n-2 = 6$ .

$$1. \quad 209 \equiv 1 \pmod{8}$$

$$2. \quad \lambda_2 = \frac{209 - 1}{8} = 26 \equiv 0 \pmod{2}, \quad b_2 = 1$$

$$3. \quad (i=3) \quad \lambda_3 = \frac{209 - 1^2}{16} = 13 \equiv 1 \pmod{2}, \quad b_3 = 1 + 8 = 9$$

$$(i=4) \quad \lambda_4 = \frac{209 - 9^2}{32} = 4 \equiv 0 \pmod{2}, \quad b_4 = 9$$



$$(i=5) \lambda_5 = \frac{209 - 9^2}{64} = 2 \equiv 0 \pmod{2}, b_5 = 9$$

$$(i=6) \lambda_6 = \frac{209 - 9^2}{128} = 1 \pmod{2}, b_6 = 9 + 2^6 = 73$$

4.

$$\begin{aligned}x_1 &= 73, \\x_2 &= -7 = 256 - 73 = 183, \\x_3 &= 73 + 128 = 201, \\x_4 &= -201 = 55.\end{aligned}$$

**Пример 4.5.**  $x^2 \equiv 97 \pmod{512}$ ,  $n = 9$ ,  $n - 2 = 7$ .

1.  $97 \equiv 1 \pmod{8}$
2.  $\lambda_2 = \frac{97-1}{8} = 12 \equiv 0 \pmod{2}, b_2 = 1$
3.  $i = 3 \quad \lambda_3 = \frac{97-1}{16} = 6 \equiv 0 \pmod{2}, b_3 = 1$   
 $i = 4 \quad \lambda_4 = \frac{97-1}{32} = 3 \equiv 1 \pmod{2}, b_4 = 1 + 2^4 = 17$   
 $i = 5 \quad \lambda_5 = \frac{97-289}{64} = \frac{-192}{64} = -3 \equiv 1 \pmod{2},$   
 $b_5 = 17 + 32 = 49$   
 $i = 6 \quad \lambda_6 = \frac{97-49^2}{128} = -18 \equiv 0 \pmod{2}, b_6 = 49$   
 $i = 7 \quad \lambda_7 = \frac{97-49^2}{256} = -9 \equiv 1 \pmod{2}, b_7 = 49 + 128 = 177$
4.  $x_1 = 177, x_2 = -177 = 512 - 177 = 335,$   
 $x_3 = 177 + 256 = 433, x_4 = -433 = 512 - 433 = 79.$

**Замечание 4.1.** Описанные выше алгоритмы решения квадратичных сравнений по примарному модулю позволяют решать такие сравнения по любому модулю  $n$ . Для этого нужно выписать каноническое разложение числа  $n = p_1^{k_1} \cdots p_t^{k_t}$ . Затем для каждого  $i = \overline{1, t}$  решить сравнения  $x^2 \equiv a \pmod{p_i^{k_i}}$ , и на основе китайской теоремы об остатках найти все решения исходного сравнения  $x^2 \equiv a \pmod{n}$ .

**Пример 4.6.** Решим сравнение

$$x^2 \equiv 1081 \pmod{10800 = 2^4 \cdot 3^3 \cdot 5^2}.$$

**Решение.**

Выписываем систему сравнений

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

Первое сравнение имеет четыре решения:

$$x_1 = 3, x_2 = -3, x_3 = 11, x_4 = -11.$$

Второе сравнение — два решения:  $y_1 = 1, y_2 = -1$ .

Третье сравнение — два решения:  $z_1 = 9, z_2 = -9$ .

Следовательно, исходное сравнение будет иметь 16 решений. Общий вид решения на основе китайской теоремы об остатках следующий:

$$\begin{aligned} X = & x_i(27 \cdot 25)[(27 \cdot 25)^{-1} \pmod{16}] + \\ & + y_j(16 \cdot 25)[(16 \cdot 25)^{-1} \pmod{27}] + \\ & + z_k(16 \cdot 27)[(16 \cdot 27)^{-1} \pmod{25}]. \end{aligned}$$

Так как

$$\begin{aligned} (27 \cdot 25)^{-1} \pmod{16} &\equiv (11 \cdot 9)^{-1} \pmod{16} \equiv 3^{-1} \pmod{16} \equiv \\ &\equiv 11 \pmod{16}, \end{aligned}$$

$$\begin{aligned} (16 \cdot 25)^{-1} \pmod{27} &\equiv 22^{-1} \pmod{27} \equiv (-5)^{-1} \pmod{27} \equiv \\ &\equiv -16 \equiv 11 \pmod{27}, \end{aligned}$$

$$\begin{aligned} (16 \cdot 27)^{-1} \pmod{25} &\equiv (16 \cdot 2)^{-1} \equiv \\ &\equiv 7^{-1} \pmod{25} \equiv -7 \pmod{25}, \end{aligned}$$

то это решение примет вид:

$$X = 7425x_i + 4400y_j + 3024z_k, \quad i = \overline{1, 4}, \quad j = \overline{1, 2}, \quad k = \overline{1, 2}.$$

Если положить  $i = 2, j = 2, k = 1$ , то получим частное решение

$$X_0 = -22275 - 4400 + 27216 \equiv 541 \pmod{10800}.$$



## Глава 5

# Порождение больших простых чисел

### 5.1 Алгоритмы порождения простых чисел

**Теорема 5.1.** Пусть выполнены следующие условия:

1.  $n$  - нечётное;
2.  $n - 1 = F \cdot R$ ,  $\text{НОД}(F, R) = 1$ ;
3.  $F \geq \sqrt{n}$ ;
4.  $F = \prod_{i=1}^k q_i^{\alpha_i}$  - каноническое разложение числа  $F$  в произведение простых чисел;
5. для любого  $i = 1, \dots, k$  существуют  $a_i$  такие, что
$$a_i^{n-1} \equiv 1 \pmod{n}, \quad \text{НОД}(a_i^{\frac{n-1}{q_i}} - 1, n) = 1,$$
 (5.1)  
тогда число  $n$  простое.

*Доказательство.* Пусть  $p$  — произвольное простое число, которое делит  $n$ . Из соотношения (5.1) следует, что  $p \mid a_i^{n-1} - 1$ , то есть для некоторого  $t$  выполнено  $a_i^{n-1} - pt = 1$ . Таким образом  $\text{НОД}(p, a_i) = 1$ , поэтому, если  $e$  является порядком числа  $a_i$  по модулю  $p$ , то  $e$  делит  $n - 1$ . С другой стороны по малой теореме Ферма  $a_i^{p-1} \equiv 1 \pmod{p}$ , следовательно  $e \mid p - 1$ . В силу того, что  $p \mid n$  и выполнено соотношение (1), вытекает:  $p$  не делит  $a_i^{\frac{n-1}{q_i}} - 1$ . А это значит, что  $a_i^{\frac{n-1}{q_i}} - 1 \not\equiv 0 \pmod{p}$ , то есть  $e$  не делит  $\frac{n-1}{q_i}$ . Отсюда, учитывая, что  $e \mid n - 1$  можно заключить, что  $q_i^{\alpha_i} \mid e$ , но  $e \mid p - 1$ , поэтому  $q_i^{\alpha_i}$  делит  $p - 1$  для любого  $i = \overline{1, k}$ , следовательно  $F = \prod_{i=1}^k q_i^{\alpha_i} \mid p - 1$ . В силу последнего соотношения получаем, что  $p - 1 \geq F$ , то есть  $p > F \geq \sqrt{n}$ . Из произвольности простого делителя  $p$  числа  $n$  вытекает равенство  $p = n$ , то есть  $n$  — простое число.  $\square$

### Алгоритм порождения больших простых чисел №1

Итерационным методом строится возрастающая последовательность простых чисел

$$p_1 < p_2 < \dots < p_i.$$

В качестве первого числа в этой последовательности берётся любое известное нечётное простое число. Алгоритм проводит вычисления до тех пор, пока не будет получено простое число заданного размера в битах.

Предположим, что мы уже построили последовательность

$$p_1, p_2, \dots, p_{i-1}$$

и нужно вычислить следующее простое число  $p_i$ .

**Шаг 1.** Выбираем  $r \in \mathbb{Z}_{p_{i-1}}^*$ ,  $1 \leq r \leq p_{i-1} - 1$  и пусть  $r = 2^s t$ ,  $\text{НОД}(t, 2) = 1$ .

**Шаг 2.** Далее положим  $n = 2rp_{i-1} + 1 = 2^{s+1}tp_{i-1} + 1$ . Из выбора  $n$  следует, что  $n - 1 = 2^{s+1}p_{i-1}t$ ,  $F = 2^{s+1}p_{i-1}$ ,  $R = t$ . Очевидно, что  $\text{НОД}(R, F) = 1$ . Покажем, что  $F > \sqrt{n}$ . Справедливость этого утверждения вытекает из следующей цепочки неравенств, если учесть, что  $1 \leq t \leq p_{i-1} - 1$ :

$$n = 2^{s+1}p_{i-1}t + 1 < 2^{s+2}p_{i-1}t \leq 2^{s+2}p_{i-1}^2 \leq 2^{2s+2}p_{i-1}^2 = F^2$$

Таким образом  $n$ ,  $R$ , и  $F$ , удовлетворяют условиям теоремы 5.1.

**Шаг 3.** Для проверки простоты нужно случайным выбором найти  $a_1$  и  $a_2$  такие, что

$$\begin{aligned} a_1^{n-1} &\equiv a_2^{n-1} \equiv 1 \pmod{n}, \\ \text{НОД}\left(a_1^{\frac{n-1}{2}} - 1, n\right) &= \text{НОД}\left(a_2^{\frac{n-1}{2}} - 1, n\right) = 1 \end{aligned} \tag{5.2}$$

Если при некоторых  $a_1$  и  $a_2$  будет выполнено условие (5.2), то  $n$  — простое число и полагаем  $n = p_i$ . В противном случае нужно выбрать другое случайное  $r$ , а значит и другое  $n$  и повторить шаги 2 и 3.

### Алгоритм порождения больших простых чисел №2

Итерационным методом строим возрастающую последовательность простых чисел. Пусть мы уже получили число  $p_{i-1} > 3$ .

Выберем случайным образом число  $r \in [1, p_{i-1} - 3]$  и положим  $n = p_{i-1}r + 1$ ,  $F = p_{i-1}$ ,  $R = r$ . Очевидно, что  $\text{НОД}(F, R) = 1$ . Далее, поскольку

$$\begin{aligned} n = p_{i-1}r + 1 &\leq p_{i-1}(p_{i-1} - 3) + 1 \leq \\ &\leq p_{i-1}^2 - 3p_{i-1} + 1 < (p_{i-1} - 1)^2, \end{aligned}$$

то  $F = p_{i-1} > \sqrt{n}$ . Таким образом число  $n$  удовлетворяет условиям теоремы 5.1, следовательно для проверки простоты  $n$ , нужно убедиться в выполнении условий

$$a^{n-1} \equiv 1 \pmod{n}, \quad \text{НОД}(a^r - 1, n) = 1 \tag{5.3}$$

для некоторого  $a \in \mathbb{N}$ . Число  $a$ , как и в алгоритме №1, выбирается случайно.

**Теорема 5.2.** Если  $n = 2rq + 1$ ,  $q$  простое,  $r \leq 2q + 1$  и для некоторого  $a \in \mathbb{N}$  выполняются условия

$$a^{n-1} \equiv 1 \pmod{n}, \quad a^{2r} \not\equiv 1 \pmod{n}, \quad (5.4)$$

то  $n$  — простое число.

*Доказательство.* Пусть  $n = p_1^{k_1} \cdots p_t^{k_t}$  — каноническое разложение числа  $n$  на простые множители. Тогда

$$\text{НОД}(n, a^{2r} - 1) = p_1^{l_1} \cdots p_t^{l_t},$$

$0 \leq l_i \leq k_i$ ,  $i = \overline{1, t}$ . Так как по условию  $n \nmid a^{2r} - 1$ , то хотя бы для одного  $i$  выполняется неравенство  $l_i < k_i$ . Поэтому существуют простое число  $p$  и  $s \in \mathbb{N}$  такие, что

$$p^s \mid n, \quad p^{s-1} \mid (a^{2r} - 1), \quad p^s \nmid (a^{2r} - 1). \quad (5.5)$$

Ясно, что  $p \neq q$ , поскольку  $q \nmid n$ . Допустим, что  $n = pN$ ,  $N > 1$ , то есть число  $n$  составное. Тогда, если  $d = \text{ord}(a) \pmod{p^s}$ , то из (5.4) и (5.5), и основного свойства порядка получим:

$$d \mid (n-1) = 2rq, \quad d \mid (p^{s-1}(p-1)) = |\mathbb{Z}_{p^s}^*|, \quad d \nmid 2r.$$

Из этих соотношений следует, что  $q \mid d$  и  $q \mid p-1$ . Поскольку,  $2 \mid p-1$ , то  $2q \mid p-1$  и поэтому  $p = 2qt + 1$ ,  $t \geq 1$ . Поскольку, по предположению  $n = pN$ , а по условию теоремы  $n = 2rq + 1$ , то  $N = 1 + 2qu$ ,  $u \geq 1$ . Отсюда следует, что

$$n = pN = (1 + 2qt)(1 + 2qu) \geq (1 + 2q)^2.$$

С другой стороны, из условия теоремы вытекает, что

$$n = 2rq + 1 \leq 2q(2q + 1) + 1 < (2q + 1)^2.$$

Пришли к противоречию, следовательно  $N = 1$ , а  $n$  — простое число.  $\square$

**Теорема 5.3.** Если  $n = 2rq + 1$ ,  $q$  простое,  $r \leq 4q + 2$  и существует  $a \in \mathbb{N}$ , удовлетворяющее условиям (5.4), то либо  $n$  простое, либо  $n = p^2$ , где  $p = 2q + 1$  простое и  $a^{p-1} \equiv 1 \pmod{p^2}$ .

**Доказательство.** Допустим, что  $n = pN$ , где  $p$  простое, а  $N > 1$ . Тогда, как было установлено при доказательстве теоремы 5.2

$$p = 1 + 2qt, t \geq 1, \quad N = 1 + 2qu, u \geq 1.$$

Рассмотрим два возможных случая.

1.  $\max(p, N) \geq 1 + 4q$ .

Тогда имеем:

$$n = pN \geq (1 + 2q)(1 + 4q) = 8q^2 + 6q + 1.$$

Но по условию теоремы

$$n = 2rq + 1 \leq 2q(4q + 2) + 1 = 8q^2 + 4q + 1.$$

Пришли к противоречию. Следовательно, в этом случае  $n$  — простое число.

2.  $p = N = 1 + 2q$ .

Тогда,  $n = pN = (1 + 2q)^2 = p^2$ . Из условий (4) следует, что

$$a^{p^2-1} \equiv 1 \pmod{p^2}.$$

Поскольку  $|\mathbb{Z}_{p^2}^*| = p(p-1) = p^2 - p$ , то  $a^{p^2-p} \equiv 1 \pmod{p^2}$ .

Поэтому

$$a^{p^2-1} = a^{(p^2-p)+p-1} \equiv a^{p-1} \equiv 1 \pmod{p^2}.$$

□



## Глава 6

# Вероятностные тесты на простоту

### 6.1 Обоснование тестов

1. Подбираются легко проверяемые и эффективно вычислимые необходимые условия  $u_1, \dots, u_m$  для простоты числа.
2. Оценивается доля  $p_0$  чисел из  $\mathbb{Z}_n$  ( $n$  — составное), для которых условия  $u_1, \dots, u_m$  выполняются; тем самым оценивается сверху величиной  $p_0$  вероятность выполнения этих условий при случайном выборе числа  $n$ .
3. Если для данного нечетного числа  $n > 5$ , для каждого случайно выбранных чисел  $a_i \in \mathbb{Z}_n$ ,  $i = \overline{1, k}$  условия  $u_1, \dots, u_m$  выполняются, то полагают, что заданное число  $n$  с вероятностью  $p \leq p_0^k$  является составным и с вероятностью  $p > 1 - p_0^k$  простым.

Таким образом, главная задача при построении вероятностных тестов на простоту — это подбор условий  $u_1, \dots, u_m$  и подсчет величины  $p_0$ .

## 6.2 Тест Соловея—Штрассена

**Теорема 6.1.** Пусть  $n$  — нечётное составное число.

$$|\{a \in \mathbb{Z}_n^* | a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}\}| < \frac{n}{2}.$$

**Доказательство.** Пусть  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  — каноническое разложение числа  $n$ . Покажем, что найдётся  $b \in \mathbb{N}$  удовлетворяющее условиям

$$\text{НОД}(b, n) = 1, \quad b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n}. \quad (6.1)$$

Рассмотрим возможные случаи:

1. Для некоторого  $i = \overline{1, k}$ ,  $\alpha_i \geq 2$ . Не ограничивая общности, будем считать, что  $\alpha_1 \geq 2$ .

$\mathbb{Z}_{p_1^{\alpha_1}}^*$  — циклическая группа, поэтому у неё есть образующий  $b_0$ . Рассмотрим систему

$$\begin{cases} x \equiv b_0 & \pmod{p_1^{\alpha_1}} \\ x \equiv 1 & \pmod{p_i^{\alpha_i}}, i = 2, \dots, k \end{cases} \quad (6.2)$$

По китайской теореме об остатках эта система имеет единственное решение  $b \in \mathbb{Z}_n$ . Из (6.2) следует, что  $\text{НОД}(b, n) = 1$ . Покажем, что  $b^{n-1} \not\equiv 1 \pmod{n}$ , то есть  $b^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$ , а это значит, что  $b$  будет удовлетворять условиям (6.1). Итак, допустим противное  $b^{n-1} \equiv 1 \pmod{n}$ , тогда  $b_0^{n-1} \equiv 1 \pmod{p_1^{\alpha_1}}$ , следовательно,

$$\text{ord}(b_0) = p_1^{\alpha_1-1}(p_1 - 1) \mid p_1^{\alpha_1} \cdots p_n^{\alpha_n} - 1 = n - 1.$$

Но последнее невозможно, поскольку,  $p_1$  не делит  $n - 1$ . Таким образом, выбранное  $b$  удовлетворяет условиям (6.1).

2. Число  $n$  свободно от квадратов, то есть  $\alpha_1 = \cdots = \alpha_k = 1$ . Пусть  $b_0$  — образующий группы  $\mathbb{Z}_{p_1}^*$ . Рассмотрим систему

$$\begin{cases} x \equiv b_0 & \pmod{p_1} \\ x \equiv 1 & \pmod{p_i}, i = 2, \dots, k. \end{cases} \quad (6.3)$$

Очевидно, что решение системы  $b$  взаимно просто с  $n$  и

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right) \cdots \left(\frac{b}{p_k}\right) = \left(\frac{b_0}{p_1}\right) \left(\frac{1}{p_2}\right) \cdots \left(\frac{1}{p_k}\right) = -1 = \left(\frac{b_0}{p_1}\right).$$

Покажем теперь, что  $b^{\frac{n-1}{2}} \not\equiv -1 \pmod{n}$ . Действительно, если  $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ , то  $b^{\frac{n-1}{2}} \equiv -1 \pmod{p_i}$ ,  $i = \overline{1, k}$ . Пришли к противоречию с (6.3). Таким образом, число  $b$  удовлетворяющее условиям, существует.

Далее рассмотрим два множества

$$W_1 = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}\},$$

$$W_2 = \{b \in \mathbb{Z}_n^* \mid b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n}\}.$$

Так как  $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$  для любых  $a \in W_1$  и  $b \in W_2$ , то наименьший неотрицательный вычет  $ba \pmod{n}$  принадлежит  $W_2$ , следовательно,  $|W_2| \geq |W_1|$ , но  $|W_1| + |W_2| \leq n$ , значит,  $|W_1| + |W_2| \leq n$  или  $|W_1| \leq \frac{n}{2}$ , то есть утверждение теоремы полностью доказано.  $\square$

### Описание алгоритма Соловея—Штассена

Очевидно, что условия теоремы 6.1 являются необходимыми для простых чисел, а величина  $p_0$  при этом равна  $\frac{1}{2}$ . Поэтому, если при случайном выборе  $a_i \in \mathbb{Z}_n$ ,  $i = \overline{1, k}$ ,  $a_i \neq a_j$  условия теоремы 6.1 выполнены для всех  $i = \overline{1, k}$ , то считаем, что с вероятностью  $p \geq 1 - \frac{1}{2^k}$  число  $n$  простое.

## 6.3 Тест Миллера—Рабина

Изложенное ниже обоснование теста Миллера—Рабина принадлежит Гашкову С.Б.

Рассмотрим подмножества  $A$  и  $S$  множества  $\mathbb{Z}_n$ , определенные следующим образом — каждый элемент  $a$  множества  $A$  удовлетворяет точно одному из условий: либо

$$a^{n-1} \not\equiv 1 \pmod{n}, \quad (6.4)$$

либо

$$\begin{aligned} a^m &\not\equiv -1 \pmod{n} \text{ для всех } m \in \mathbb{Z} \\ \text{и } ord_p(a) &= p-1 \text{ для некоторого } p | n. \end{aligned} \quad (6.5)$$

Далее, если  $n-1 = 2^r t$ ,  $\text{НОД}(2, t) = 1$ , то каждый элемент  $s \in S$  удовлетворяет точно одному из условий: либо

$$s^t \equiv 1 \pmod{n}, \quad (6.6)$$

либо

$$s^{\frac{n-1}{2^k}} \equiv -1 \pmod{n} \text{ для некоторого } k \in \{1, \dots, r\}. \quad (6.7)$$

**Лемма 6.1.**  $aS \cap S = \emptyset$  для любого  $a \in A$ .

*Доказательство.*

1. Если  $a$  удовлетворяет условию (6.4) и  $s \in S$ , то из (6.6) и (6.7) следует, что  $(as)^{n-1} \not\equiv 1 \pmod{n}$ . Поэтому для  $as$  ни условие (6.6), ни условие (6.7) не выполнимо, то есть  $as \notin S$ .

2. Пусть теперь  $a \in A$ ,  $a^{n-1} \equiv 1 \pmod{n}$  и, следовательно, существует  $i \geq 0$  такое, что

$$a^{\frac{n-1}{2^i}} \equiv 1 \pmod{n}. \quad (6.8)$$

Например, (6.8) выполняется при  $i = 0$ . Далее будем полагать, что  $i$  — максимальное, удовлетворяющее условию (6.8). По условию (6.5) для некоторого простого  $p | n$ ,  $ord_p(a) = p-1$ , следовательно, по основному свойству порядка из (6.8) получаем:  $\frac{n-1}{2^i} = v(p-1)$ . Отсюда, учитывая чётность числа  $p-1$ , будем иметь:

$$n-1 = 2^i(p-1)v = 2^{i+1}uv. \quad (6.9)$$

Таким образом,  $i < r$ . Из максимальности выбора  $i$  получаем:

$$a^{\frac{n-1}{2^r}} = a^t \not\equiv 1 \pmod{n}. \quad (6.10)$$

Если  $s^t \equiv 1 \pmod{n}$ , то из (6.10) следует, что

$$(as)^t \equiv a^t s^t \equiv a^t \not\equiv 1 \pmod{n}.$$

С другой стороны, по условию (6.5)  $a^m \neq -1$  для любого  $m \in \mathbb{Z}$ , поэтому  $(as)^{\frac{n-1}{2^k}} \equiv a^{\frac{n-1}{2^k}} \not\equiv -1 \pmod{n}$  для любого  $k \in \{1, 2, \dots, r\}$ . Это значит, что  $as \notin S$ .

Пусть теперь  $s \in S$ ,  $s^t \not\equiv 1 \pmod{n}$  и, следовательно,  $s$  удовлетворяет условию (6.7) при некотором  $k \in \{1, \dots, r\}$ . Покажем, что  $i < k$  и  $s$  для всех  $j \in \{0, \dots, i\}$  удовлетворяет сравнению

$$s^{\frac{n-1}{2^j}} \equiv 1 \pmod{n}. \quad (6.11)$$

Действительно, если  $k > i$ , то возводя обе части (6.7) в квадрат, убеждаемся в справедливости сравнения (6.11) для любого  $j \in \{0, \dots, i\}$ .

Рассмотрим случай, когда  $k \leq i$ . Поскольку  $p \mid n$ , то из условия (6.7) следует, что

$$s^{\frac{n-1}{2^k}} \equiv -1 \pmod{p}. \quad (6.12)$$

С другой стороны, из (6.9) вытекает, что

$$(p-1) \mid \frac{n-1}{2^i} \mid \frac{n-1}{2^k}.$$

Отсюда по теореме Ферма получим:

$$s^{\frac{n-1}{2^k}} \equiv 1 \pmod{p}.$$

Пришли к противоречию с условием (6.12). Таким образом  $k > i$  и сравнение (6.11) справедливо для  $j \in \{0, \dots, i\}$ .

Так как  $i$  выбрано максимальным, а для элемента  $a$  выполняется сравнение (6.5), то

$$\frac{n-1}{2^i} \equiv 1 \pmod{n}, \quad a^{\frac{n-1}{2^{i+1}}} \not\equiv \pm 1 \pmod{n}. \quad (6.13)$$

Поэтому для любого  $j = 0, \dots, i$  справедливо сравнение

$$(as)^{\frac{n-1}{2^j}} \equiv a^{\frac{n-1}{2^j}} s^{\frac{n-1}{2^j}} \equiv 1 \pmod{n}. \quad (6.14)$$

Далее, поскольку  $k \geq i+1$  и  $s^{\frac{n-1}{2^k}} \equiv -1 \pmod{n}$ , то

$$s^{\frac{n-1}{2^{i+1}}} \equiv \pm 1 \pmod{n}.$$

Поэтому, учитывая (6.13), получим:

$$(as)^{\frac{n-1}{2^{i+1}}} \equiv a^{\frac{n-1}{2^{i+1}}} s^{\frac{n-1}{2^{i+1}}} \equiv \pm a^{\frac{n-1}{2^{i+1}}} \not\equiv \pm 1 \pmod{n}.$$

Следовательно,  $(as)^{\frac{n-1}{2^j}} \not\equiv \pm 1 \pmod{n}$  для  $j = i+1, \dots, r$ . Отсюда из сравнения (6.14) вытекает, что для любого  $j = 1, \dots, r$

$$(as)^{\frac{n-1}{2^j}} \not\equiv -1 \pmod{n}.$$

Таким образом, и в этом случае  $as \notin S$  и  $aS \cap S = \emptyset$ .  $\square$

**Упражнение 6.1.** Пусть  $a, b \in \mathbb{Z}_n^*$ , тогда  $aS \cap bS = \emptyset$  если и только если  $ab^{-1}S \cap S = \emptyset$ .

**Упражнение 6.2.** Пусть  $G < \mathbb{Z}_n^*$ , тогда  $g_1S \cap g_2S = \emptyset$  для любых  $g_1, g_2$  из множества  $G$  если и только если для любого элемента  $g$  из  $G$ , отличного от единичного,  $gS \cap S = \emptyset$ .

**Упражнение 6.3.** Если  $p$  простое и  $p^2 \mid n$ , тогда

$$G = \{1 + k \frac{n}{p} \mid k \in \mathbb{Z}_p\} < \mathbb{Z}_n^*$$

и  $|G| = p$ .



**Лемма 6.2.** Если  $p$  простое и  $p^2 \mid n$ , то

$$|S| < \frac{\varphi(n)}{4}.$$

*Доказательство.* Пусть  $G$  — подгруппа из Упражнения 6.3. Если  $p \mid n$  и  $p$  не делит  $n - 1$ , то для любого элемента  $g \neq 1$  из  $G$  справедливо сравнение  $g^{n-1} \not\equiv 1 \pmod{n}$ , следовательно,  $g \in A$  и по лемме 6.1  $S \cap gS = \emptyset$ . Из Упражнения 6.2 следует, что  $g_1S \cap g_2S = \emptyset$  для любых  $g_1 \neq g_2$  из  $G$ , поэтому

$$\left| \bigcup_g Sg \right| = |G| \cdot |S| = p|S|, \quad p|S| \leq |\mathbb{Z}_n^*| = \varphi(n).$$

Учитывая, что  $p \geq 5$ , получаем следующую оценку

$$|S| \leq \frac{\varphi(n)}{p} < \frac{\varphi(n)}{4}.$$

□

**Упражнение 6.4.** Если  $n = pq$ ,  $p \neq q$ ,  $p$  и  $q$  простые, то либо  $p - 1$  не делит  $n - 1$ , либо  $q - 1$  не делит  $n - 1$ .

**Лемма 6.3.** Если  $n = p_1p_2$ ,  $p_1 \neq p_2$ , то

$$|S| \leq \frac{\varphi(n)}{4}.$$

*Доказательство.* Пусть  $b_i$  — образующие групп  $\mathbb{Z}_{p_i}^*$ ,  $i = 1, 2$ . Рассмотрим системы

$$\begin{cases} x \equiv 1 \pmod{p_2}, \\ x \equiv b_1 \pmod{p_1}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{p_1}, \\ x \equiv b_2 \pmod{p_2}. \end{cases}$$

Пусть  $a_1$  и  $a_2$  решения этих систем по модулю  $n$ , тогда

$$1 = a_1^k \not\equiv -1 \pmod{p_2} \text{ и } 1 = a_2^k \not\equiv -1 \pmod{p_1}$$

при любом  $k \in \mathbb{N}$ . Отсюда следует, что при любом  $k \in \mathbb{N}$   $a_1^k \not\equiv -1 \pmod{n}$ ,  $a_2^k \not\equiv -1 \pmod{n}$ . Кроме того, так как  $a_i$  — образующие групп  $\mathbb{Z}_{p_i}^*$ , то  $\text{ord}_{p_i}(a_i) = p_i - 1$  и  $p_i \mid n = p_1 p_2$ ,  $i = 1, 2$ . Следовательно,  $a_i \in A$  и  $a_i^{-1} \in A$ . Пусть  $a = a_1 a_2 \pmod{n}$ . Если  $a^{n-1} \equiv 1 \pmod{n}$ , то  $a^{n-1} \equiv 1 \pmod{p_i}$  следовательно,  $p_i - 1$  делит  $n - 1$ ,  $i = 1, 2$ . Из упражнения 6.4 вытекает невозможность такого деления. Поэтому  $a^{n-1} \not\equiv 1 \pmod{n}$ . Таким образом,  $a_1 a_2 \in A$ .

Теперь рассмотрим множества  $S$ ,  $Sa_1$ ,  $Sa_2$ ,  $Sa$ . Из Леммы 6.1 и Упражнения 6.1 следует, что они попарно непересекаются, состоят из одинакового числа элементов и содержатся в  $\mathbb{Z}_n^*$ , поэтому

$$|S| \leq \frac{\varphi(n)}{4}.$$
□

**Лемма 6.4.** *Если число  $n$  свободно от квадратов и имеет вид  $n = p_1 \cdots p_k$ ,  $k \geq 3$ , то*

$$|S| \leq \frac{\varphi(n)}{4}.$$

**Доказательство.** Пусть  $b_1, b_2$  — образующие групп  $\mathbb{Z}_{p_1}^*$  и  $\mathbb{Z}_{p_2}^*$  соответственно. Рассмотрим системы

$$\begin{cases} x \equiv 1 \pmod{\frac{n}{p_1}}, \\ x \equiv b_1 \pmod{p_1} \end{cases}, \quad \begin{cases} x \equiv 1 \pmod{\frac{n}{p_2}}, \\ x \equiv b_2 \pmod{p_2} \end{cases}.$$

Пусть  $a_1$  и  $a_2$  решения этих систем по модулю  $n$ . Очевидно, что  $a_1 \not\equiv a_2 \pmod{n}$ . Так как  $a_1 \equiv 1 \pmod{p_3}$  и  $a_2 \equiv 1 \pmod{p_3}$ , то  $a = a_1 a_2 \equiv 1 \pmod{p_3}$ . Поэтому  $c^k \not\equiv -1 \pmod{n}$  при любом  $k \in \mathbb{N}$  и любом  $c \in \{a_1, a_2, a\}$ .

Действительно, если  $c^k \equiv -1 \pmod{n}$ , то  $c^k \equiv -1 \pmod{p_3}$ . Но это сравнение противоречит установленному выше. Таким образом,  $a_1, a_2, a \in A$  и эти числа попарно различны. Из Леммы 6.1 и Упражнения 6.1 следует, что множества  $S$ ,  $Sa_1$ ,  $Sa_2$ ,  $Sa$  попарно не пересекаются и равномощны. Отсюда следует,

что

$$|S| \leq \frac{|\mathbb{Z}_n^*|}{4} = \frac{\varphi(n)}{4}. \quad \square$$

Из лемм 6.1–6.4 вытекает справедливость следующей теоремы.

**Теорема 6.2.** *Если  $n$  — нечётное составное число такое, что*

$$n - 1 = 2^r \cdot t, \quad \text{НОД}(t, 2) = 1,$$

*то мощность множества*

$$S = \{x \in \mathbb{Z}_n^* \mid \text{либо } x^t \equiv 1 \pmod{n}, \\ \text{либо } \exists k = \overline{1, r} \text{ такое, что } x^{\frac{n-1}{2^k}} \equiv -1 \pmod{n}\}$$

*не больше  $n/4$ .*

### Описание алгоритма Миллера—Рабина

Для заданного нечетного числа  $n \geq 5$  выбираем случайным образом  $k$  попарно различных чисел  $x_1, \dots, x_k$  из  $\mathbb{Z}_n^*$ . Для каждого из выбранных чисел проверяем условия (6.6) и (6.7). Если все проверки прошли успешно, то полагаем, что число  $n$  простое с вероятностью  $p \geq 1 - \frac{1}{4^k}$ .

## Глава 7

# Конечные поля

### 7.1 Общие определения

Пусть  $F_q$  — поле из  $q$  элементов.

**Определение 7.1.** Поле  $P$  называется *простым*, если не существует полей  $P'$ , содержащегося в поле  $P$ .

**Теорема 7.1.** Конечное поле  $F_q$  содержит единственное простое поле  $P$ . Это поле изоморфно полю  $\mathbb{Z}_p$ , где  $p$  — некоторое простое число, называемое *характеристикой* поля  $F_q$ .

*Доказательство.* Пусть  $\mathcal{K} = \{ne = e + \dots + e \mid n \in \mathbb{N}\}$ . Очевидно, множество  $\mathcal{K}$  является коммутативным кольцом. В силу конечности поля  $F_q$  найдётся натуральное число  $m$  такое, что  $me = 0$ . Пусть  $p$  — минимальное из таких чисел. Число  $p$  обязательно является простым, если бы это было не так, то существовали бы числа  $u, v < p$  такие, что  $p = uv$ , но  $pe = uve = 0$ , а так как в поле нет делителей нуля, то необходимо  $ue = 0$ , либо  $ve = 0$ , что невозможно в силу минимальности  $p$ . Из простоты числа  $p$  вытекает, что  $\mathcal{K} = \{0, e, \dots, (p-1)e\}$  является подполем  $F_q$ . Отображение  $\varphi: \mathcal{K} \rightarrow \mathbb{Z}_p$ , определённое по правилу  $\varphi(me) = m$  является изоморфизмом. Единственность подполя  $P$  вытекает из его простоты и из того, что пересечение подполей является подполем.  $\square$

**Следствие 7.1.** Если  $p$  — характеристика конечного поля  $F_q$ , то для любых  $x, y \in F_q$  и любого натурального  $k$  справедливо тождество

$$(x + y)^{p^k} = x^{p^k} + y^{p^k}.$$

*Доказательство.* Справедливость этого утверждения следует из бинома Ньютона и следующего свойства характеристики  $px = p(ex) = (pe)x = 0 \cdot x = 0$  для любого элемента  $x$  из поля.  $\square$

**Теорема 7.2.** Число элементов конечного поля есть некоторая степень его характеристики.

*Доказательство.* Требуется доказать, что если  $F_q$  — поле, состоящее из  $q$  элементов, с характеристикой  $p$ , то существует натуральное число  $m$ , для которого верно соотношение  $q = p^m$ .

Пусть  $P$  — простое подполе рассматриваемого поля, тогда  $|P| = p$ . Будем искать максимальную линейно независимую над  $P$  систему элементов поля  $F_q$ . В качестве первого элемента  $a_0$  последовательности возьмём  $e$ . Если для любого  $a \in F_q$  система  $(e, a)$  линейно зависима, то  $q = p$  и  $F_q$  изоморфно  $\mathbb{Z}_p$ . В противном случае найдётся элемент  $a_1 \in F_q$  такой, что система  $(e, a_1)$  линейно независимая. Продолжая рассуждения аналогичным образом, мы построим систему из трёх, четырёх, и так далее, элементов, линейно независимую над  $P$ . На некотором шаге мы и получим максимальную линейно независимую систему  $(e, a_1, a_2, \dots, a_{m-1})$  над  $P$ , то есть для любого  $a \in F_q$  система  $(e, a_1, \dots, a_{m-1}, a)$  является линейно зависимой. Заметим, что любой элемент из поля  $F_q$  может быть однозначно представлен в виде линейной комбинации элементов  $e, a_1, \dots, a_{m-1}$ , то есть

$$a = \alpha_0 + \alpha_1 a_1 + \cdots + \alpha_{m-1} a_{m-1}, \quad \forall a \in F_q$$

Все  $\alpha_i$  в этом представлении принадлежат подполю  $P$ , изоморфному  $\mathbb{Z}_p$ , значит всего наборов  $\alpha_i$  ровно  $p^m$ , то есть мощность множества  $F_q = p^m$ .  $\square$

## 7.2 Построение конечных полей

Пусть  $P = \mathbb{Z}_p$ ,  $f(x)$  — многочлен степени  $m$ , неприводимый над полем  $P$  и  $P[x]$  — кольцо многочленов над полем  $P$ . Проведём факторизацию кольца  $P[x]$  по многочлену  $f(x)$ , то есть два многочлена  $g(x)$  и  $k(x)$  отнесём к одному классу эквивалентности, если остатки от деления этих многочленов на  $f(x)$  совпадают (заметим, что остаток является многочленом степени, не превосходящей  $m - 1$ ). Таким образом,

$$\begin{aligned} P[x]/f(x) = \bigcup_{\alpha \in P^m} & \{\alpha_0 + \alpha_1 x + \cdots + \\ & + \alpha_{m-1} x^{m-1} + h(x)f(x) \mid h(x) \in P[x]\}. \end{aligned}$$

Классы эквивалентностей не пересекаются и образуют поле относительно естественным образом введённых операций сложения и умножения многочленов по модулю  $f(x)$ .

Обозначим класс, содержащий многочлен  $x$  через  $\bar{x}$  (считаем, что  $m > 1$ ), тогда  $f(\bar{x}) = 0$ . Действительно, если  $f(x) = x^m + \beta_{m-1}x^{m-1} + \cdots + \beta_0$ , то при любом  $h(x) \in P[x]$  имеем:

$$\begin{aligned} f(x + h(x)f(x)) &= (x + h(x)f(x))^m + \\ &+ \beta_{m-1}(x + h(x)f(x))^{m-1} + \cdots + \beta_1(x + h(x)f(x)) + \beta_0. \end{aligned}$$

Раскроем скобки, используя бином Ньютона, и получим

$$\begin{aligned} f(x + h(x)f(x)) &= x^m + \beta_{m-1}x^{m-1} + \cdots + \\ &+ \beta_1x + \beta_0 + f(x)g(x) = 0 + f(x)(1 + g(x)). \end{aligned}$$

Следовательно,  $f(x + h(x)f(x)) \in \bar{0} = \langle f(x) \rangle$  при любом  $h(x) \in P[x]$ , а это и означает, что  $f(\bar{x}) = \bar{0}$ , в частности,  $f(x) \in \bar{0}$ , поэтому поле  $P[x]/f(x)$  можно рассматривать как поле, полученное из  $P[x]$  присоединением корня неприводимого над  $P$  многочлена  $f(x)$ .

Пример 7.1.  $P = \mathbb{Z}_2$ ,  $m = 2$ ,  $f(x) = x^2 + x + 1$ ;

$$F_4 = \{0, 1, x, x + 1\}.$$

Найдём произведение двух элементов:

$$x(x + 1) = x^2 + x = \{f(x) = 0 \Rightarrow x^2 = x + 1\} = (x + 1) + x = 1.$$

Пример 7.2.  $P = \mathbb{Z}_2$ ,  $m = 3$ ,  $f_1(x) = x^3 + x + 1$  или  $f_2(x) = x^3 + x^2 + 1$ ;

$$F_8 = \{\alpha_0 + \alpha_1x + \alpha_2x^2 \mid \alpha_i \in \mathbb{Z}_2\}.$$

Пример 7.3.  $P = \mathbb{Z}_5$ ,  $m = 2$ ,  $f_1(x) = x^2 + x + 2$  или  $f_2(x) = x^2 + 2$ ;

$$F_{25} = \{\alpha_0 + \alpha_1x \mid \alpha_i \in \mathbb{Z}_5\}.$$

Вычислим  $(x + 2)(x + 1)$ :

$$(x + 2)(x + 1) = x^2 + 3x + 2 = \begin{cases} 2x, & \text{если } F_{25} = \mathbb{Z}_5[x]/(f_1(x)) \\ 3x, & \text{если } F_{25} = \mathbb{Z}_5[x]/(f_2(x)). \end{cases}$$

### 7.3 Минимальные многочлены и их свойства

Пусть  $F_q$  — конечное поле, где  $q = p^m$ .

**Определение 7.2.** Многочлен  $f_\beta(x) \in \mathbb{Z}_p[x]$  минимальной степени такой, что  $f_\beta(\beta) = 0$  называется **минимальным** для элемента  $\beta \in F_q$ .

В дальнейшем будем считать, что старший коэффициент этого многочлена равен единице.

Пример 7.4.  $F_{16} = \mathbb{Z}_2[x]/(x^4 + x + 1)$ , тогда минимальным многочленом для элемента  $\beta = x$  будет  $f_\beta(x) = x^4 + x + 1$ .

**Пример 7.5.**  $F_{16} = \mathbb{Z}_2[x]/(x^4 + x + 1)$ ,  $\beta = x^2 + x$ , тогда  $f_\beta(x) = x^2 + x + 1$ , так как

$$\begin{aligned} f_\beta(x) &= (x^2 + x)^2 + (x^2 + x) + 1 = \\ &= x^4 + 2x^3 + x^2 + x^2 + x + 1 = x^4 + x + 1 = 0. \end{aligned}$$

Из минимальности степени многочлена  $f_\beta(x)$  следует справедливость следующего утверждения.

**Утверждение 7.1.** Многочлен  $f_\beta(x)$  является неприводимым и делит любой другой многочлен из  $P[x]$ , обращающийся в 0 при  $x = \beta$ .

**Следствие 7.2.** Для любого  $\beta \in F_q$ , где  $F_q$  — поле,  $f_\beta(x)$  делит  $x^q - x$ .

**Доказательство.** Справедливость утверждения вытекает из теоремы о примитивном элементе поля.  $\square$

**Утверждение 7.2.** Пусть  $q = p^m$  и  $F_q$  — поле, тогда  $\deg f_\beta(x) \leq m$  для любого  $\beta \in F_q$ .

**Доказательство.**  $F_q$  — линейное пространство над  $\mathbb{Z}_p$  размерности  $m$ , поэтому элементы  $1, \beta, \dots, \beta^m$  линейно зависимы над полем  $\mathbb{Z}_p$ . Следовательно, найдутся такие коэффициенты  $\alpha_0, \dots, \alpha_m \in \mathbb{Z}_p$ , что

$$\alpha_m \beta^m + \dots + \alpha_1 \beta + \alpha_0 = 0.$$

Это означает, что  $\beta$  является корнем многочлена

$$h(x) = \alpha_m x^m + \dots + \alpha_1 x + \alpha_0.$$

Из определения  $f_\beta(x)$  вытекает, что  $\deg f_\beta(x) \leq m$ .  $\square$

**Утверждение 7.3.** Пусть  $\beta$  примитивный элемент поля  $F_q$ ,  $q = p^m$ , тогда  $\deg f_\beta(x) = m$ .

*Доказательство.* Пусть  $\deg f_\beta(x) = k$ . Построим поле

$$\mathbb{Z}_p[\beta] / (f_\beta(\beta)) = F_{p^k}.$$

Так как  $\beta$  примитивный элемент, то  $F_{p^k} \supseteq F_{p^m}$ , следовательно,  $k \geq m$ , но по предыдущему утверждению  $k \leq m$ , значит  $k = m$ .

□

**Теорема 7.3.** Все конечные поля из  $q = p^m$  элементов изоморфны.

*Доказательство.* Пусть  $|F| = |G| = p^m$  и  $\alpha$  — примитивный элемент поля  $F$ . Из Следствия 7.1 вытекает, что  $f_\alpha(x) \mid x^{p^m} - x$ . Любой элемент поля  $G$  является корнем многочлена  $x^{p^m} - x$ , поэтому обязательно найдётся примитивный элемент  $\beta$  поля  $G$ , являющийся корнем именно многочлена  $f_\alpha(x)$ . Представим  $F$  и  $G$  в виде:

$$F = \mathbb{Z}_p[\alpha] / (f_\alpha(\alpha)), \quad G = \mathbb{Z}_p[\beta] / (f_\alpha(\beta)).$$

Очевидно, что соответствие  $\alpha \leftrightarrow \beta$  задаёт изоморфизм.

□

**Теорема 7.4.** Поле  $F_{p^n}$  содержит подполе  $G$  изоморфное полю  $F_{p^m}$ , если и только если  $m$  делит  $n$ .

*Доказательство.*

**Необходимость.** Пусть  $\beta$  — примитивный элемент поля  $G$ , тогда  $\beta^{p^m-1} = 1$ . С другой стороны  $\beta \in F_{p^n}$  и, следовательно,  $\beta^{p^n-1} = 1$ . Из свойств порядка следует, что  $p^m - 1 \mid p^n - 1$ , отсюда вытекает делимость  $n$  на  $m$ .

**Достаточность.** Пусть  $m$  делит  $n$ , то есть  $p^m - 1 \mid p^n - 1$ . Рассмотрим многочлен  $h(x) = x^{p^m} - x$ . Все элементы поля  $F_{p^n}$  являются корнями многочлена  $x^{p^n} - x$ , а многочлен  $x^{p^m} - x$  его делит, следовательно корни  $h(x)$  являются корнями  $x^{p^n} - x$ , поэтому они принадлежат полю  $F_{p^n}$ . С другой стороны для любого  $\alpha$  такого, что  $h(\alpha) = 0$  верно соотношение

$$\alpha^{p^m} \equiv \alpha. \tag{7.1}$$

Число корней многочлена  $h(x)$  равно  $p^m$  и все они образуют поле, так как из (7.1) для всех  $\alpha$  и  $\beta$  таких, что  $h(\alpha) = h(\beta) = 0$ , следуют соотношения

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m} \text{ и } (\alpha\beta)^{p^m} = \alpha^{p^m}\beta^{p^m}, \alpha^{p^m-1} = e.$$

Это поле, естественно, содержится в  $F_{p^m}$ . Достаточность установлена.  $\square$

### Пример 7.6.

$$\begin{aligned} GF(2^4) &= GF(2)[\theta]/(\theta^4 + \theta + 1) = \\ &= \{a_3\theta^3 + a_2\theta^2 + a_1\theta + a_0 \mid a_i \in \{0, 1\}\}. \end{aligned}$$

Тогда  $G = \{0, 1, \theta^2 + \theta, \theta^2 + \theta + 1\} \sim GF(4)$ . Действительно,

$$\begin{aligned} (\theta^2 + \theta)^4 &= \theta^8 + \theta^4 = (\theta^4)^2 + \theta^4 = \\ &= (\theta + 1)^2 + \theta + 1 = \theta^2 + 1 + \theta + 1 = \theta^2 + \theta, \\ (\theta^2 + \theta + 1)^4 &= (\theta^2 + \theta)^4 + 1 = \theta^2 + \theta + 1. \end{aligned}$$

Следовательно, любой  $\beta \in G$  является корнем уравнения  $h(x) = x^4 - x$ .

**Утверждение 7.4.** Если  $m \mid n$ , то любое  $\beta$  из поля  $F_{p^n}$  принадлежит полю  $F_{p^m}$ , если и только если  $\beta^{p^m} = \beta$ .

*Доказательство.*

Необходимость утверждения вытекает из теоремы о примитивном элементе.

Достаточность следует из того, что множество всех корней многочлена  $h(x) = x^{p^m} - x$  является подполем поля  $F_{p^n}$ , а так как  $\beta$  — некоторый корень этого многочлена, то  $\beta$  принадлежит полю корней многочлена  $h(x)$ , которое является единственным подполем поля  $F_{p^n}$ .  $\square$

**Теорема 7.5.** Многочлен  $h(x) = x^{p^n} - x$  равен произведению всех неприводимых над полем  $\mathbb{Z}_p$  многочленов, степени которых делят  $n$ .

**Доказательство.** Пусть  $f(x)$  неприводим над полем  $\mathbb{Z}_p$  и  $\deg f(x) = m \mid n$ . Возможны два случая:

1.  $f(x) = x$ . Очевидно, что  $f(x) = x \mid h(x)$ .
2.  $f(x) \neq x$ . Построим поле  $F_{p^m} = \mathbb{Z}_p[\alpha]/f(\alpha)$ . В этом поле найдётся элемент  $\beta$  такой, что  $f_\beta(x) = f(x)$ , например,  $\beta = \alpha$ . Из Следствия 1 вытекает, что  $f(x) \mid x^{p^m-1} - 1$ . Так как  $m$  делит  $n$ , то  $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ , поэтому  $f(x) \mid x^{p^n} - x = x(x^{p^n-1} - 1)$ .

Пусть теперь  $f(x)$  — неприводимый многочлен степени  $m$  и  $f(x)$  делит  $x^{p^n} - x$ . Покажем, что  $m \mid n$ . Как и раньше, будем считать, что  $f(x) \neq x$ . Построим поле  $F_{p^m} = \mathbb{Z}_p[\alpha]/f(\alpha)$ ,  $\beta$  — примитивный элемент поля  $F_{p^m}$ . Тогда

$$\beta = a_0 + a_1\alpha^1 + \cdots + a_{m-1}\alpha^{m-1}.$$

Так как  $f(\alpha) = 0$  и  $f(x) \mid x^{p^n-1} - 1$ , то  $\alpha^{p^n} = \alpha$ , поэтому

$$\beta^{p^n} = (a_0 + a_1\alpha^1 + \cdots + a_{m-1}\alpha^{m-1})^{p^n} = \beta.$$

Это означает, что  $ord(\beta) = p^m - 1 \mid p^n - 1$ , следовательно,  $m$  делит  $n$ .  $\square$

**Пример 7.7.** Пусть  $n = 4$ ,  $p = 2$ , тогда

$$\begin{aligned} x^{2^4} + x &= x(x+1)(x^2+x+1)(x^4+x+1) \times \\ &\quad \times (x^4+x^3+1)(x^4+x^3+x^2+x+1). \end{aligned}$$

Если  $n = 2$ ,  $p = 3$ , то

$$x^9 - x = x(x-1)(x-2)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

Только что доказанная теорема допускает следующее обобщение.

**Теорема 7.6.** Для любого натурального  $n$  многочлен  $x^{q^n} - x$  над полем  $F_q$  можно представить в виде произведения всех неприводимых нормированных многочленов над этим полем, степени которых делят  $n$ .

**Теорема 7.7.** Пусть  $I_q(n)$  — число нормированных неприводимых многочленов над  $F_q$  степени  $n$ , тогда

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}. \quad (7.2)$$

*Доказательство.* При перемножении многочленов их степени складываются, поэтому

$$q^n = \deg(x^{q^n} - x) = \sum_{\substack{f(x) \text{ — неприводимый,} \\ \deg f|n}} \deg f(x) = \sum_{d|n} d I_q(d).$$

Функции  $F(n) = n I_q(n)$  и  $G(n) = q^n$  являются мультипликативными и удовлетворяют условиям теоремы обращения Мёбиуса, поэтому

$$n I_q(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}}, \text{ то есть } I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

□

**Следствие 7.3.** В любом конечном поле существует неприводимый многочлен степени  $n$ .

*Доказательство.* Так как  $q \geq 2$ ,  $\mu(1) = 1$ ,  $\mu(d) \geq -1$  при  $d > 1$  из (7.2) получаем цепочку неравенств

$$\begin{aligned} I_q(n) &> \frac{1}{n} \left( q^n - \sum_{d>1: d|n} q^{\frac{n}{d}} \right) \geq \frac{1}{n} (q^n - \dots - q) = \\ &= \frac{1}{n} \left( q^n - \frac{q^n - 1}{q - 1} \right) = \frac{1}{n} \cdot \frac{q^{n+1} - 2q^n + 1}{q - 1} > 0. \end{aligned}$$

Следовательно,  $I_q(n) \geq 1$ , а это означает наличие неприводимого многочлена степени  $n$ . □

**Теорема 7.8.** Для любого простого  $p$  и любого натурального  $n$  существует поле из  $q = p^n$  элементов.

**Доказательство.** Для заданного  $p$  выбираем произвольный неприводимый многочлен  $f(x)$  степени  $n$ . Согласно описанной выше конструкции множество

$$F_q = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathbb{Z}_p \right\}$$

относительно операций сложения многочленов и умножения многочленов по модулю  $f(x)$  является полем из  $q = p^n$  элементов.  $\square$

**Теорема 7.9.** Если  $\beta$  — примитивный элемент поля  $GF(p^n)$  и  $f(x)$  — его минимальный многочлен, то все  $n$  корней этого многочлена попарно различны, являются также примитивными элементами поля  $F$  и имеют вид:

$$\beta_i = \beta^{p^i}, \quad i = \overline{0, n-1}, \quad \beta_0 = \beta.$$

**Доказательство.** Пусть  $f(x) = \sum_{i=0}^n a_i x^i$ ,  $a_i \in \mathbb{Z}_p$ . Так как по условию  $f(\beta) = 0$ , а по теореме Ферма  $a^{p^i} = a$  при любом  $a \in \mathbb{Z}_p$  и любом  $i \in \mathbb{N}$ , то  $f(\beta^{p^i}) = (f(\beta))^{p^i} = 0$ . Таким образом,  $\beta_i$  — корни многочлена  $f(x)$ .

Покажем, что  $\beta_i \neq \beta_j$  при  $i \neq j$ . Допустим, что  $i > j$  и

$$\beta_i = \beta^{p^i} = \beta_j = \beta^{p^j}. \quad (7.3)$$

Поскольку  $\beta^{p^n} = \beta$ , то из (7.3) следует, что

$$\beta = (\beta^{p^i})^{p^{n-i}} = (\beta^{p^j})^{p^{n-i}} \quad (7.4)$$

Отсюда вытекает, что  $\beta^{p^{n-i+j}} = \beta$ . Поэтому,  $\beta^{p^{n-(i-j)-1}} = e$ .

Так как  $i - j > 0$ , то это означает, что  $ord(\beta) < p^n - 1$ . Но  $\beta$  — примитивный элемент и  $ord(\beta) = p^n - 1$ . Пришли к противоречию.

Осталось показать, что

$$\text{ord}(\beta_i) = \text{ord}(\beta) = p^n - 1 = s.$$

Пусть  $\text{ord}(\beta_i) = t$ . Очевидно, что  $t \mid s$ . С другой стороны

$$\beta^t = (\beta^{p^n})^t = (\beta^{p^i})^{p^{n-i}t} = (\beta_i)^{t \cdot p^{n-i}} = e.$$

Следовательно,  $s \mid t$ . Отсюда следует, что  $s = t$ .  $\square$

**Утверждение 7.5.** Если  $f(x)$  над полем  $\mathbb{Z}_p$  — минимальный многочлен степени  $n$  примитивного элемента  $\beta$  поля  $GF(p^n)$ , то

$$f(x) \mid x^{p^n-1} - 1 \text{ и } f(x) \nmid x^k - 1, \quad k < p^n - 1. \quad (7.5)$$

**Доказательство.** По условию  $f_\beta(x) = f(x)$ , следовательно,  $f(x) \mid x^{p^n-1} - 1$ . Допустим, что  $f(x) \mid x^k - 1$  и  $k < p^n - 1$ . Так как  $f(\beta) = 0$ , то отсюда  $\beta^k = e$ . Противоречие с тем, что  $\text{ord}(\beta) = p^n - 1$ .  $\square$

**Замечание 7.1.** В дальнейшем многочлен, удовлетворяющий условию (7.5), будем называть *примитивным*.

Из Утверждения 7.5 получаем критерий примитивности многочлена, который по своей сути совпадает с критерием примитивности элемента конечного поля.

**Теорема 7.10** (критерий примитивности многочлена).

Многочлен  $f(x) \in \mathbb{Z}_p[x]$  степени  $n$  является примитивным тогда и только тогда, когда для любого простого  $q \mid p^n - 1$  выполнено соотношение

$$x^{\frac{p^n-1}{q}} \not\equiv 1 \pmod{f(x)}.$$

Пусть  $F$  и  $P$  — конечные поля и  $F \supset P$ . Поле  $F$  называется расширением поля  $P$ .

Например,  $F = GF(p^n) = \mathbb{Z}_p[x]/(f(x)) \supset P = \mathbb{Z}_p$ ,  $f(x)$  — неприводимый над  $P$ .

Поскольку  $\beta = x \in F$  и  $f(\beta) \equiv 0 \pmod{f(x)}$ , то будем говорить, что поле  $F$  получено из  $P$  присоединением корня  $\beta$  неприводимого над  $P$  многочлена  $f(x)$  степени  $n$  (обозначение  $F = P(\beta)$ ).

**Утверждение 7.6.** Для любого  $n \in \mathbb{N}$  существует примитивный над полем  $P$  многочлен степени  $n$ .

**Доказательство.** Рассмотрим поле  $F = GF(p^n)$  и пусть  $\beta$  — примитивный элемент и  $f_\beta(x)$  — минимальный многочлен элемента  $\beta$  над полем  $P$ . Из доказанного ранее следует, что  $\deg f_\beta = n$  и  $f_\beta(x) \mid x^{p^n-1} - 1$ . Допустим, что  $f_\beta \mid x^m - 1$  и  $m < p^n - 1$ . Так как  $f_\beta(\beta) = 0$ , то  $\beta^m - 1 = 0$ . Из свойства порядка получаем, что  $p^n - 1 \mid m$ . Пришли к противоречию. Таким образом,  $f_\beta(x)$  — примитивный многочлен.  $\square$

**Утверждение 7.7.** Если  $f(x)$  — примитивный многочлен степени  $n$  над полем  $P$ , то в некотором расширении

$$F = P[x]/(f(x)) = P(\beta), \quad \beta = x$$

поля  $P$  этот многочлен будет минимальным для некоторого примитивного элемента поля  $F$ .

**Доказательство.**  $F = P[x]/(f(x)) = P(x)$ . Покажем, что существует  $\beta \in F$  такой, что  $f_\beta(x) = f(x)$ . Действительно, в качестве  $\beta$  можно взять, например, многочлен  $\beta = x \in F$ . Так как  $f(x) \mid x^{p^n-1} - 1$  и  $f(x) \nmid x^m - 1$  при  $m < p^n - 1$ , то это означает, что  $or(\beta) = p^n - 1$  в поле  $F$  и  $f(\beta) = 0$ .  $\square$

Из теоремы 7.9 вытекает

**Следствие 7.4.** Если  $f(x) \in P[x]$  — примитивный многочлен степени  $n$  и  $F = P[x]/(f(x)) = P(\beta)$ , то  $\beta, \beta^p, \dots, \beta^{p^{n-1}}$  суть все корни  $f(x)$  в  $F$ , эти корни попарно различны и являются примитивными элементами в  $F$ .

## 7.4 Группа автоморфизмов конечных полей

Пусть, как и ранее,  $F$  — расширение степени  $n$  поля  $P$ .

**Определение 7.3.** Взаимно однозначное отображение  $\sigma$  поля  $F$  в себя называется *автоморфизмом* поля  $F$ , если:

1.  $\sigma(a) = a$  для всех  $a \in P$ ;
2.  $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ ;
3.  $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$ .

**Теорема 7.11.** Если поле  $F$  есть расширение степени  $n$  поля  $P$ , то множество всех автоморфизмов поля  $F$  над  $P$  представляет собой циклическую группу порядка  $n$ , которая состоит из следующих автоморфизмов:

$$\sigma_0(x) = x, \sigma_1(x) = x^p, \sigma_2(x) = x^{p^2}, \dots, \sigma_{n-1}(x) = x^{p^{n-1}}. \quad (7.6)$$

*Доказательство.* Из свойств характеристики и теоремы Ферма следует, что  $\sigma_i$  удовлетворяют условиям 1–3 определения автоморфизма и, следовательно, действительно являются автоморфизмами.

Покажем, что любой автоморфизм  $\sigma$  поля  $F$  над  $P$  имеет вид (7.6).

Пусть  $\beta$  — примитивный элемент поля  $F$  и

$$f_\beta = f(x) = x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_1x + \alpha_0 —$$

минимальный многочлен элемента  $\beta$  над  $P$ . Можно считать, что  $F = P(\beta) = P[\beta]/(f(\beta))$ . Из определения  $f_\beta$  и свойств 1–3 автоморфизмов  $\sigma$  имеем:

$$\begin{aligned} \sigma(0) &= 0 = \sigma(\beta^n + \alpha_{n-1}\beta^{n-1} + \dots + \alpha_1\beta + \alpha_0) = \\ &= (\sigma(\beta))^n + \alpha_{n-1}(\sigma(\beta))^{n-1} + \dots + \alpha_1\sigma(\beta) + \alpha_0 = f(\sigma(\beta)). \end{aligned}$$

Таким образом,  $\sigma(\beta)$  — корень примитивного многочлена  $f(x)$ . Из следствия 7.4 получаем, что  $\sigma(\beta) = \beta^{p^k}$  для некоторого  $k \in \{0, 1, \dots, n-1\}$ . Поэтому

$$x = \sum_{i=0}^{n-1} \delta_i \beta^i,$$

если  $x \in F$ , и

$$\sigma(x) = \sum_{i=0}^{n-1} \delta_i (\sigma(\beta))^i = \sum_{i=0}^{n-1} \delta_i (\beta^{p^k})^i = \left( \sum_{i=0}^{n-1} \delta_i \beta^i \right)^{p^k} = x^{p^k}.$$

□

**Упражнение 7.1.** Доказать, что в конечном поле  $F$  характеристики  $p$  для любого  $a \in F$  существует  $b = \sqrt[p]{a}$ .

## Глава 8

# Детерминированные алгоритмы дискретного логарифмирования

Введём понятие дискретного логарифма. Пусть  $G$  — некоторая конечная группа и  $H = \langle a \rangle$  — циклическая группа, порождённая элементом  $a \in G$ . Для любого  $y \in H$  найдётся число  $n \in \mathbb{N}$ , не превосходящее мощности  $H$ , и такое, что  $y = a^n$ . Число  $n$  называется *дискретным логарифмом* элемента  $y$  по основанию  $a$ .

Дискретный логарифм обладает следующими свойствами:

1.  $\log_a yz = \log_a y + \log_a z \pmod{n}$ ;
2.  $\log_a yz^{-1} = \log_a \frac{y}{z} = \log_a y - \log_a z \pmod{n}$ ;
3.  $\log_a y^k = k \log_a y \pmod{n}$ ;
4. Если  $b$  — другой образующий группы  $H$ , то

$$\log_b y = \log_a y \log_b a \pmod{n}.$$

5. Учитывая, что в предыдущем пункте  $\text{НОД}(\log_b a, n) = 1$ , получим

$$\log_b y = \frac{\log_a y}{\log_b a} = \log_a y (\log_b a)^{-1} \pmod{n}.$$

Вычисление дискретного логарифма в группах большого порядка с заданной, вычислимой, групповой операцией сложная задача. В общем случае не доказано существование полиномиальных алгоритмов дискретного логарифмирования. Мы рассмотрим простейшие детерминированные алгоритмы вычисления дискретного логарифма в конечных полях.

## 8.1 Алгоритм согласования

Пусть  $G = \langle a \rangle$  — циклическая группа порядка  $n$ . Требуется по элементу  $y \in G$  определить  $x \in \mathbb{N}$  такое, что

$$y = a^x, \quad x \in \{1, \dots, n-1\}. \quad (8.1)$$

Суть метода согласования заключается в следующем.

Пусть  $m = \lfloor \sqrt{n-1} \rfloor + 1$ , тогда  $m^2 \geq n$  и

$$\{mi - j \mid 1 \leq i \leq m, 0 \leq j \leq m-1\} \supset \{1, \dots, n-1\}.$$

Поэтому, если неизвестный дискретный логарифм  $x$  представить в виде  $x = mi - j$ , то равенство (8.1) эквивалентно

$$a^j y = (a^m)^i. \quad (8.2)$$

Соотношение (8.2) и определяет алгоритм согласования. Все вычисления производятся в группе  $G$  и определяются заданной групповой операцией.

### Описание алгоритма

Шаг 1. Вычислить  $m = \lfloor \sqrt{n-1} \rfloor + 1$ .

Шаг 2. Найти  $c = a^m$ .

Шаг 3. Составить множество  $\mathcal{A} = \{c^i \mid i = \overline{1, m}\}$  и упорядочить его.

Шаг 4. Составить множество  $\mathcal{B} = \{ya^j \mid j = \overline{0, m-1}\}$  и упорядочить его.

Шаг 5. Найти номера  $i, j$  совпадающих элементов множеств  $\mathcal{A}$  и  $\mathcal{B}$ . Тогда получим:

$$ya^j = c^i \text{ или } a^x a^j = c^i.$$

Шаг 6. По  $i$  и  $j$  определяем  $x = mi - j$ .

**Пример 8.1.** Рассмотрим группу  $G = \mathbb{Z}_{25}^*$ ,  $|G| = 20$ .

Нетрудно убедиться, что  $G = \langle 2 \rangle$ . Будем искать дискретный логарифм  $\log_2 17$ , то есть решать сравнение  $17 \equiv 2^x \pmod{25}$ .

Шаг 1.  $m = [\sqrt{19}] + 1 = 5$ .

Шаг 2.  $c = 2^5 \equiv 7 \pmod{25}$ .

Шаг 3.  $\mathcal{A} = \{7, 24, 18, 1\}$ .

Шаг 4.  $\mathcal{B} = \{17, 9, 18, 11, 22\}$ .

Шаг 5. Общий элемент  $\mathcal{A}$  и  $\mathcal{B}$  — 18. Поэтому  $i = 3$ ,  $j = 2$ . Следовательно,  $x = 3 \cdot 5 - 2 = 13$ .

**Пример 8.2.** Вычислим  $\log_5 173$  в группе  $G = \mathbb{Z}_{256}^*$ ,  $|G| = 64$ .

Шаг 1.  $m = 8$ .

Шаг 2.  $c = 5^8 \equiv 225 \pmod{256}$ .

Шаг 3.  $\mathcal{A} = \{225, 193, 161, 129, 97, 65, 33, 1\}$ .

Шаг 4.  $\mathcal{B} = \{173, 97, 229, 181, 93, 209, 277, 105\}$ .

Шаг 5. Общий элемент  $\mathcal{A}$  и  $\mathcal{B}$  — 97. Поэтому  $i = 5$ ,  $j = 1$ . Следовательно,  $\log_5 173 = 5 \cdot 8 - 1 = 39$ .

## 8.2 Алгоритм Полига—Хеллмана

Пусть известно разложение числа  $n = |G|$  на простые множители:

$$n = q_1^{\alpha_1} \cdots q_s^{\alpha_s},$$

и для данного  $b \in G = \langle a \rangle$  нужно вычислить  $\log_a b = y$ .

Шаг 1. Для каждого простого числа  $q$ ,  $q \mid n$  составляем таблицу чисел

$$a(q, j) = a^{j \frac{n}{q}}, \quad j = 0, \dots, q-1. \quad (*)$$

Шаг 2. Для каждого простого  $q_i \mid n$ , находим  $y_i = \log_a b \pmod{q_i^\alpha}$ . Пусть  $q_i = q$ ,  $\alpha_i = \alpha$  и

$$x \equiv \log_a b \equiv x_0 + x_1 q + \cdots + x_{\alpha-1} q^{\alpha-1} \pmod{q^\alpha},$$

где  $0 \leq x_i \leq q-1$ . Если  $y \equiv x \pmod{q^\alpha}$ , то  $y = x + vq^\alpha$ . Поэтому  $b^{\frac{n}{q}} = (a^y)^{\frac{n}{q}} = a^{\frac{(x+vq^\alpha)(n)}{q}} = a^{\frac{xn}{q}}$  и

$$b_0^{\frac{n}{q}} = a^{\frac{(x_0+x_1q+\cdots+x_{\alpha-1}q^{\alpha-1})(n)}{q}} = a^{\frac{x_0n}{q}}.$$

Теперь с помощью таблицы, полученной на первом шаге находим  $x_0$ . Положим  $c_1 = ba^{-x_0}$ . Далее рассмотрим соотношение

$$(b_1^{\frac{n}{q^2}}) = (ba^{-x_0})^{\frac{n}{q^2}} = a^{\frac{x_0n}{q^2}}.$$

По таблице (\*) находим  $x_1$ . Если уже вычислены  $x_0, \dots, x_{i-1}$ , то положим

$$c_i = (ba^{-x_0-x_1q-\dots-x_{i-1}q^{i-1}}).$$

Далее вычисляем  $c_i^{\frac{n}{q^{i+1}}} = a^{\frac{x_i n}{q}}$  и по таблице (\*) определяем  $x_i$ . Таким образом, мы вычислим все компоненты  $y_i$  дискретного логарифма элемента  $b$  по модулю  $q_i^{\alpha_i}$ ,  $i = \overline{1, s}$ .

**Шаг 3.** Найдя  $y_i = \log_a b \pmod{q_i^{\alpha_i}}$ ,  $i = 1, \dots, s$ , находим  $y = \log_a b \pmod{n}$  по китайской теореме об остатках из системы:

$$\{y = y_i \pmod{q_i^{\alpha_i}} \mid i = 1, \dots, s\}.$$

**Пример 8.3.**  $G = \mathbb{Z}_{81}^*$ ,  $|G| = n = 2 \cdot 3^3 = 54$ ,  $G = \langle 2 \rangle$ . Требуется найти  $\log_2 74$ , то есть  $a = 2$ ,  $b = 74$ . Предварительно нужно убедиться, что 2 — образующий группы  $G$ .

**Шаг 1.** Вычисляем  $a(2, 0) = 1$ ,  $a(2, 1) = 2^{27} \equiv -1 \pmod{81}$ ,  $a(3, 0) = 1$ ,  $a(3, 1) = 2^{18} \equiv 28 \pmod{81}$ ,  $a(3, 2) = 2^{36} \equiv 55 \pmod{81}$ .

**Шаг 2.1.**  $q = 2$ . Вычисляем  $\lambda_0 = \log_2 74 \pmod{2}$ .

Вычисляем

$$b^{\frac{n}{2}} = 74^{27} \equiv 74^{16} \cdot 74^8 \cdot 74^2 \cdot 74 \equiv -1 = a(2, \lambda_0).$$

Из Шага 1 следует, что  $\lambda_0 = 1 = x_1$ .

**Шаг 2.2.**  $q = 3$ . Вычисляем  $\log_{3^3} 74 = \lambda_0 + \lambda_1 3 + \lambda_2 9 \pmod{27}$ .  
Находим

$$b^{\frac{n}{3}} = 74^{18} \equiv 74^{16} \cdot 74^2 \equiv 70 \equiv 28 \pmod{81} = a(3, \lambda_0).$$

Из Шага 1 получаем, что  $\lambda_0 = 1$ .

Далее, вычисляем

$$(b \cdot a^{-\lambda_0})^{\frac{n}{q^2}} = (74 \cdot 2^{-1})^6 \equiv 37^6 = 37^2 \cdot 37^4 \equiv 55 = a(3, \lambda_1).$$

Из Шага 1 следует, что  $\lambda_1 = 2$ .

И наконец, вычисляем

$$\begin{aligned} (ba^{-\lambda_0-3\lambda_1})^{\frac{n}{q^3}} &= (74 \cdot 2^{-7})^2 \equiv (37 \cdot 64^{-1})^2 \equiv \\ &\equiv (37 \cdot 19)^2 \equiv 55^2 \equiv 28 = a(3, \lambda_2). \end{aligned}$$

Из Шага 1 находим, что  $\lambda_2 = 1$ .

Таким образом,  $x_2 \equiv \log_2 74 \pmod{27} = 1 + 2 \cdot 3 + 9 = 16$ .

**Шаг 3.** Вычисляем искомый логарифм  $\log_2 74 \pmod{54}$ . Для этого по китайской теореме об остатках находим решение системы:

$$\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 16 \pmod{27}. \end{cases}$$

Решение этой системы будет следующее:

$$\log_2 74 = 1 \cdot 27 \cdot 1 + 16 \cdot 2 \cdot 14 \equiv 43 \pmod{54}.$$

**Пример 8.4.** Вычислить  $\log_5 173$  в

$$G = \langle 5 \rangle \subset \mathbb{Z}_{256}^*, |G| = 2^{8-2} = 64,$$

$$\log_5 173 = x_0 + x_1 2 + x_2 2^2 + x_3 2^3 + x_4 2^4 + x_5 2^5, x_i = ?, i = \overline{0, 5}.$$

**Шаг 1.** Вычисляем  $a(2, 0) = 1$ ,  $a(2, 1) = 5^3 2 \equiv 129 \pmod{256}$ .

Применим алгоритм повторного возведения в квадрат:

$5^2$	$5^4$	$5^8$	$5^{16}$	$5^{32}$
25	113	225	193	129

**Шаг 2.0.** Далее вычисляем  $x_0$ . Для этого вычислим

$$b^{\frac{n}{q}} = (173)^{\frac{64}{2}} = (173)^{32} \equiv 129 \pmod{256}.$$

Таблица промежуточных степеней числа 173 следующая:

$173^2$	$173^4$	$173^8$	$173^{16}$	$173^{32}$
-23	17	33	65	129

Таким образом,  $a(2, x_0) = a(2, 1)$ , то есть  $x_0 = 1$ .

Шаг 2.1. Далее вычисляем

$$b_1 = b \cdot a^{-x_0} = 173 \cdot 5^{-1} = 173 \cdot 205 \equiv 137 \pmod{256}$$

и

$$b_1^{\frac{n}{q^2}} = (137)^{16} \equiv 129 \pmod{256} = a(2, x_1),$$

то есть  $x_1 = 1$ .

Шаг 2.2. Вычисляем

$$\begin{aligned} b_2 &= ba^{-x_0-qx_1} = 173 \cdot 5^{-3} \equiv 137 \cdot 205^2 \equiv \\ &\equiv 137 \cdot 41 \equiv 241 \equiv -15 \pmod{256} \end{aligned}$$

и

$$b_2^{\frac{n}{q^3}} = b_2^8 = (-15)^8 \equiv 225^4 = 129 \pmod{256} = a(2, x_2).$$

Отсюда следует, что  $x_2 = 1$ .

Шаг 2.3. Вычисляем

$$\begin{aligned} b_3 &= ba^{-x_0-qx_1-q^2x_2} = 173 \cdot 5^{-7} = \\ &= (173 \cdot 5^{-3})5^{-4} \equiv 129 \pmod{256} \end{aligned}$$

и

$$b_3^{\frac{n}{q^4}} = 129^4 \equiv 1 \pmod{256}.$$

Следовательно,  $x_3 = 0$ .

**Шаг 2.4.** Вычисляем

$$b_4 = ba^{-x_0 - qx_1 - q^2x_2 - q^3x_3} \equiv b_3 \equiv 129 \pmod{256}$$

и

$$b_4^{\frac{n}{q^5}} \equiv 1 \pmod{256}, \quad x_4 = 0.$$

**Шаг 2.5.**

$$b_5 = ba^{-x_0 - qx_1 - q^2x_2 - q^3x_3 - q^4x_4} = b_3,$$

$$b_5^{\frac{n}{q^4}} \equiv 129 \pmod{256}.$$

Таким образом,  $x_5 = 1$  и  $\log_5 173 = 7 + 32 = 39$ .

**Пример 8.5.** Вычислить  $\log_3 26$  в группе  $G = \mathbb{Z}_{73}^*$ . Порядок  $|G| = 7^2 \cdot 2 \cdot 3 = 294$ . Определяем  $a(q, i)$ , для  $q = 2, 3, 7$ .

**Шаг 1.**  $a(2, 0) = 1$ ,  $a(2, 1) = 3^{\frac{294}{2}} \equiv -1 \pmod{343}$ ,  $a(3, 0) = 1$ ,  $a(3, 1) = 3^{98} \equiv 324 \pmod{343}$ ,  $a(3, 2) = 324^2 \equiv 18 \pmod{343}$ ,  $a(7, 0) = 1$ ,  $a(7, 1) = 3^{42} \equiv 295$ ,  $a(7, 2) = 3^{84} \equiv 246$ ,  $a(7, 3) \equiv 197$ ,  $a(7, 4) \equiv 148$ ,  $a(7, 5) \equiv 99$ ,  $a(7, 6) \equiv 50$ .

Для вычисления  $a(q, i)$  предварительно вычисляем следующие величины по модулю 343:  $3^2 = 9$ ,  $3^4 = 81$ ,  $3^8 = 44$ ,  $3^{16} = 221$ ,  $3^{32} = 135$ ,  $3^{64} = 46$ ,  $3^{128} = 58$ .

**Шаг 2.1.** Находим  $\log_3 26 = \lambda_0 \pmod{2}$ . Для этого вычисляем  $b^{\frac{n}{2}} = a(2, \lambda_0) = -1$ . Из Шага 1 следует, что  $\lambda_0 = 1$ .

**Шаг 2.2.** Находим  $\mu_0 = \log_3 26 \pmod{3}$ . Для этого вычисляем  $b^{\frac{n}{3}} = a(3, \mu_0) = 18$ . Откуда следует, что  $\mu_0 = 2$  (см. Шаг 1).

**Шаг 2.3.** Находим  $\log_3 26 = \delta_0 + \delta_1 7 \pmod{7^2}$ .

Для определения  $\delta_0$  вычисляем  $a(7, \delta_0) = 197$ . Из этого сравнения вытекает, что  $\delta_0 = 3$  (см. Шаг 1).

Вычисляем

$$b_1 = ba^{-\delta_0} = 26 \cdot 27^{-1} \equiv 216 \cdot 26 \equiv 128 \pmod{343}.$$

Далее определяем  $\delta_1$  из сравнения  $a(7, \delta_1) = 99$ . Из шага 1 следует, что  $\delta_1 = 5$ . Таким образом,  $\log_3 26 = 3 + 5 \cdot 7 = 38$ .

**Шаг 3.** Находим искомый логарифм  $\log_3 26$  в группе  $\langle 3 \rangle = \mathbb{Z}_{73}^*$ .

$$\log_3 26 \equiv 1 \cdot 147 \cdot 1 + 2 \cdot 98 \cdot 2 + 38 \cdot 6 \cdot 41 \equiv 185 \pmod{294}.$$

Установим оценку сложности алгоритма в случае, когда  $G = GF(n)$ . Набор элементов  $a^{\frac{n}{q_i}}$  вычисляется за  $\sum_{i=1}^s O(\log n)$  групповых операций. Затем набор  $r_{q_i, j}$  для всех  $q_i, j$  вычисляется за  $\sum_{i=1}^s O(q_i)$  групповых операций. Для нахождения очередного  $x_i$  на шаге 2 надо возвести в степень (то есть найти  $a^{x_{i-1}q^{i-1}}$ ), найти обратный элемент, умножить, возвести в степень и пройти по таблице. Обратный элемент находится с помощью алгоритма Евклида за  $O(\log p)$  операций. Всё вместе даёт указанную оценку алгоритма Полига-Хеллмана.

Следует заметить, что алгоритм Полига-Хеллмана имеет полиномиальную сложность  $O((\log p)^{c_1})$  в случае, когда все простые делители  $q_i$  числа  $p$  не превосходят  $(\log p)^{c_2}$ , где  $c_1, c_2$  — положительные постоянные. Это имеет место, например, для простых чисел  $p$  вида  $p = 2^\alpha + 1$ ,  $p = 2^{\alpha_1}3^{\alpha_2} + 1$ . Если же у  $p - 1$  есть простой делитель  $q$ ,  $q \geqslant p^c$ , где  $c > 0$ , то алгоритм Полига-Хеллмана будет иметь экспоненциальную сложность.

**Упражнение 8.1.** В  $\mathbb{Z}_{101}$  вычислить  $\log_2 39$  двумя способами.

**Упражнение 8.2.** В  $\mathbb{Z}_{37}$  вычислить  $\log_2 24$ .

### 8.3 $\rho$ -алгоритм Полларда

$\rho$ -алгоритм Полларда для вычисления дискретных логарифмов является алгоритмом аналогичным по времени алгоритму со-

гласования, но нуждающемуся в довольно малом объеме памяти. Поэтому, он представляет больший практический интерес. Не ограничивая общности, будем считать, что  $G$  — циклическая группа порядка  $n$ .

Группа  $G$  разделяется на три множества  $S_1$ ,  $S_2$  и  $S_3$  приблизительно равного размера, которые базируются на свойствах, которые легко проверить. При выборе данных множеств нужно проверять, чтобы они не были тривиальными, например,  $1 \notin S_2$ . Определим последовательность элементов  $x_0 = 1, x_1, x_2, \dots$  так что

$$x_{i+1} = f(x_i) \stackrel{\text{def}}{=} \begin{cases} \beta \cdot x_i, & \text{если } x_i \in S_1, \\ x_i^2, & \text{если } x_i \in S_2, \\ \alpha \cdot x_i, & \text{если } x_i \in S_3, \end{cases} \quad (8.3)$$

где  $i \geq 0$ . Эта последовательность элементов группы определяет две последовательности элементов

$$a_0, a_1, a_2, \dots \text{ и } b_0, b_1, b_2, \dots,$$

удовлетворяющих условию  $x_i = \alpha^{a_i} \beta^{b_i}$  для  $i \geq 0$ :  $a_0 = 0$ ,  $b_0 = 0$  и для  $i \geq 0$

$$a_{i+1} = \begin{cases} a_i, & \text{если } x_i \in S_1, \\ 2a_i \pmod{n}, & \text{если } x_i \in S_2, \\ a_i + 1 \pmod{n}, & \text{если } x_i \in S_3, \end{cases} \quad (8.4)$$

и

$$b_{i+1} = \begin{cases} b_i + 1 \pmod{n}, & \text{если } x_i \in S_1, \\ 2b_i \pmod{n}, & \text{если } x_i \in S_2, \\ b_i, & \text{если } x_i \in S_3. \end{cases} \quad (8.5)$$

Алгоритм Флойда<sup>1</sup> может быть использован для поиска двух групп элементов  $x_i$  и  $x_{2i}$  таких, что  $x_i = x_{2i}$ .

<sup>1</sup> Алгоритм Флойда поиска циклов. На вход подается пара  $(x_1, x_2)$ . Вычисляем пары  $(x_i, x_{2i})$  по парам  $(x_{i-1}, x_{2i-2})$  до тех пор, пока не получим  $x_m = x_{2m}$  для некоторого  $m$ . Если длина нашей последовательности равна  $\lambda$  и длина цикла равна  $\mu$ , то  $m = \mu(1 + [\lambda/\mu])$ . Отсюда  $\lambda \leq m \leq \lambda + \mu$  и ожидаемое время работы алгоритма равно  $O(\sqrt{n})$ .

Так как  $x_i = \alpha^{a_i} \beta^{b_i}$ , то  $\alpha^{a_i} \beta^{b_i} = \alpha^{a_{2i}} \beta^{b_{2i}}$ . Следовательно,  $\beta^{b_i - b_{2i}} = \alpha^{a_{2i} - a_i}$ . Прологарифмировав по основанию  $\alpha$  обе части последнего равенства, получим

$$(b_i - b_{2i}) \log_\alpha \beta \equiv (a_{2i} - a_i) \pmod{n}.$$

Убедившись, что  $b_i \not\equiv b_{2i}$ , это сравнение может быть эффективно решено для определения  $\log_\alpha \beta$ .

Вход: образующий элемент  $\alpha$  циклической группы  $G$  порядка  $n$ , где  $n$  — простое число; элемент  $\beta \in G$ .

Выход: дискретный логарифм  $x = \log_\alpha \beta$ .

1. Положим  $x_0 = 1$ ,  $a_0 = 0$ ,  $b_0 = 0$ .

2. Для  $i = 0, 1, 2, \dots$  проделываем следующие действия:

(a) Используя  $x_{i-1}$ ,  $a_{i-1}$ ,  $b_{i-1}$  и  $x_{2i-2}$ ,  $a_{2i-2}$ ,  $b_{2i-2}$ , вычисляем  $x_i$ ,  $a_i$ ,  $b_i$  и  $x_{2i}$ ,  $a_{2i}$ ,  $b_{2i}$  по формулам (8.3), (8.4) и (8.5).

(b) Если  $x_i = x_{2i}$ , то

- Положить  $r = b_i - b_{2i} \pmod{n}$ .
- Если  $r = 0$ , то закончить работу алгоритма с ошибкой, иначе вычислить  $x = r^{-1}(a_{2i} - a_i) \pmod{n}$  и возвратить  $x$ .

*Замечание 8.1.* Если алгоритм закончил работу с ошибкой, то его можно запустить заново, выбрав  $a_0, b_0 \in_R [1, n-1]$ , и положив  $x_0 = \alpha^{a_0} \beta^{b_0}$ .

### Пример 8.6.

Элемент  $\alpha = 2$  — образующий подгруппы  $G$  группы  $\mathbb{Z}_{383}^*$  порядка  $n$ . Пусть  $\beta = 228$ . Разделим элементы из  $G$  на три множества по правилу  $x \in S_1$ , если  $x \equiv 1 \pmod{3}$ ,  $x \in S_2$ , если  $x \equiv 0 \pmod{3}$ ,  $x \in S_3$ , если  $x \equiv 2 \pmod{3}$ . В таблице ниже приведены значения  $x_i$ ,  $a_i$ ,  $b_i$ ,  $x_{2i}$ ,  $a_{2i}$ ,  $b_{2i}$  после каждой итерации шага 2 алгоритма 2.

$i$	$x_i$	$a_i$	$b_i$	$x_{2i}$	$a_{2i}$	$b_{2i}$
1	228	0	1	279	0	2
2	279	0	2	184	1	4
3	92	0	4	14	1	6
4	184	1	4	256	2	7
5	205	1	5	304	3	8
6	14	1	6	121	6	18
7	28	2	6	144	12	38
8	256	2	7	235	48	152
9	152	2	8	72	48	154
10	304	3	8	14	96	118
11	372	3	9	256	97	119
12	121	6	18	304	98	120
13	12	6	19	121	5	51
14	144	12	38	144	10	104

Из таблицы видно, что  $x_{14} = x_{28} = 144$ . Вычисляем

$$r = b_{14} - b_{28} = 125 \pmod{191},$$

$$r^{-1} = 125^{-1} = 136 \pmod{191}.$$

Откуда

$$r^{-1}(a_{28} - a_{14}) = 110 \pmod{191}.$$

Получаем, что  $\log_2 228 = 110$ .

## 8.4 Алгоритм вычисления индексов

Алгоритм вычисления индексов является наиболее сильным методом для вычисления дискретных логарифмов. Данная техника не применима для всех групп, но когда ей можно воспользоваться, то она дает субэкспоненциальную сложность.

Алгоритм вычисления индексов нуждается в выборе довольно малого подмножества  $S$  элементов из  $G$ , которое называется фактор-базой, так что существенное деление элементов из  $G$  может быть выражено через элементы из  $S$ . Данный

алгоритм требует предвычисления всех логарифмов элементов из  $S$ .

Нижеприведенное описание алгоритма вычисления индексов является неполным по двум причинам. Во-первых, не описано, каким образом выбирается фактор-база. Во-вторых, метод эффективной генерации отношений (8.6) и (8.8) также не описан.

Вход: образующий  $\alpha$  циклической группы  $G$  порядка  $n$ , элемент  $\beta \in G$ .

Выход: дискретный логарифм  $y = \log_{\alpha} \beta$ .

1. (Выбор фактор-базы  $S$ ) Выбираем подмножество

$$S = \{p_1, \dots, p_t\}$$

из  $G$  такое, что «значимая пропорция» элементов из  $G$  может быть получена из элементов из  $S$ .

2. (Вычислить линейные отношения, включающие логарифмы элементов из  $S$ .)

(a) Выбираем случайное  $k \in_R [0, n - 1]$  и вычисляем  $\alpha^k$ .

(b) Пытаемся выразить  $\alpha^k$  через элементы из  $S$ :

$$\alpha^k = \prod_{i=1}^t p_i^{c_i}, \quad c_i \geq 0. \quad (8.6)$$

Если успешно, то логарифмируем равенство (8.6) и получаем линейное отношение

$$k \equiv \sum_{i=1}^t c_i \log_{\alpha} p_i \pmod{n}. \quad (8.7)$$

- (c) Повторяем шаги 2a и 2b до тех пор, пока не будут получены  $t + c$  отношений из сравнения (8.7) ( $c$  есть некоторое малое положительное число такое, что система равенств, получаемая из  $t+c$  отношений, имеет единственное решение с большой вероятностью).

3. (Ищем логарифмы элементов из  $S$ ) Решаем систему из  $t + c$  сравнений (8.7) для вычисления  $\log_\alpha p_i$ ,  $1 \leq i \leq t$ .
4. (Вычисляем  $y$ )

(а) Выбираем  $k \in_R [0, n - 1]$  и вычисляем  $\beta\alpha^k$ .

(б) Пытаемся выразить  $\beta\alpha^k$  через элементы из  $S$ :

$$\beta\alpha^k = \prod_{i=1}^t p_i^{d_i}, \quad d_i \geq 0. \quad (8.8)$$

Если итерация неудачна, то повторяем 4а. Иначе, логарифмируем равенство (8.8) и получаем

$$y = \log_\alpha \beta = \left( \sum_{i=1}^t d_i \log_\alpha p_i - k \right) \pmod{n}. \quad (8.9)$$

#### 8.4.1 Алгоритм вычисления индексов в $\mathbb{Z}_p^*$

Для поля  $\mathbb{Z}_p^*$ , где  $p$  — простое, первые  $t$  простых элементов могут быть взяты в качестве фактор-базы  $S$ . Соотношение (8.6) получается при вычислении  $\alpha^k \pmod{p}$  и проверки, выражается ли данное число через элементы из  $S$ .

**Пример 8.7.** Пусть  $p = 229$ . Элемент  $\alpha = 6$  — образующий группы  $\mathbb{Z}_{229}^*$  порядка  $n = 228$ . Положим  $\beta = 13$ . Вычислим  $\log_6 13$ .

1.  $S = \{2, 3, 5, 7, 11\}$ .

2. Ниже описаны 6 соотношений с элементами из  $S$ :

$$6^{100} \pmod{229} = 180 = 2^2 \cdot 3^2 \cdot 5$$

$$6^{18} \pmod{229} = 176 = 2^4 \cdot 11$$

$$6^{12} \pmod{229} = 165 = 3 \cdot 5 \cdot 11$$

$$6^{62} \pmod{229} = 154 = 2 \cdot 7 \cdot 11$$

$$6^{143} \pmod{229} = 198 = 2 \cdot 3^2 \cdot 11$$

$$6^{206} \pmod{229} = 210 = 2 \cdot 3 \cdot 5 \cdot 7$$

Отсюда:

$$\begin{aligned} 100 &\equiv 2 \log_6 2 + 2 \log_6 3 + \log_6 5 \pmod{228} \\ 18 &\equiv 4 \log_6 2 + \log_6 11 \pmod{228} \\ 12 &\equiv \log_6 3 + \log_6 5 + \log_6 11 \pmod{228} \\ 62 &\equiv \log_6 2 + \log_6 7 + \log_6 11 \pmod{228} \\ 143 &\equiv \log_6 2 + 2 \log_6 3 + \log_6 11 \pmod{228} \\ 206 &\equiv \log_6 2 + \log_6 3 + \log_6 5 + \log_6 7 \pmod{228} \end{aligned}$$

3. Решая систему из 6 сравнений, получим:

$$\begin{aligned} \log_6 2 &= 21 \\ \log_6 3 &= 208 \\ \log_6 5 &= 98 \\ \log_6 7 &= 107 \\ \log_6 11 &= 162 \end{aligned}$$

4. Положим  $k = 77$ . Тогда

$$\beta \alpha^k = 13 \cdot 6^{77} \pmod{229} = 147 = 3 \cdot 7^2.$$

Откуда следует, что

$$\log_6 13 = (\log_6 3 + 2 \log_6 7 - 77) \pmod{228} = 117.$$

#### 8.4.2 Алгоритм вычисления индексов в $\mathbb{F}_{2^m}^*$

Элементы конечного поля  $\mathbb{F}_{2^m}$  представимы в виде полиномов в  $\mathbb{Z}_2[x]$  степени не больше  $m - 1$ , где вычисления ведутся по модулю фиксированного неприводимого многочлена  $f(x)$  степени  $m$  в  $\mathbb{Z}_2[x]$ . Фактор-база  $S$  выбирается как множество всех неприводимых полиномов в  $\mathbb{Z}_2[x]$  степени не больше некоторого фиксированного числа  $b$ . Соотношения (8.6) получаются при вычислении  $\alpha^k \pmod{f(x)}$  и проверки, что эти полиномы выражаются через элементы из  $S$ .

**Пример 8.8.** Полином  $f(x) = x^7 + x + 1$  является неприводимым над  $\mathbb{Z}_2$ . Отсюда, элементы конечного поля  $\mathbb{F}_{2^7}$  порядка 128 могут быть представлены как множество полиномов в  $\mathbb{Z}_2[x]$  степени не выше 6, где умножение выполняется по модулю  $f(x)$ . Порядок  $\mathbb{F}_{2^7}^*$  равен  $n = 2^7 - 1 = 127$ , и  $\alpha = x$  — образующий  $\mathbb{F}_{2^7}^*$ . Положим  $\beta = x^4 + x^3 + x^2 + x + 1$ . Вычислим  $y = \log_x \beta$ .

1. Выбираем фактор-базу как множество всех неприводимых на  $\mathbb{Z}_2[x]$  полиномов степени не выше 3:

$$S = \{x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1\}.$$

2. Выполним шаг 2 алгоритма исчисления индексов (см. алгоритм 4); все вычисления проводятся по модулю  $f(x)$ :

$$x^{18} = x^6 + x^4 = x^4(x + 1)^2$$

$$x^{105} = x^6 + x^5 + x^4 + x = x(x + 1)^2(x^3 + x^2 + 1)$$

$$x^{72} = x^6 + x^5 + x^3 + x^2 = x^2(x + 1)^2(x^2 + x + 1)$$

$$x^{45} = x^5 + x^2 + x + 1 = (x + 1)^2(x^3 + x + 1)$$

$$\begin{aligned} x^{121} &= x^6 + x^5 + x^4 + x^4 + x^3 + x^2 + x + 1 = \\ &= (x^3 + x + 1)(x^3 + x^2 + 1) \end{aligned}$$

Положим

$$p_1 = \log_x x,$$

$$p_2 = \log_x (x + 1),$$

$$p_3 = \log_x (x^2 + x + 1),$$

$$p_4 = \log_x (x^3 + x + 1),$$

$$p_5 = \log_x (x^3 + x^2 + 1).$$

Тогда

$$18 \equiv 4p_1 + 2p_2 \pmod{127}$$

$$105 \equiv p_1 + 2p_2 + p_5 \pmod{127}$$

$$72 \equiv 2p_1 + 2p_2 + p_3 \pmod{127}$$

$$45 \equiv 2p_2 + p_4 \pmod{127}$$

$$121 \equiv p_4 + p_5 \pmod{127}$$

3. Решая систему линейных сравнений, получим

$$\begin{aligned} p_1 &= 1, \\ p_2 &= 7, \\ p_3 &= 56, \\ p_4 &= 31, \\ p_5 &= 90. \end{aligned}$$

4. Выберем  $k = 66$ . Тогда

$$\begin{aligned} \beta\alpha^k &= (x^4 + x^3 + x^2 + x + 1)x^{66} \pmod{f(x)} = \\ &= x^5 + x^3 + x = x(x^2 + x + 1)^2, \end{aligned}$$

откуда следует, что

$$\log_x(x^4 + x^3 + x^2 + x + 1) = p_1 + 2p_3 - 66 \pmod{127} = 47.$$

**Замечание 8.2.** Для оптимизации алгоритма вычисления индексов размер  $t$  фактор-базы должен быть выбран правильно. Оптимальный выбор должен основываться на знании равномерного распределения чисел на отрезке  $[1, p - 1]$  для  $\mathbb{Z}_p^*$  и распределении в  $\mathbb{F}_{2^m}^*$  гладких полиномов (т.е. полиномов, чьи неприводимые множители имеют довольно малые степени) из полиномов в  $\mathbb{F}_2[x]$  степени меньше  $m$ . При оптимальном выборе  $t$  алгоритм вычисления индексов в  $\mathbb{Z}_p^*$  и в  $\mathbb{F}_{2^m}^*$  имеет ожидаемое время исполнения  $L_q \left[ \frac{1}{2}, c \right]$ , где  $q = p$  либо  $q = 2^m$  и  $c > 0$ .

**Замечание 8.3.** Наилучший алгоритм вычисления дискретных логарифмов в  $\mathbb{F}_{2^m}^*$  на сегодняшний день является вариацией алгоритма вычисления индексов (Coppersmith's algorithm) с временем исполнения порядка  $L_{2^m} \left[ \frac{1}{3}, c \right]$  для некоторой константы  $c < 1.587$ . Наилучший алгоритм для  $\mathbb{Z}_p^*$  есть алгоритм решета числового поля с временем исполнения порядка  $L_p \left[ \frac{1}{3}, 1.923 \right]$ .

## Глава 9

# Рекуррентные последовательности над конечными полями

Пусть  $F$  — конечное поле,

$$F^\infty = \{\tilde{a} = (\alpha_1, \alpha_2, \dots, \alpha_n, \dots) : \alpha_i \in F\} —$$

множество всех бесконечных последовательностей над  $F$ . Очевидно, что  $F^\infty$  есть бесконечномерное линейное пространство.

**Определение 9.1.** Последовательность  $\tilde{a} \in F^\infty$  называется *рекуррентной последовательностью* ранга  $n$ , если для некоторой функции  $f: F^n \rightarrow F$  последовательность  $\tilde{a}$  удовлетворяет уравнению:

$$\alpha_i + f(\alpha_{i-n}, \dots, \alpha_{i-1}) = 0, \quad i = n+1, n+2, \dots \quad (9.1)$$

Уравнение (9.1) эквивалентно уравнению

$$\alpha_i = g(\alpha_{i-n}, \dots, \alpha_{i-1}), \quad i = n+1, n+2, \dots \quad (9.2)$$

Набор  $\tilde{a}_0 = (\alpha_1, \alpha_2, \dots, \alpha_n)$  — начальный кусок рекуррентной последовательности  $\tilde{a}$ , называется *начальным заполнением*, а уравнение (9.1) — *характеристическим уравнением* рекуррентной последовательности.

Если  $f(g)$  — линейная функция, то рекуррентная последовательность называется *линейной рекуррентной последовательностью* (ЛРП).

**Пример 9.1.** Пусть  $F = \mathbb{Z}_3$ ,  $n = 2$ . Рассмотрим последовательность

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

Здесь  $\tilde{a}_0 = (1, -1)$ , а уравнение (9.2) будет следующим:

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

**Пример 9.2.** Если положить  $\tilde{a}_0 = (0, 0)$  в предыдущем примере, то

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

**Определение 9.2.** Рекуррентная последовательность  $\tilde{a}$  называется *периодической*, если существует такое число  $T \in \mathbb{N}$ , что для любого  $i = 1, 2, \dots$  выполняется условие

$$\alpha_{i+T} = \alpha_i. \quad (9.3)$$

Обычно под периодом последовательности будем понимать наименьшее из чисел  $T$ , при котором выполняются условия (9.3).

Всем рекуррентным последовательностям  $\tilde{a}$ , удовлетворяющим условию (9.2) с данной функцией (называемой функцией обратной связи), соответствует регистр сдвига  $R_g$ :

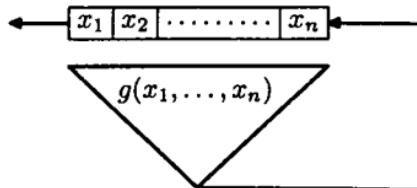


Рис. 9.1. Автономный автомат  $R_g$

$R_g$  — это автономный автомат, множество состояний  $S$  которого совпадает со множеством начальных значений  $F^n$ , функция переходов (отображение  $\varphi_g: F^n \rightarrow F^n$ ) имеет вид:

$$\begin{cases} y_1(t) = x_2(t-1) \\ y_2(t) = x_3(t-1) \\ \vdots \\ y_{n-1}(t) = x_n(t-1) \\ y_n(t) = g(x_1(t-1), \dots, x_n(t-1)), \quad t = 1, 2, \dots \\ (x_1(0), \dots, x_n(0)) = (\alpha_1, \dots, \alpha_n) \end{cases} \quad (9.4)$$

Функция выходов  $\lambda(t) = x_1(t)$ . Очевидно, что при заданном начальном заполнении  $(\alpha_1, \dots, \alpha_n)$ , выходная последовательность имеет следующий вид

$$\tilde{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_n, \lambda_{n+1}, \dots) = (\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1}, \dots) = \tilde{a}.$$

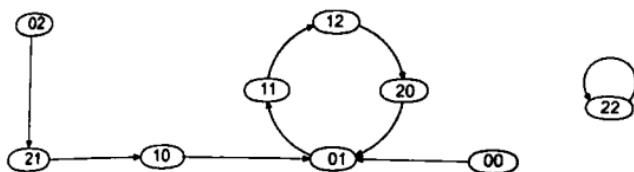
Преобразование  $\varphi_g$  однозначно определяет ориентированный граф  $\Gamma_g$ , который строится следующим образом. Множество вершин этого графа совпадает с  $F^n$ . Далее, вершина  $\tilde{a} \in F^n$  соединяется направленным ребром с вершиной  $\tilde{b} \in F^n$  в том и только в том случае, когда  $\varphi_g(\tilde{a}) = \tilde{b}$ .

**Пример 9.3.** Для рассмотренного выше примера система (9.4) имеет вид

$$\begin{cases} y_1 = x_2, \\ y_2 = x_1 x_2 + 1 \pmod{3}, \quad (g = x_1 x_2 + 1). \end{cases}$$

Соответствующий граф  $\Gamma_g$  изображен на рисунке 9.2.

**Утверждение 9.1.** Рекуррентная последовательность  $\tilde{a}$ , заданная уравнением (9.2), будет периодической для любого начального заполнения  $\tilde{a} \in F^n$ , если и только если при любом наборе  $(\alpha_2, \dots, \alpha_{n-1}) \in F^{n-1}$  функция  $h(x) = g(x, \alpha_2, \dots, \alpha_{n-1})$  является подстановкой на  $F$ .

Рис. 9.2. Граф  $\Gamma_g$ ,  $g = x_1x_2 + 1 \pmod{3}$ 

*Доказательство.* Покажем, что условия утверждения являются необходимыми и достаточными условиями для того, чтобы преобразование  $\varphi_g$  было подстановкой на множестве  $F^n$ . Поскольку период выходной последовательности автомата, является делителем периода последовательности состояний, то тем самым будет установлена справедливость утверждения. Далее заметим, что из (9.4) следует, что  $\varphi_g$  будет подстановкой на  $F^n$ , если и только если преобразование  $\varphi_g$  обратимо, то есть  $x_1, \dots, x_n$  однозначно вычисляются по  $y_1, \dots, y_n$ . Из (9.4) следует, что  $x_2 = y_1, \dots, x_n = y_{n-1}$ . Чтобы определить однозначно  $x_1$  из уравнения  $y_n = g(x_1, y_1, \dots, y_{n-1})$  при произвольных  $y_1, \dots, y_n$  необходимо и достаточно, чтобы функция  $g$  удовлетворяла условиям Утверждения 9.1.  $\square$

**Следствие 9.1.** Если  $F = \mathbb{Z}_2$ , то рекуррентная последовательность  $\tilde{a}$ , заданная уравнением (9.2) будет периодической для любого начального заполнения  $\tilde{a}_0 \in F^n$ , если и только если  $g(x_1, \dots, x_n)$  имеет вид:

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

*Доказательство.* Справедливость следует из свойств функций алгебры логики.  $\square$

Далее мы будем рассматривать линейные рекуррентные последовательности. Пусть  $\tilde{a}$  — линейная рекуррентная последовательность, удовлетворяющая уравнению (9.1). Тогда это

уравнение имеет вид

$$\alpha_i + \sum_{j=0}^{n-1} a_j \alpha_{i-n+j} = 0, \quad i = n+1, n+2, \dots \quad (9.5)$$

Уравнение (9.5) определяет многочлен

$$v(x) = x^n + \sum_{j=0}^{n-1} a_j x^j, \quad (9.6)$$

который называется *характеристическим многочленом* линейной рекуррентной последовательности  $\tilde{a}$ .

**Пример 9.4.** Пусть  $F = \mathbb{Z}_2$ ,  $n = 4$  и  $\tilde{a}$  удовлетворяет уравнению:

$$\alpha_i + \alpha_{i-2} + \alpha_{i-4} = 0, \quad i = 5, 6, \dots$$

Характеристический многочлен для этой последовательности будет следующим:

$$v(x) = x^4 + x^2 + 1.$$

На пространстве  $F^\infty$  определим оператор левого сдвига  $L$ :

$$L[(\alpha_1, \dots, \alpha_n, \dots)] = (\alpha_2, \dots, \alpha_{n-1}, \dots).$$

Очевидно, что это линейный оператор на  $F^\infty$ .

Естественным образом определяется  $i$ -ая степень оператора  $L^i$ ,  $i \geq 2$ . По определению полагаем  $L^0 = E$  — тождественный оператор на  $F^\infty$ . Также по определению полагаем, что если  $f(x) = \sum_{i=0}^m a_i x^i$  и  $f(L) = \sum_{i=0}^m a_i L^i$ , то  $f(L)[\tilde{a}] = \sum_{i=0}^{m-1} a_i L^i(\tilde{a})$ .

В операторной форме уравнение (9.5) примет вид:

$$v(L)[\tilde{a}] = \tilde{0}. \quad (9.7)$$

Пусть  $M(v) = \{\tilde{a} \in F^\infty : v(L)[\tilde{a}] = \tilde{0}\}$ . Заметим, что если  $\tilde{a} \in M(v)$ , то  $L^k(\tilde{a}) \in M(v)$  для любого  $k \in \mathbb{N}$ . Очевидно,

что  $M(v)$  — подпространство пространства  $F^\infty$  и его размерность равна  $\deg v$ . В качестве базиса можно взять, например, последовательности  $\tilde{e}_1, \dots, \tilde{e}_n$  из  $M(v)$  начальными заполнениями  $e_i^0 = (0, \dots, \underset{i}{1}, \dots, 0)$ ,  $i = \overline{1, n}$ .

Тогда любая последовательность  $\tilde{a} = (\alpha_1, \dots, \alpha_n, \dots)$  из  $M(v)$  линейно выражается через последовательности  $\tilde{e}_1, \dots, \tilde{e}_n$  следующим образом:

$$\tilde{a} = \alpha_1 \tilde{e}_1 + \cdots + \alpha_n \tilde{e}_n.$$

**Определение 9.3.** Многочлен  $f(x) \in F[x]$  называется *аннулирующим* для  $\tilde{a} \in M(v)$ , если  $f(L)[\tilde{a}] = \tilde{0}$ .

Пусть  $M(\tilde{a})$  — множество всех аннулирующих  $\tilde{a}$  многочленов, то есть

$$M(\tilde{a}) = \{f(x) \in F[x]: f(L)[\tilde{a}] = \tilde{0}\}.$$

Очевидно, что характеристический многочлен  $v(x) \in M(\tilde{a})$ .

**Утверждение 9.2.**  $M(\tilde{a})$  — идеал в  $F[x]$ .

Поскольку  $F[x]$  — кольцо главных идеалов, то существует многочлен  $f_\alpha(x)$  минимальной степени такой, что

$$M(\tilde{a}) = (f_\alpha(x)) = \{h(x)f_\alpha(x): h(x) \in F[x]\}.$$

Можно считать, что  $f_\alpha(x)$  — нормированный многочлен, то есть старший коэффициент равен 1. В дальнейшем  $f_\alpha(x)$  будем называть *минимальным* многочленом линейной рекуррентной последовательности  $\tilde{a}$ .

**Пример 9.5.** Пусть  $F = \mathbb{Z}_2$ ,  $v(x) = x^4 + x^2 + 1$ . Характеристическое уравнение будет иметь вид

$$\alpha_i = \alpha_{i-2} \oplus \alpha_{i-4}, \quad i = 5, 6, \dots$$

Для последовательности

$$\tilde{a}_1 = (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, \dots)$$

минимальным многочленом будет являться

$$f_1(x) = v(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

Для последовательности  $\tilde{a}_2 = (1, 1, 0, 1, 1, 0, 1, 1, 0, \dots)$  минимальный многочлен есть  $f_2(x) = x^2 + x + 1$ .

Для последовательности  $\tilde{a}_3 = \tilde{0}$  минимальный многочлен —  $f_3(x) = x + 1$ .

Заметим, что для  $\tilde{a} \neq 0$  минимальный многочлен делит характеристический многочлен.

**Пример 9.6.** Рассмотрим  $M(v)$ ,  $v(x) = x^5 + x^4 + x^3 + 1$ ,  $n = 5$ ,  $F = \mathbb{Z}_2$ . Выясним, какие минимальные аннулирующие многочлены у рекуррентных последовательностей из  $M(v)$ , с начальным заполнением  $\tilde{a}_0$ :

$$\begin{cases} \tilde{a}_0 = (0, 0, 0, 0, 0) = 0, & t_0(x) = 0 \\ \tilde{a}_0 = (1, 1, 1, 1, 1) = 31, & t_{31}(x) = x + 1, T = 1; \\ \tilde{a}_0 = (0, 1, 0, 1, 0) = 10, & t_{10}(x) = x^2 + 1, T = 2; \\ \tilde{a}_0 = (1, 0, 0, 0, 1) = 17, & t_{17}(x) = v(x), T = 14; \\ \tilde{a}_0 = (0, 1, 1, 0, 0) = 12, & t_2(x) = \\ \tilde{a}_0 = (0, 0, 0, 1, 0) = 2, & = t_{12}(x) = x^4 + x^2 + x + 1, T = 7; \\ \tilde{a}_0 = (0, 1, 1, 1, 0) = 14, & t_{14}(x) = x^3 + x^2 + 1, T = 7. \end{cases}$$

**Замечание 9.1.** Минимальный многочлен ЛРП  $\tilde{a}$  и  $L\tilde{a}$  совпадают, т.е.  $f_{\tilde{a}} = f_{L\tilde{a}}$ . Действительно, пусть  $f_{\tilde{a}}$  — минимальный аннулирующий многочлен для  $\tilde{a}$ , то есть  $f_{\tilde{a}}(L)[\tilde{a}] = \tilde{0}$ . Отсюда следует, что  $f_{\tilde{a}}(L)[L\tilde{a}] = \tilde{0}$ , то есть  $f_{L\tilde{a}} | f_{\tilde{a}}$ . В то же время  $L^T\tilde{a} = \tilde{a}$ ,  $T$  — период ЛРП  $\tilde{a}$  и  $f_{L^T\tilde{a}} | f_{L^{T-1}\tilde{a}}$ , отсюда следует, что  $f_{L^T\tilde{a}} = f_{\tilde{a}} | f_{L\tilde{a}}$ .

**Теорема 9.1.**

Если  $(v_1, v_2) = 1$ , то  $M(v_1v_2) = M(v_1) + M(v_2)$ .

*Доказательство.*

Рассмотрим произвольную ЛРП  $\tilde{g} \in M(v_1) + M(v_2)$ , то есть  $\tilde{g} = \tilde{a} + \tilde{b}$ ,  $\tilde{a} \in M(v_1)$ ,  $\tilde{b} \in M(v_2)$ . Тогда

$$\begin{aligned} v_1(L)v_2(L)[\tilde{g}] &= v_1(L)v_2(L)[\tilde{a} + \tilde{b}] = v_2(L)v_1(L)[\tilde{a}] + \\ &\quad + v_1(L)v_2(L)[\tilde{b}] = \tilde{0} + \tilde{0} = \tilde{0}. \end{aligned}$$

Таким образом, мы показали, что  $M(v_1) + M(v_2) \subseteq M(v_1v_2)$ .

Теперь возьмём последовательность  $\tilde{a} \in M(v_1) \cap M(v_2)$ . Так как НОД( $v_1, v_2$ ) = 1, то найдутся такие  $w, u$ , что  $1 = v_1w + v_2u$ . Тогда  $v_1(L)w(L) + v_2(L)u(L) = E$ . Отсюда, подставляя  $\tilde{a}$ , получим, что  $E\tilde{a} = \tilde{a} = v_1(L)w(L)[\tilde{a}] + v_2(L)u(L)[\tilde{a}] = \tilde{0}$ .

Осталось заметить, что

$$\dim M(v_1v_2) = \dim M(v_1) + \dim M(v_2).$$

Теорема полностью доказана.  $\square$

### Теорема 9.2.

Если  $(v_1, v_2) = 1$ ,  $\tilde{a} \in M(v_1)$ ,  $\operatorname{per} \tilde{a} = T_1$ ,  $\tilde{b} \in M(v_2)$ ,  $\operatorname{per} \tilde{b} = T_2$ , то  $\operatorname{per}(\tilde{a} + \tilde{b}) = \text{HOK}(T_1, T_2) = T$ .

*Доказательство.*

Обозначим  $\operatorname{per}(\tilde{a} + \tilde{b}) = T'$ . Так как

$$\alpha_{i+T} + \beta_{i+T} = \alpha_{i+T_1k_1} + \beta_{i+T_2k_2} = \alpha_i + \beta_i, \text{ то } T' \mid T.$$

С другой стороны, так как  $(v_1, v_2) = 1$ , то  $M(v_1) \cap M(v_2) = \tilde{0}$ . И мы имеем  $\alpha_{i+T'} + \beta_{i+T'} = \alpha_i + \beta_i$ , то есть  $\alpha_{i+T'} - \alpha_i = \beta_i - \beta_{i+T'}$ . Откуда получаем  $L^{T'}\tilde{a} - \tilde{a} = \tilde{b} - L^{T'}\tilde{b} \in M(v_1) \cap M(v_2) = \tilde{0}$ . Следовательно,  $\alpha_{i+T'} = \alpha_i$  и  $\beta_{i+T'} = \beta_i$ . Поэтому  $T_1 \mid T'$  и  $T_2 \mid T'$ , то есть  $T \mid T'$ . Теорема доказана.  $\square$

*Определение 9.1.* Число  $\operatorname{per} f = N \in \mathbb{N}$  называется *периодом многочлена*  $f(x)$ , если  $f(x) \mid x^N - 1$ , но  $f(x) \nmid x^k - 1$ ,  $\forall k < N$ .

**Пример 9.7.** Пусть  $F = \mathbb{Z}_2$ , рассмотрим несколько многочленов:

$$\begin{aligned} f_1 &= x^2 + x + 1, & \text{per } f_1 = 3, \\ && \text{так как } f_1 \mid x^3 + 1 = (x+1)(x^2 + x + 1), \\ f_2 &= x^3 + x + 1, & \text{per } f_2 = 7, \\ && \text{так как } f_2 \nmid x^4 + 1, x^5 + 1, x^6 + 1, \text{ но} \\ && f_2 \mid x^7 + 1, \text{ при этом} \\ && x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1), \\ f_3 &= x^4 + x^2 + 1, & \text{per } f_3 = 6, \text{ так как } f_3 \nmid x^5 + 1, \\ && \text{но } f_3 \mid x^6 + 1 = (x^2 + 1)(x^4 + x^2 + 1), \\ f_4 &= x^4 + x + 1, & \text{per } f_4 = 15 \text{ (проверить!).} \end{aligned}$$

**Лемма 9.1.**

Если  $\tilde{a} \in M(f)$ , то  $\text{per } \tilde{a} \mid \text{per } f$ .

*Доказательство.*

Пусть  $\text{per } f = T$ . По условию,  $f \mid x^T - 1$ , отсюда, с учётом того, что  $f(L)[\tilde{a}] = \tilde{0}$ , следует, что  $(L^T - E)[\tilde{a}] = \tilde{0}$ . Таким образом,  $T$  — период для  $\tilde{a}$ . Если  $T'$  — минимальный период, то  $T' \mid T$ .  $\square$

**Лемма 9.2.**

$\text{per } \tilde{a} = \text{per } f_\alpha$ .

*Доказательство.*

Пусть  $\tilde{a} \in M(x^{T'} - 1)$ . Тогда  $f_\alpha \mid x^{T'} - 1$  и  $\text{per } f_\alpha \leq T'$ . С другой стороны, из леммы 9.1 следует, что  $T' \mid \text{per } f_\alpha$ . Следовательно,  $\text{per } \tilde{a} = \text{per } f_\alpha$ .  $\square$

**Следствие 1.** Если  $f(x)$  неприводим, то для любого  $\tilde{a} \not\equiv 0$  из  $M(f)$  выполняется следующее равенство

$$\text{per } \tilde{a} = \text{per } f.$$

Если  $f(x)$  — неприводим, значит  $f_\alpha = f$ . Отсюда и следует справедливость утверждения.

Из лемм 9.1, 9.2 вытекает справедливость следующей теоремы.

**Теорема 9.3.** Если  $f(x)$  — примитивный многочлен степени  $n$  над полем  $F_q$ , то для любого  $\bar{a} \not\equiv 0$  из  $M(f)$  выполняется следующее равенство

$$\operatorname{per} \bar{a} = q^n - 1.$$

**Теорема 9.4.**

Пусть  $h(x) = f^r(x)$ ,  $r \in (p^k; p^{k+1}]$ ,  $k \geq 0$ ,  $f(x)$  — неприводимый многочлен степени  $n$  над полем  $GF(q)$  характеристики  $p$ ,  $\operatorname{per}(f) = T$ . Тогда периоды ЛРП из  $M(h)$  принимают значения:

$$T_0 = 1, T_1 = T, T_{j+1} = p^j \cdot T, j = \overline{1, k} \quad (9.8)$$

Причем, если  $N_j$  — число ЛРП из  $M(h)$  периода  $T_j$ , то

$$N_0 = 1, N_1 = q^n - 1, N_{j+2} = q^{np^{j+1}} - q^{np^j}, j = \overline{0, k-1}, \quad (9.9)$$

$$N_{k+1} = q^{n \cdot r} - q^{np^k}$$

*Доказательство.*

Поскольку  $T|q^n - 1$ , то  $(T, p) = 1$ . Поэтому для любого корня  $\alpha$  многочлена  $f(x)$

$$(x^T - 1)'|_{\alpha} = Tx^{T-1}|_{\alpha} \neq 0.$$

Отметим, что корни многочлена можно рассматривать как элементы поля  $GF(q)[x]/(f(x))$ . Следовательно,  $f(x)|(x^T - 1)$ . Поэтому для любого целого  $j \geq 0$ :

$$f^{p^j}(x)|(x^{p^j T} - 1) = (x^T - 1)^{p^j} \quad (9.10)$$

Покажем, что  $Q = \operatorname{per}(f^{p^j}) = p^j \cdot T$ . Действительно, из  $f^{p^j}(x)|(x^Q - 1)$  следует, что  $f|(x^Q - 1)$ . Поэтому,  $T|Q$ , т.е.  $Q = T \cdot w$  и поскольку  $f^{p^j}(x)|(x^{p^j T} - 1)$ ,  $(T, p) = 1$ , то  $Q = p^j \cdot T$ . Отсюда, с учетом (9.10), получим, что  $j = i$ , т.е.  $Q = p^j \cdot T$ , для любого целого  $j \geq 0$ . Пусть целое  $s \in (0; (p-1)p^j]$ . Тогда  $p^j + s \leq p^{j+1}$  и

$$f^{p^j}|f^{p^{j+s}}|f^{p^{j+1}}.$$

Таким образом из определения периода многочлена получаем, что

$$p^j \cdot T \mid \text{per}(f^{p^j+s}) \mid T p^{j+1} = \text{per}(f^{p^{j+1}}) \quad (9.11)$$

Так как  $(T, p) = 1$ , то из (9.11) следует, что  $\text{per}(f^{p^j+s}) = T \cdot p^t$ , для всех  $t \geq j$ . Но  $f^{p^j+s} \nmid (x^{Tp^j} - 1)$ , следовательно,  $t = j + 1$  и  $\text{per}(f^{p^j+s}) = T \cdot p^{j+1}$  для любого  $s \in (0; (p-1)p^j]$  и любого  $j \geq 0$ . Пусть  $N(j, s)$  — количество ЛРП  $\tilde{\alpha} \in M(f^{p^j+s})$ , для которых  $f_{\tilde{\alpha}} = f^{p^j+s}$  и, следовательно,  $\text{per}(\tilde{\alpha}) = T \cdot p^{j+1}$ . Поскольку ЛРП однозначно определяется своим начальным заполнением, то

$$N(j+2, s) = q^{n(p^j+s)} - q^{n(p^j+s-1)}. \quad (9.12)$$

Из (9.12) получаем:

$$\begin{aligned} N(j+2) &= |\{\tilde{\alpha} \in M(f^r) : \text{per}(\tilde{\alpha}) = T \cdot p^{j+1}\}| = \\ &= \sum_{s=1}^{(p-1)p^j} N(j+1, s) = q^{np^{j+1}} - q^{np^j}, \quad j = \overline{0, k-1}. \end{aligned}$$

При  $j = k$  имеем:

$$N(k+2) = \sum_{s=1}^r N(k+1, s) = q^{np^r} - q^{np^k}.$$

И, наконец,  $\text{per}(\tilde{\alpha}) = \text{per}(f)$  для  $\tilde{\alpha} \in M(f)$  и, поэтому  $N_1 = q^n - 1$ .  $\square$

**Следствие 9.2.** Если  $\text{per}(f) = T$ ,  $f$  — неприводим, то цикловая структура графа  $\Gamma(f^r)$  содержит  $\frac{q^n - 1}{T}$  циклов длины  $T$ ,  $\frac{q^{np^j} - q^{np^{j-1}}}{p^j T}$  циклов длины  $p^j T$ ,  $j = \overline{1, k}$  и  $\frac{q^{nr} - q^{np^k}}{p^{k+1} \cdot T}$  циклов длины  $p^{k+1} T$  и один цикл длины 1.

## Глава 10

# Автономные автоматы

### 10.1 Определения. Регистры сдвига

Напомним, что автономный автомат задаётся системой

$$\mathcal{A} = (S, Y, \phi, \psi),$$

где  $S$  — множество состояний,  $Y$  — выходной алфавит, отображение  $\phi : S \rightarrow S$  — функция переходов, отображение  $\psi : S \rightarrow Y$  — функция выходов.

В том случае, если  $S = F^n$ ,  $Y = F$  и

$$\phi = (x_2, \dots, x_n, f(x_1, \dots, x_n)), \psi(x_1, \dots, x_n) = x_1,$$

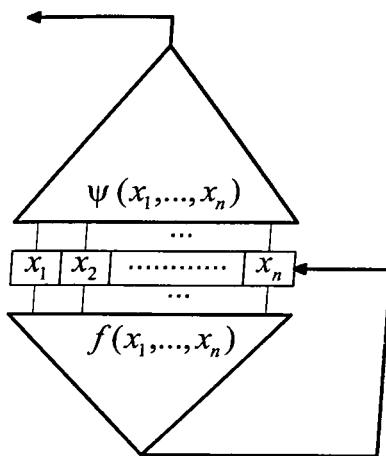
то автономный автомат  $\mathcal{R}(f, \psi) = (F^n, \phi, \psi)$  задаёт рекуррентную последовательность над полем  $F$  с характеристическим уравнением

$$x_i = f(x_{i-1}, \dots, x_{i-n}), \quad i = n+1, n+2, \dots$$

Такие автоматы ещё называются регистрами сдвига. В общем случае, когда  $\psi$  — произвольная функция, регистр сдвига

$$\mathcal{R}(f, \psi) = (F^n, F, \phi, \psi)$$

можно графически представить следующим образом:

Рис. 10.1. Автомат  $\mathcal{R}(f, \psi)$ 

Канонические уравнения автомата  $\mathcal{R}(f, \psi)$  имеют вид:

$$\left\{ \begin{array}{l} x_1(t) = x_2(t-1) \\ \dots \\ x_{n-1}(t) = x_n(t-1) \\ x_n(t) = f(x_1(t-1), \dots, x_n(t-1)) \\ y(t-1) = \psi(x_1(t-1), \dots, x_n(t-1)) \\ x_i(0) = \alpha_i, \quad i = \overline{1, n} - \text{начальное состояние}, t = 1, 2, \dots \end{array} \right.$$

На практике при построении шифров над полем  $\mathbb{Z}_2$  применяются регистры сдвига  $\mathcal{R}(f, \psi)$ , в которых  $f$ —линейная функция. При этом условии, как было показано раньше, можно выбрать  $f$  такой, чтобы граф автомата состоял из двух циклов длины  $2^n - 1$  и 1. Такая структура графа обеспечивает возможно большую длину выходной последовательности автомата. Это свойство и позволяет использовать такие схемы для

построения шифров гаммирования. Ключом в такой криптосистеме может служить как начальное состояние, так и функция  $\psi$ . Например, в качестве ключа можно использовать перестановку переменных или/и замену переменной её отрицанием. При этом возникает задача эквивалентности ключей. Два ключа (две подстановки из  $S_n$ ) называются *эквивалентными*, если при любом начальном состоянии соответствующие выходные последовательности (гаммы шифрования и расшифрования) одинаковы. Из этого определения следует, что функция  $\psi$  должна иметь тривиальную группу инерции относительно  $S_n$ . Известно, что при  $n \rightarrow \infty$  почти все функции алгебры логики имеют тривиальную группу инерции, но поиск таких функций весьма сложная задача. Кроме всего прочего, для обеспечения надлежащей стойкости такой системы функция  $\psi$  должна обладать определёнными криптографическими свойствами. В данном пособии эти проблемы не рассматриваются. Здесь же основной задачей является изучение цикловой структуры функции переходов  $\phi$ .

Важным классом автономных автоматов являются, так называемые, регулярные автоматы.

*Определение 10.1.* Автомат  $A = (S, Y, \phi, \psi)$  называется *регулярным*, если  $\phi$  — взаимно однозначное отображение множества  $S$  на себя.

Граф такого автомата состоит из непересекающихся циклов, поэтому регулярный автомат для любого начального заполнения генерирует периодическую выходную последовательность. При этом период последовательности является делителем длины цикла графа, на котором лежит начальное состояние.

Для регистра сдвига  $\mathcal{R}(f, \psi)$  над полем  $F$  регулярность обеспечивается выполнением условия:  $h(x) = f(x, \alpha_2, \dots, \alpha_n)$  для любого набора  $\alpha_2, \dots, \alpha_n$  из  $F$  является подстановкой на  $F$ . Напомним, что в случае, когда  $F = \mathbb{Z}_2$ , это условие принимает вид:

$$f(x_1, x_2, \dots, x_n) = x_1 \oplus g(x_2, \dots, x_n) \quad (10.1)$$

Возникает вопрос: как строить нелинейные регулярные регистры сдвига максимального периода  $2^n$ . Опишем процедуру, которая полностью решает эту задачу.

Пусть  $\mathcal{R}_{f,\phi}$  — регулярный регистр сдвига,

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

$$\phi : (x_1, x_2, \dots, x_n) \rightarrow (x_2, \dots, f(x_1, \dots, x_n))$$

и  $\Gamma_f$  — граф регистра и два его состояния  $\tilde{a} = (\alpha_1, \alpha_2, \dots, \alpha_n)$  и  $\tilde{b} = (\bar{\alpha}_1, \alpha_2, \dots, \alpha_n)$  лежат на разных циклах  $C_1$  и  $C_2$  соответственно. Рассмотрим регистр сдвига  $\mathcal{R}_{f',\phi'}$ , где

$$f' = x_1 \oplus g(x_2, \dots, x_n) \oplus x_2^{\alpha_2} \dots x_n^{\alpha_n},$$

$$\phi' : (x_1, x_2, \dots, x_n) \rightarrow (x_2, \dots, f'(x_1, \dots, x_n)).$$

Очевидно, для любого  $\tilde{c} \neq \tilde{a}$  и  $\tilde{c} \neq \tilde{b}$ ,  $f'(\tilde{c}) = f(\tilde{c})$ ,  $\phi(\tilde{c}) = \phi'(\tilde{c})$ , тогда  $\Gamma_{f'} \setminus \{C_1, C_2\} = \Gamma_f \setminus \{C_1, C_2\}$ . Посмотрим, что происходит на наборах  $\tilde{a}, \tilde{b}$ :

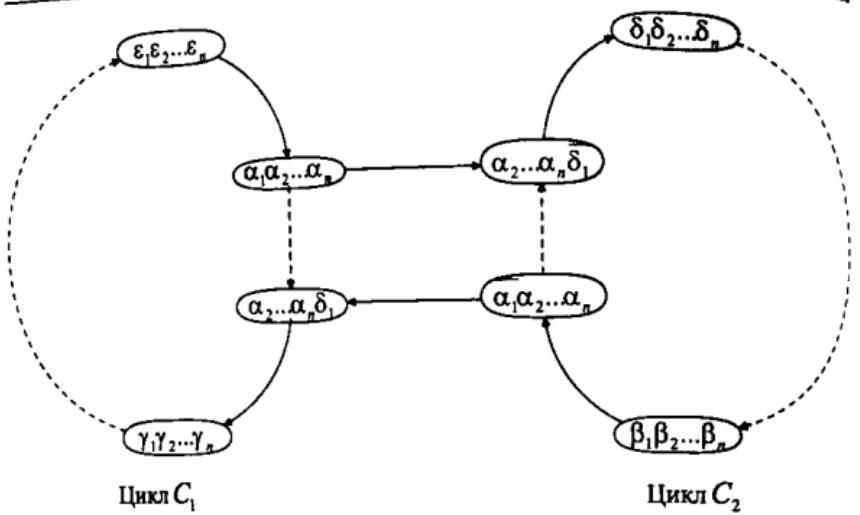
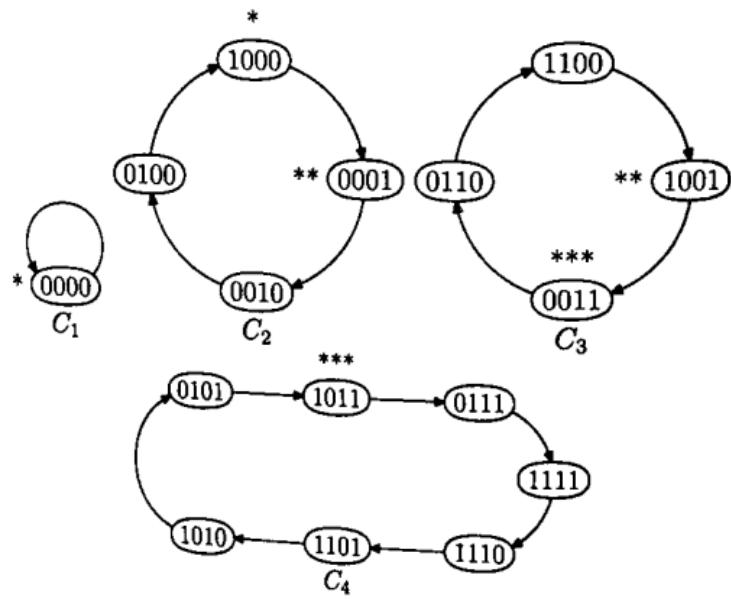
$$\begin{aligned}\phi(\tilde{a}) &= (\alpha_2, \dots, \alpha_n, \delta_1) = \tilde{a}_1, & \delta_1 &= \alpha_1 \oplus g(\alpha_2, \dots, \alpha_n); \\ \phi'(\tilde{a}) &= (\alpha_2, \dots, \alpha_n, \delta_2) = \tilde{b}_1, & \delta_2 &= \bar{\delta}_1; \\ \phi(\tilde{b}) &= (\alpha_2, \dots, \alpha_n, \delta_2) = \tilde{b}_1; \\ \phi'(\tilde{b}) &= (\alpha_2, \dots, \alpha_n, \delta_1) = \tilde{a}_1; \\ \phi'(\tilde{x}) &= \phi(\tilde{x}) \quad \forall \tilde{x} \in C_1 \cup C_2, & \tilde{x} &\neq \tilde{a}, \tilde{x} \neq \tilde{b}\end{aligned}$$

Таким образом график  $\Gamma_{f'}$  будет содержать все циклы графа  $\Gamma_f$ , кроме циклов  $C_1$  и  $C_2$ , а также в нём появится новый цикл, «склеенный» из  $C_1$  и  $C_2$ , который изображен на рисунке (рис. 10.2).

Такая процедура позволяет «исправлять» цикловую структуру графа нелинейного цикла над полем  $\mathbb{Z}_2$ .

**Следствие 10.1.** Если  $\mathcal{R}_f$  — линейный регистр сдвига максимального периода над полем  $\mathbb{Z}_2$ , и  $f' = f \oplus \bar{x}_2 \dots \bar{x}_n$ , то нелинейный регистр сдвига  $\mathcal{R}_{f'}$  имеет полный период равный  $2^n$ , где  $n$  длина регистра сдвига.

**Пример 10.1.** Пусть  $n = 4$ ,  $f = x_1 \oplus x_2 x_4$ .

Рис. 10.2. Склейивание циклов  $C_1$  и  $C_2$ Рис. 10.3. Граф  $\Gamma_1$

Построим граф  $\Gamma_1 = \Gamma_f$

Циклы  $C_1$  и  $C_2$  содержат соседние состояния 0000 и 0001. Циклы  $C_2$  и  $C_3$  — 0001 и 1001,  $C_3$  и  $C_4$  — 0011 и 1011. После «склеивания» цикла  $C_1$  с  $C_2$  и  $C_3$  с  $C_4$  получим граф  $\Gamma_2$ , состоящий из циклов  $C'_1$  и  $C'_2$  (рис. 10.4)

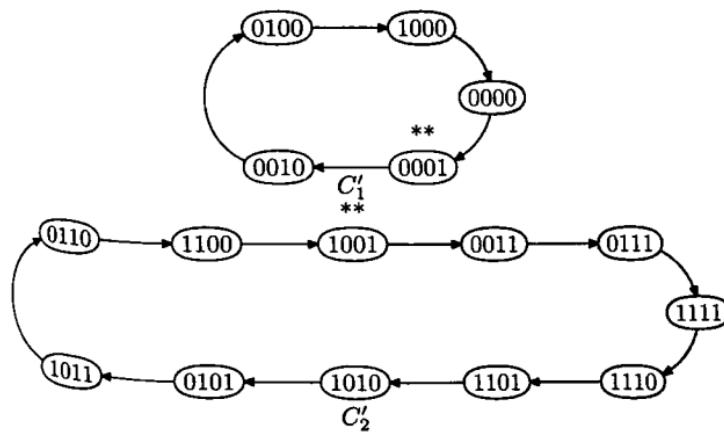


Рис. 10.4. Граф  $\Gamma_2$

Склейвая  $C'_1$  с  $C'_2$ , образуем граф  $\Gamma_3$  с единственным циклом (рис. 10.5).

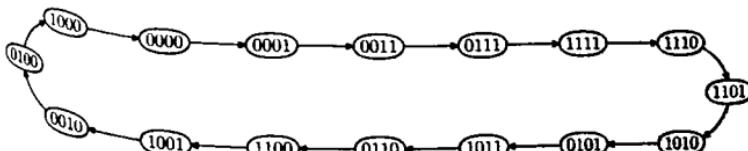


Рис. 10.5. Граф  $\Gamma_3$

В результате процедуры «склеивания» циклов мы получили регистр сдвига  $\mathcal{R}_{f'}$  с функцией обратной связи

$$\begin{aligned} f'(x_1, x_2, x_3, x_4) &= x_1 \oplus \bar{x}_2 \bar{x}_3 \bar{x}_4 \oplus \bar{x}_2 \bar{x}_3 x_4 \oplus \bar{x}_2 x_3 x_4 = \\ &= x_1 \oplus \bar{x}_2 \bar{x}_3 \oplus \bar{x}_2 x_3 x_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3 \oplus x_3 x_4 \oplus x_2 x_3 x_4 \oplus 1. \end{aligned}$$

Граф регистра  $\mathcal{R}_{f'}$  состоит из единственного цикла, который изображен на рис. 10.5.

**Пример 10.2.**  $n = 3$ ,  $f = x_1 \oplus x_2$ , то есть  $\mathcal{R}_f$  — линейный регистр сдвига максимального периода. Граф  $\Gamma_f$  изображен на рисунке 10.6.

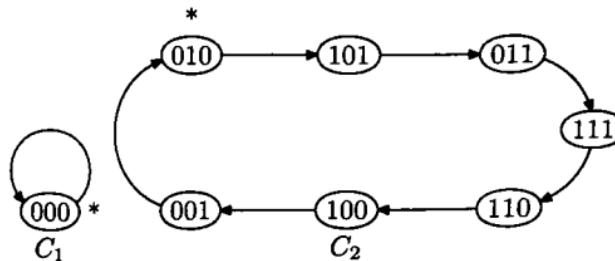


Рис. 10.6.

«Склейвая» циклы  $C_1$  и  $C_2$  по состояниям 001 и 000, получим нелинейный регистр сдвига

$$\mathcal{R}_{f'}, \quad f' = x_1 \oplus \bar{x}_2 \bar{x}_3 = x_2 x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$$

с одним циклом  $C$  (рис. 10.7).

## 10.2 Критерии регулярности автономных автоматов

$\mathcal{A} = (S, Y, \phi, \psi)$  — конечный автономный автомат, множество состояний и выходной алфавит которого состоят более чем из одного элемента. Множество всех отображений из множества

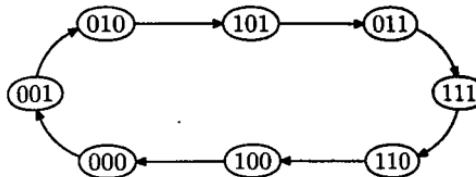


Рис. 10.7.

$S$  в множество  $Y$  будем обозначать через  $Y^S$ . Для любого элемента  $a \in Y = \{a_1, \dots, a_m\}$  и отображений  $\mu \in Y^S$  можно определить

$$\|\mu\|_a = |\{s \in S | \mu(s) = a\}|.$$

Весом отображения  $\mu \in Y^S$  будем называть набор

$$\|\mu\| = \{\|\mu\|_{a_1}, \dots, \|\mu\|_{a_m}\}.$$

Функция называется константой, если для некоторого  $i$  выполнено  $\|\mu\|_{a_i} = |S|$ . Как уже говорилось раньше, автомат называется регулярным, если  $\phi$  — подстановка на  $S$ . Композицией двух отображений  $\mu \in Y^S$  и  $\phi \in S^S$  называется отображение  $\mu \circ \phi : S \rightarrow Y$ , определённое по правилу  $\mu \circ \phi(s) = \mu(\phi(s))$ .

**Утверждение 10.1.** Автомат  $A = (S, Y, \phi, \psi)$  является регулярным, если и только если для любого, неравного тождественно константе, отображения  $\mu$  из множества  $Y^S$  выполнено одно из условий:

$$\|\mu \circ \phi\| = \|\mu\| \quad (10.2)$$

$$\|\mu \circ \phi\|_a = \|\mu\|_a, \forall a \in Y \quad (10.3)$$

**Доказательство.** Сначала заметим, что из (10.3) следует (10.2), поэтому будем проводить доказательство только для (10.3).

**Необходимость.** В силу того, что  $\phi$  подстановка на  $S$ , то  $\{\phi(s) | s \in S\} = S$ . Отсюда следует, что  $\|\mu \circ \phi\|_a = \|\mu\|_a, \forall a \in Y$ .

*Достаточность.* Допустим, что выполнено условие (10.3), а  $\phi$  не является подстановкой над  $S$ , тогда найдётся элемент  $s_0 \in S$  такой, что для любого  $s \in S$ ,  $\phi(s) \neq s_0$ . Построим функцию  $\mu_0 \in Y^S$  следующим образом:

$$\mu_0(s) = \begin{cases} a, & \text{если } s = s_0 \\ a' \neq a, & \text{если } s \neq s_0 \end{cases}$$

Из определения функции вытекает  $\|\mu_0\|_a = 1$ ,  $\|\mu \circ \phi\|_a = 0$ . Пришли к противоречию с условием (10.3).  $\square$

**Следствие 10.2.** Автомат  $A = (S, Y, \phi, \psi)$  является регулярным, если и только если для любого отображения  $\mu \in Y^S$ , отличного от тождественной константы, композиция  $\mu \circ \phi$  также отлична от постоянной.

Рассмотрим конечное коммутативное кольцо  $K$  с единицей. **Определение 10.2.** Модулем  $M$  над кольцом  $K$  называется множество, на котором определены операции сложения и умножения на элементы из  $K$ , причём для любых  $m, m_1, m_2 \in M$ ,  $k \in K$  должны выполняться условия:

- 1)  $m_1 + m_2 \in M$
- 2)  $k \cdot m \in M$

Очевидно, множество  $K^S$  является модулем над  $K$ . Операции сложения и умножения на элементы из  $K$  для функций из  $K^S$  вводятся естественным образом.

Для множества  $M \subset S$  можно ввести функцию  $\chi_M \in K^S$ , которая называется *характеристической функцией* множества  $M$  и определяется следующим образом:

$$\chi_M(s) = \begin{cases} e, & \text{если } s \in M \\ 0, & \text{иначе.} \end{cases}$$

Любую функцию  $\mu \in K^S$  можно однозначно представить в виде

$$\mu(s) = \sum_{a \in S} \mu(a) \chi_a(s).$$

Таким образом  $K^S$ —это  $|S|$ -мерный модуль над  $K$ .

**Определение 10.3.** Следом функции  $\mu \in K^S$  называется элемент кольца  $K$

$$Tr(\mu) = \sum_{s \in S} \mu(s)$$

**Утверждение 10.2.** Автомат  $A = (S, K, \phi, \psi)$  регулярный, если и только если для любой функции  $\mu \in K^S$  выполнено условие

$$Tr(\mu \circ \phi) = Tr(\mu) \quad (10.4)$$

*Доказательство.* Необходимость. В силу того, что  $\phi$  — перестановка на  $S$ , то сумма, определяющая следы отображений  $\mu$  и  $\mu \circ \phi$ , отличаются порядком слагаемых, но  $K$ —коммутативное кольцо, поэтому эти суммы равны.

Достаточность. Доказательство будем вести от противного. Пусть выполнено условие (10.4) и существует элемент  $s_0 \in S$  такой, что  $\forall s \in S, \phi(s) \neq s_0$ . Определим функцию  $\nu \in K^S$  следующим образом

$$\nu(s) = \begin{cases} e, & \text{при } s = s_0 \\ 0, & \text{иначе.} \end{cases}$$

Для неё выполнено следующее  $Tr(\nu) = e, Tr(\nu \circ \phi) = 0$ . Пришли к противоречию.  $\square$

### Теорема 10.1.

Автомат  $A = (S, K, \phi, \psi)$  регулярен, если и только если условие (10.4) выполнено для некоторого базиса модуля  $K^S$ .

*Доказательство.*

Необходимость. Следует из предыдущего утверждения.

Достаточность. Возьмём любую функцию  $\mu \in K^S$ , тогда  $\mu = \sum_{i=1}^N c_i \mu_i$ , где  $\mu_1, \dots, \mu_N$ —некоторый базис модуля  $K^S$ . Для каждой функции базиса выполняется условие (10.4), поэтому

верна следующая цепочка равенств:

$$\begin{aligned} Tr(\mu) &= \sum_{s \in S} \mu(s) = \sum_{s \in S} \left( \sum_{i=1}^N c_i \mu_i(s) \right) = \sum_{i=1}^N c_i \left( \sum_{s \in S} \mu_i(s) \right) = \\ &= \sum_{i=1}^N c_i Tr(\mu_i) = \sum_{i=1}^N c_i Tr(\mu_i \circ \phi) = \sum_{i=1}^N c_i \left( \sum_{s \in S} \mu_i(\phi(s)) \right) = \\ &= \sum_{s \in S} \left( \sum_{i=1}^N c_i \mu_i(\phi(s)) \right) = \sum_{s \in S} \mu(\phi(s)) = Tr(\mu \circ \phi). \end{aligned}$$

Итак, для любой функции  $\mu \in K^S$  мы доказали справедливость соотношения  $Tr(\mu) = Tr(\mu \circ \phi)$ , значит, в силу утверждения 10.2, достаточность доказана.  $\square$

**Следствие 10.3.** Автомат  $A = (S, K, \phi, \psi)$  регулярен, если и только если для некоторого базиса  $\mu_1, \dots, \mu_N$  модуля  $K^S$  выполнено условие

$$\|\mu_i\| = \|\mu_i \circ \phi\|, \quad i = \overline{1, N} \quad (10.5)$$

*Доказательство. Необходимость.* Следствие из утверждения 10.1.

*Достаточность.* Вытекает из того, что условие (10.5) для базиса влечёт за собой выполнение условия (10.2) для любого элемента.  $\square$

Теперь рассмотрим более узкий класс автоматов. Раньше множество  $S$  было любым, пусть теперь  $S = K^n$ , то есть множество состояний представляет собой упорядоченный  $n$ -элементный кортеж над кольцом  $K$ . В этом случае любое отображение  $\phi : S \rightarrow S$  задаётся системой из  $n$  функций, каждая из которых имеет  $n$  переменных, принимающих значения из кольца  $K$ , то есть

$$\phi = (f_1, \dots, f_n), \text{ где } f_i : K^n \rightarrow K.$$

Будем называть  $\phi$  в этом случае преобразованием. Введём в рассмотрение характеристическую функцию элемента  $a$  из кольца  $K$ :

$$x^{(a)} = \begin{cases} e, & \text{если } x = a \\ 0, & \text{иначе.} \end{cases}$$

Эта функция является обобщением соответствующей функции алгебры логики

$$x^{(a)} = x^a = \begin{cases} \bar{x}, & a = 0 \\ x, & a = 1. \end{cases}$$

Отметим, что функцию вида  $x_i^{(a)}$  мы будем рассматривать, как функцию, зависящую от  $n$  переменных, причём от всех, кроме  $i$ -той, фиктивно.

**Определение 10.4.** Характеристической функцией состояния

$$\tilde{a} = (a_1, \dots, a_n) \in K^n$$

называется отображение, заданное следующим образом:

$$\chi_{\tilde{a}}(x_1, \dots, x_n) = x_1^{(a_1)} x_2^{(a_2)} \cdots x_n^{(a_n)} = \begin{cases} e, & \text{если } \tilde{x} = \tilde{a} \\ 0, & \text{иначе.} \end{cases}$$

Функция  $\chi_{\tilde{a}}(\tilde{x}^n)$  при  $K = \mathbb{Z}_2$  обращается в конъюнкцию ранга  $n$ .

Из всего выше сказанного ясно, что любая функция

$$g(x_1, \dots, x_n) \in K^{K^n}$$

может быть представлена в виде

$$g(x_1, \dots, x_n) = \sum_{(a_1, \dots, a_n) \in K^n} g(a_1, \dots, a_n) x_1^{(a_1)} \cdots x_n^{(a_n)} \quad (10.6)$$

Представление (10.6) — это аналог совершенной дизъюнктивной нормальной формы для функции алгебры логики, зависящей от  $n$  переменных.

Таким образом, множество

$$\{x_1^{(a_1)} \cdots x_n^{(a_n)} = \tilde{x}^{\tilde{a}} | (a_1, \dots, a_n) \in K^n\}$$

есть базис модуля  $K^{K^n}$ . Применяя следствие 10.3 для данного базиса, получим следующее утверждение.

**Следствие 10.4.** *Преобразование  $\phi = (f_1, \dots, f_n)$  модуля  $K^{K^n}$  взаимно однозначно, если и только если для любых  $a_1, \dots, a_n$  из кольца  $K$  выполняется условие*

$$\|f_1^{(a_1)} \cdots f_n^{(a_n)}\|_e = 1.$$

*Доказательство.* Воспользуемся следствием 10.3. В нашем случае  $\mu_i = \chi_{\tilde{a}}$ , и если  $\phi = (f_1, \dots, f_n)$ , то  $\mu \circ \phi = f_1^{(a_1)} \cdots f_n^{(a_n)}$ , но  $\|\chi_{\tilde{a}}\|_e = 1$ , поэтому и  $\|\chi_{\tilde{a}} \circ \phi\|_e = 1$ .  $\square$

Заметим, что предложенный базис избыточен, ибо

$$x_i^{(0)} = e - \sum_{a \in K \setminus \{0\}} x_i^{(a)},$$

поэтому можно исключить функцию  $x_i^{(0)}$  из всех базисных функций  $x_1^{(a_1)} \cdots x_n^{(a_n)}$ . В результате получим новый базис модуля  $K^n$

$$\{e, x_{i_1}^{(a_1)} \cdots x_{i_n}^{(a_n)} | 1 \leq i_1 < i_2 < \dots < i_n \leq n, a_i \in K \setminus \{0\}\}.$$

**Следствие 10.5.** *Преобразование  $\phi = (f_1, \dots, f_n)$  модуля  $K^n$  взаимно однозначно, если и только если*

$$Tr(f_{i_1}^{(a_1)} \cdots f_{i_m}^{(a_m)}) = 0; m = \overline{1, n-1},$$

$$1 \leq i_1 < i_2 < \dots < i_m \leq n, a_i \in K \setminus \{0\}$$

$$Tr(f_1^{(a_1)} \cdots f_n^{(a_n)}) = 1; a_i \in K \setminus \{0\}$$

*Доказательство.* В конечном кольце  $K$  при любом  $a \in K$   $a|K| = 0$ , так как относительно сложения  $K$ -абелева группа

порядка  $|K|$ . Учитывая это свойство конечных колец, получаем при  $m < n$ :

$$\text{Tr}(x_{i_1}^{(a_1)} \cdots x_{i_m}^{(a_m)}) = \left( \sum_{(b_{i_1} \dots b_{i_m}) \in K^m} b_{i_1}^{(a_1)} \cdots b_{i_m}^{(a_m)} \right) |K|^{n-m} = 0,$$

а для  $m = n$

$$\text{Tr}(x_1^{(a_1)} \cdots x_n^{(a_n)}) = \sum_{(b_1 \dots b_n) \in K^n} b_1^{(a_1)} \cdots b_n^{(a_n)} = e.$$

Отсюда и из следствия 10.3 получаем требуемый результат.  $\square$

**Следствие 10.6.** Преобразование  $\phi = (f_1, \dots, f_n)$  модуля  $K^{K^n}$  взаимно однозначно, если и только если соотношение

$$\|f_{i_1}^{(a_1)} \cdots f_{i_m}^{(a_m)}\|_e = |K|^{n-m} \quad a_i \in K \setminus \{0\}$$

выполняется для всех  $1 \leq i_1 < i_2 < \dots < i_m \leq n$ .

**Доказательство.** Справедливость следствия вытекает из того, что  $\|x_{i_1}^{(a_1)} \cdots x_{i_m}^{(a_m)}\|_e = |K|^{n-m}$  и  $\|x_{i_1}^{(a_1)} \cdots x_{i_m}^{(a_m)}\|_a = 0$ , если  $a \neq e, a \neq 0$ .  $\square$

Наложим на  $K$  дополнительные условия, а именно, пусть  $K = F_q$  — поле из  $q$  элементов. При этих условия

$$x_i^{(a)} = 1 - (x_i - a)^{q-1},$$

поэтому из разложения (10.6) следует, что любая функция  $f: F_q^n \rightarrow F_q$  может быть представлена в виде многочлена с коэффициентами из  $F$  от переменных  $x_1, \dots, x_n$ , причём степень вхождения каждой переменной не превосходит  $q-1$ . Представление в виде многочлена является обобщением полинома Жегалкина функций алгебры логики для полей, отличных от  $\mathbf{Z}_2$ .

Из всего, выше сказанного, следует, что система

$$\{1, x_{i_1}^{l_1} \cdots x_{i_m}^{l_m} | m = \overline{1, n}, 1 \leq i_1 < i_2, \dots < i_m \leq n, 1 \leq l_i \leq q-1\}$$

является базисом модуля  $F_q^{F_q^n}$ .

**Лемма 10.1.**

След функции  $f$  равен старшему коэффициенту в полиномиальном представлении  $f$  от  $n$  переменных, при чётном  $n$  взятым с положительным знаком, а при нечётном — с отрицательным.

**Доказательство.**

Требуется доказать, что  $\text{Tr}(f) = (-1)^n a_{12\dots n}$ , где  $a_{12\dots n}$  коэффициент при старшем члене  $x_1^{q-1} \cdots x_n^{q-1}$  в полиноме функции  $f$ .

Рассмотрим несколько случаев:

1.  $m < n$ .

$$\text{Tr}(x_{i_1}^{l_1} \cdots x_{i_m}^{l_m}) = \left( \sum_{(b_{i_1}, \dots, b_{i_m}) \in F_q^m} b_{i_1}^{l_1} \cdots b_{i_m}^{l_m} \right) q^{n-m} = 0;$$

2.  $m = n$ ,  $\exists l_i \neq q - 1$ , не ограничивая общности, можно считать, что  $l_1 < q - 1$ . Тогда будем иметь:

$$\begin{aligned} \text{Tr}(x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}) &= \sum_{(b_1, \dots, b_n) \in F_{q^n}} b_1^{l_1} b_2^{l_2} \cdots b_n^{l_n} = \\ &= \sum_{(b_2, \dots, b_n) \in F_{q^{n-1}}} b_2^{l_2} \cdots b_n^{l_n} \left( \sum_{b_1 \in F_q} b_1^{l_1} \right), \end{aligned}$$

но поскольку  $\sum_{x \in F_q} x^t = 0$  для всех  $t < q - 1$ , то

$$\text{Tr}(x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}) = 0;$$

3.  $m = n$ ,  $l_i = q - 1$ ,  $\forall i = \overline{1, n}$

Так как  $\sum_{x \in F_q} x^{q-1} = -1$ , то

$$\begin{aligned} Tr(x_1^{q-1}x_2^{q-1} \dots x_n^{q-1}) &= \sum_{(b_1, \dots, b_n) \in F_q^n} b_1^{q-1}b_2^{q-1} \dots b_n^{q-1} = \\ &= \left( \sum_{b_1 \in F_q} b_1^{q-1} \right) \left( \sum_{b_2 \in F_q} b_2^{q-1} \right) \dots \left( \sum_{b_n \in F_q} b_n^{q-1} \right) = (-1)^n. \end{aligned}$$

Для завершения доказательства нужно заметить, что

$$Tr(v + w) = Tr(v) + Tr(w).$$

Итак, лемма полностью доказана.  $\square$

**Теорема 10.2** (Э.Ф. Скворцов).  $\square$

Преобразование  $\phi = (f_1, \dots, f_n)$  векторного пространства  $F_q^n$  взаимно однозначно, если и только если для какого либо базиса  $g_1, \dots, g_{q^n}$  модуля  $F_q^{F_q^n}$  старшие коэффициенты у приведённых многочленов функций

$$g_i(x_1, \dots, x_n) \text{ и } g_i(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$

равны для любого  $i = \overline{1, q^n}$ .

*Доказательство.*

Справедливость следует из леммы и теоремы 10.1.  $\square$

**Следствие 10.7.** (*Обобщённый критерий Хаффмана*). Преобразование  $\phi = (f_1, \dots, f_n)$  пространства  $F_q^n$  взаимно однозначно, если и только если старший коэффициент приведённого многочлена функций

$$f_{i_1}^{l_1} \dots f_{i_m}^{l_m}, \quad m = \overline{1, n-1}, \quad 1 \leq i_1 < \dots < i_m \leq n, \quad 1 \leq l_i \leq q-1$$

и функций

$$f_1^{l_1} \dots f_n^{l_n}, \quad \exists l_i \neq q-1$$

равен 0, а функции

$$f_1^{q-1} \dots f_n^{q-1}$$

равен 1.

## Глава 11

# Линейный конгруэнтный метод

Пусть  $f(x) \in \mathbb{Z}[x]$ . Будем говорить, что многочлен  $f(x)$  *биективен по модулю  $n$* , если отображение  $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ , индуцированное этим многочленом, биективно.

**Упражнение 11.1.** Доказать, что если  $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ , то  $f$  биективен по модулю  $n$  тогда и только тогда, когда  $f$  биективен по всем модулям  $p_i^{k_i}$  для  $i = \overline{1, t}$ .

Отсюда, в частности, следует, что для построения биективных многочленов в кольце вычетов необходимо уметь строить биективные многочлены по модулю степени простого числа.

### Теорема 11.1.

Многочлен  $f(x) \in \mathbb{Z}[x]$  биективен по модулю  $p^n$  для любого  $n = 1, 2, \dots$  тогда и только тогда, когда выполняются следующие условия:

- (1)  $f(x)$  биективен по модулю  $p$ ;
- (2)  $f'(x) \not\equiv 0 \pmod{p}$  для любого  $x \in \mathbb{Z}$ .

*Доказательство.*

Разложим многочлен  $f(x + yp^r)$  степени  $m \geq 1$  в ряд Тейлора по модулю  $p^{r+1}$ :

$$f(x + yp^r) = f(x) + yp^r f'(x) + \sum_{i=2}^m y^i p^{ri} \frac{f^{(i)}(x)}{i!} \pmod{p^{r+1}}$$

Так как  $p^{ri} \geq p^{r+1}$  для всех  $i = \overline{2, m}$ , то мы получаем, что

$$f(x + yp^r) = f(x) + yp^r f'(x) \pmod{p^{r+1}} \quad (11.1)$$

Перейдём теперь непосредственно к доказательству теоремы.

**Необходимость.** Пусть  $f(x)$  биективен по  $\text{mod } p^k$ ,  $k \geq 2$ . Следовательно,  $f(x)$  будет биективен по  $\text{mod } p$ .

Допустим, что  $f'(x_0) = 0 \pmod{p}$  для некоторого  $x_0 \in \mathbb{Z}$ . Из (11.1) следует, что  $f(x_0 + p) = f(x_0) + pf'(x_0) = f(x_0) \pmod{p^2}$ .

Таким образом,  $f(x_0 + p) = f(x_0) \pmod{p^2}$ , что противоречит биективности многочлена  $f$ , поскольку  $x_0 + p \neq x_0 \pmod{p^2}$ .

**Достаточность** будем доказывать индукцией по  $n$ . При  $n = 1$  биективность многочлена следует из первого условия теоремы. Пусть мы установили биективность  $f(x)$  по модулю  $p^k$  ( $k \geq 1$ ) и пусть  $f(u) = f(v) \pmod{p^{k+1}}$ . Тогда  $f(u) = f(v) \pmod{p^k}$  и, следовательно, по индуктивному предположению  $u \equiv v \pmod{p^k}$ , что равносильно равенству  $u = v + yp^k$ . Отсюда с учётом (1) получим:

$$f(u) = f(v) + yp^k f'(v) \pmod{p^{k+1}}.$$

Поскольку по условию теоремы  $f'(v) \not\equiv 0 \pmod{p}$ , последнее равенство означает, что  $p \mid y$ , и, следовательно,

$$u \equiv v \pmod{p^{k+1}}.$$

Теорема полностью доказана. □

**Определение 11.1.** Многочлен  $f(x) \in \mathbb{Z}[x]$  называется транзитивным по модулю  $m$ , если индуцируемое им отображение  $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_m$  является подстановкой на  $\mathbb{Z}_m$ , состоящей из одного цикла.

**Упражнение 11.2.** Доказать, что многочлен  $f(x)$  транзитивен по модулю  $m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$  тогда и только тогда, когда он транзитивен по всем модулям  $p_i^{k_i}$  для  $i = \overline{1, t}$ .

**Лемма 11.1.**

Многочлен  $f(x) = a + bx$  транзитивен по модулю простого числа  $p$  тогда и только тогда, когда выполняются условия:

$$\begin{cases} \text{НОД}(a, p) = 1, \\ b \equiv 1 \pmod{p}. \end{cases} \quad (11.2)$$

*Доказательство.*

Заметим, что поскольку выполняются условия предыдущей теоремы, то  $f(x)$  есть подстановка на  $\mathbb{Z}_p$ .

**Достаточность.** Возьмём в качестве начального значения  $x = 0$ , будем иметь:

$$\begin{aligned} f(0) &= f^1(0) = a, \\ f^2(0) &= f(a) = a + ba, \\ f^3(0) &= f(a + ba) = a + ab + b^2a = a(1 + b + b^2). \end{aligned}$$

Нетрудно убедиться, что

$$f^i(0) = a(1 + b + \dots + b^{i-1}), \quad i = 1, 2, \dots \quad (11.3)$$

Из (11.3) следует, что если  $b \equiv 1 \pmod{p}$  и  $\text{НОД}(a, p) = 1$ , то  $f^i(0) = ai \pmod{p}$ .  $f^i(0) \neq 0$  при  $i = \overline{1, p-1}$  и, следовательно, подстановка  $f(x)$  состоит в  $\mathbb{Z}_p$  из одного цикла. Достаточность условий леммы установлена.

**Необходимость.** Ясно, что если  $f(x)$  — полноцикловая подстановка, то  $\text{НОД}(a, p) = 1$ . В противном случае

$$f(0) = a = 0 \pmod{p}$$

и подстановка  $f(x)$  содержит цикл длины 1.

Допустим, что  $b \not\equiv 1 \pmod{p}$ . Тогда из (11.3) следует, что

$$a_i = f^i(0) = \frac{a(b^i - 1)}{b - 1} = a(b^i - 1)(b - 1)^{-1} \pmod{p}, \quad i = 0, 1, \dots$$

Из последнего соотношения, положив  $i = p$ , получим:

$$0 = a_p = a(b^p - 1)(b - 1)^{-1} \pmod{p} \quad (11.4)$$

Поскольку  $b^p = b \pmod{p}$ , то из (11.4) немедленно следует, что  $a = 0 \pmod{p}$ . Пришли к противоречию и лемма полностью доказана.  $\square$

**Теорема 11.2** (Критерий транзитивности линейного многочлена).

Многочлен  $f(x) = a + bx$  транзитивен по  $\pmod{p^n}$  для любого натурального  $n$  тогда и только тогда, когда выполняются условия:

$$\begin{aligned} \text{при } p \neq 2: \quad & \begin{cases} HO\Delta(a, p) = 1, \\ b \equiv 1 \pmod{p}; \end{cases} \\ \text{при } p = 2: \quad & \begin{cases} HO\Delta(a, p) = 1, \\ b \equiv 1 \pmod{4}. \end{cases} \end{aligned} \quad (11.5)$$

*Доказательство.*

**Необходимость.** При  $p \neq 2$  необходимость выполнения условий теоремы следует из Леммы 1. Пусть  $p = 2$ . Первое условие должно выполняться в силу Леммы 1. Допустим, что второе условие не выполняется и, следовательно,  $b = 3 \pmod{4}$ . Тогда  $f(0) = a$ ,  $f(a) = a + 3a = 0 \pmod{4}$ . Таким образом, подстановка  $f$  на  $\mathbb{Z}_4$  имеет цикл длины 2. Пришли к противоречию.

**Достаточность.** Доказательство достаточности будемвести индукцией по  $n$ .

Случай  $p \geq 3$ . При  $n = 1$  справедливость теоремы следует из Леммы 1. Так как для  $f$  выполнены условия Теоремы 1, то  $f$  — подстановка на  $\mathbb{Z}_{p^n}$  и допустим, что  $f$  транзитивна по модулю  $p^n$ ,  $n \geq 1$ . Рассмотрим цикл этой подстановки, содержащий 0:  $(0, f^1(0), \dots, f^{i-1}(0)) \pmod{p^{n+1}}$ , где  $i$  — минимальное число такое, что  $f^i(0) \equiv 0 \pmod{p^{n+1}}$ . Следовательно,  $f^i(0) \equiv 0 \pmod{p^n}$ . Это означает, что  $i = lp^n$ ,  $1 \leq l \leq p$  ( $p^n$  есть минимальный период последовательности  $\{f^k(0): k = 0, 1, \dots\} \pmod{p^n}$ , а любой другой период кратен минимальному). Из определения  $f^{lp^n}(0) \equiv 0 \pmod{p^{n+1}}$  имеем:  $f^{lp^n}(0) = a(1 + b + \dots + b^{lp^n-1})$ . Так как  $b \equiv 1 \pmod{p}$ , то  $b = 1 + sp$ . Если  $s = 0$ , то  $f^{lp^n}(0) = alp^n$  и будет равно 0 тогда и только тогда, когда  $l = p$ , и, следовательно, длина цикла подстановки  $f(x)$  на  $\mathbb{Z}_{p^{n+1}}$  будет равна  $p^{n+1}$ . Если  $s \neq 0$ , то

$$\begin{aligned} f^{lp^n}(0) &= \frac{a(b^{lp^n} - 1)}{b - 1} = \frac{a((1 + sp)^{lp^n} - 1)}{sp} = \\ &= alp^n + a \sum_{j=2}^{lp^n} \binom{lp^n}{j} s^{j-1} p^{j-1} \equiv 0 \pmod{p^{n+1}} \end{aligned} \quad (11.6)$$

Покажем, что  $B_j = \binom{lp^n}{j} s^{j-1} p^{j-1} \equiv 0 \pmod{p^{n+1}}$ . Используя равенство

$$\begin{aligned} \binom{m}{j} &= \frac{m(m-1)\dots(m-j+1)}{12\dots(j-1)j} = \\ &= \frac{m}{j} \left(\frac{m}{1}-1\right) \left(\frac{m}{2}-1\right) \dots \left(\frac{m}{j-1}-1\right), \end{aligned}$$

получим:

$$\binom{lp^n}{j} = \frac{lp^n}{j} \left(\frac{lp^n}{1}-1\right) \left(\frac{lp^n}{2}-1\right) \dots \left(\frac{lp^n}{j-1}-1\right).$$

Очевидно, что при  $k < lp^n$ ,  $w_k = \frac{lp^n}{k} = \frac{s}{k'} = s(k')^{-1} \pmod{p}$ , где  $\text{НОД}(k', p) = 1$  (степень вхождения простого числа  $p$  в разложение числа  $k$  не превосходит  $n$ ). Поэтому

$$\binom{lp^n}{j} = \frac{lp^n}{j} (w_1-1)(w_2-1)\dots(w_{j-1}-1) = \frac{lp^n}{j} \Omega_j \pmod{p^{n+1}}.$$

Возможны случаи:

- a)  $\text{НОД}(j, p) = 1$ . Тогда  $B_j = j^{-1}l\Omega_js^{j-1}p^{n+j-1} \equiv 0 \pmod{p^{n+1}}$ , так как  $j \geq 2$ , то  $n + j - 1 \geq n + 1$ .
- b)  $j = p^t r$ ,  $t \geq 1$ ,  $\text{НОД}(r, p) = 1$ . В этом случае

$$B_j = r^{-1}\Omega_js^{j-1}p^{n+p^tr-t-1} \pmod{p^{n+1}}.$$

Так как  $p \geq 3$ , то  $p^t \geq t + 2$  и, следовательно,

$$n + p^tr - t - 1 \geq n + (t + 2) \cdot 1 - t - 1 = n + 1$$

и  $B_j \equiv 0 \pmod{p^{n+1}}$ .

Отсюда с учётом (11.6) получаем, что

$$f^{lp^n}(0) = alp^n \equiv 0 \pmod{p^{n+1}}.$$

Так как  $\text{НОД}(a, p) = 1$ , то  $l = p$ . Следовательно, длина цикла подстановки  $f$  на  $\mathbb{Z}_{p^{n+1}}$  равна  $p^{n+1}$ .

Случай  $p = 2$ . Если  $n = 2$ , то  $f(x) = x + 1 \pmod{4}$  и, очевидно, что  $f$  полноцикловая на  $\mathbb{Z}_4$ . Допустим, что  $f(x)$  транзитивна по модулю  $2^n$  ( $n \geq 2$ ). Рассмотрим последовательность

$$(0, f^1(0), \dots, f^{2^n-1}(0), f^{2^n}(0), f^{2^n+1}(0), \dots, f^{2^{n+1}-1}(0)) \pmod{2^{n+1}} \quad (11.7)$$

Так как  $f$  полноцикловая по модулю  $2^n$ ,

$$f^{2^n}(0) \equiv 0 \pmod{2^n}.$$

Если мы докажем, что  $f^{2^n}(0) \not\equiv 0 \pmod{2^{n+1}}$ , то это будет означать, что последовательность (11.7) является циклом подстановки  $f$  на  $\mathbb{Z}_{2^{n+1}}$ , поскольку  $f^{2^n+j}(0) = f^j(0) \pmod{2^n}$  при  $j = \overline{0, 2^n - 1}$ .

По определению  $f^{2^n}(0) = a(1 + b + \dots + b^{2^n-1})$ , где по условию теоремы  $b = 1 + 4s$ . Если  $s = 0$ , то  $f$  транзитивна по

модулю  $2^{n+1}$ , так как  $f^i(0) = ai$ ,  $i = \overline{0, 2^{n+1} - 1}$ ,  $\text{НОД}(a, 2) = 1$ . Рассмотрим ситуацию, когда  $s \neq 0$ . Тогда будем иметь

$$\begin{aligned} f^{2^n}(0) &= a \sum_{j=0}^{2^n-1} b^j = a \frac{b^{2^n} - 1}{b - 1} = a \frac{(1 + 4s)^{2^n} - 1}{4s} = \\ &= a \sum_{j=1}^{2^n} \binom{2^n}{j} 4^{j-1} s^{j-1} = a 2^n + \sum_{j=2}^{2^n} \binom{2^n}{j} 4^{j-1} s^{j-1} \pmod{2^{n+1}} \end{aligned} \quad (11.8)$$

Так как  $\binom{2^n}{j} = \frac{2^n}{j} \left(\frac{2^n}{1} - 1\right) \dots \left(\frac{2^n}{j-1} - 1\right)$  и  $\frac{2^n}{k} = w_k$  при  $k < 2^n$  – обратимый элемент в  $\mathbb{Z}_{2^{n+1}}$  ( $2$  входит в каноническое разложение числа  $k$  с показателем степени меньше, чем  $n$ ), то

$$\binom{2^n}{j} = \frac{2^n}{j} (w_1 - 1)(w_2 - 1) \dots (w_{j-1} - 1) = \frac{2^n}{j} \Omega_j \quad (11.9)$$

Пусть  $j = j' 2^{r_j}$ , где  $\text{НОД}(j', 2) = 1$  и  $r_j$  – максимальная степень вхождения  $2$  в каноническое разложение числа  $j$ . Очевидно, что  $r_j \leq \log_2 j$ . Рассмотрим слагаемое  $B_j = \binom{2^n}{j} 2^{2j-2} s^{j-1}$  суммы (11.8) с номером  $j \geq 2$ . С учётом (11.9) будем иметь:

$$\begin{aligned} B_j &= \frac{2^{n+2j-2} \Omega_j s^{j-1}}{j} = \frac{2^{n+2j-2-r_j} \Omega_j s^{j-1}}{j'} = \\ &= 2^{n+2j-2-r_j} (j')^{-1} s^{j-1} \pmod{2^{n+1}}. \end{aligned}$$

Поскольку при  $j \geq 2$  справедливо равенство  $2j-3 \geq \log_2 j \geq r_j$ , то  $n+2j-2-r_j \geq n+1$ , следовательно,  $B_j \equiv 0 \pmod{2^{n+1}}$ . Так как  $\text{НОД}(a, 2) = 1$ , то из (11.8) получаем, что

$$f^{2^n}(0) = a 2^n \not\equiv 0 \pmod{2^{n+1}}.$$

Тем самым достаточность условия теоремы для случая  $p = 2$  доказана, что завершает доказательство всей теоремы.  $\square$

## Глава 12

# Строение конечных групп

### 12.1 Конечные абелевы группы

**Теорема 12.1.**

*Любая конечная абелева группа порядка  $p^n$  (р простое) является прямым произведением своих циклических подгрупп.*

*Доказательство.*

Применим индукцию по  $n$ . При  $n = 1$  утверждение справедливо, поскольку группа простого порядка циклическая.

Допустим, что мы установили справедливость теоремы для всех групп порядка  $p^k$ , где  $k < n$ ,  $n \geq 1$ , и рассмотрим группу  $G$  порядка  $p^n$ . Из конечности группы следует, что найдётся элемент  $a_0 \in G$ , имеющий максимальный порядок. Очевидно, что  $\text{ord}(a_0) = p^m$ ,  $1 \leq m \leq n$ . Если  $m = n$ , то  $G$  — циклическая. В случае, когда  $m < n$ , рассмотрим фактор-группу  $\bar{G} = G/A_0$ , где  $A_0$  — циклическая группа, порождённая элементом  $a_0$ , то есть  $A_0 = \langle a_0 \rangle$  и  $|A_0| = p^m$ .

По теореме Лагранжа порядок группы  $\bar{G}$  равен  $p^{n-m} < p^n$ . Следовательно, согласно предположению индукции, абелева группа  $\bar{G}$  является прямым произведением своих циклических подгрупп:

$$\bar{G} = \bar{A}_1 \times \bar{A}_2 \times \cdots \times \bar{A}_r, \quad (12.1)$$

где  $\overline{G} = \{A_0, g_2 A_0, \dots, g_{p^{n-m}} A_0\}$ ,  $g_i A_0$  — смежные классы группы  $G$  по подгруппе  $A_0$ .

Из цикличности группы  $\overline{A}_i$  следует, что

$$\overline{A}_i = \langle \bar{b}_i \rangle = \langle b_i A_0 \rangle, \quad |\overline{A}_i| = p^{m_i}, \quad \sum m_i = n - m,$$

где  $b_i$  — некоторый элемент смежного класса  $b_i A_0$ .

Таким образом,

$$\overline{A}_i = \{\bar{e}, \bar{b}_i, \bar{b}_i^2, \dots, \bar{b}_i^{p^{m_i}-1}\} = \{A_0, b_i A_0, \dots, b_i^{p^{m_i}-1} A_0\}.$$

По определению группы  $\overline{A}_i$  имеем:

$$\bar{b}_i^{p^{m_i}} = \bar{e}, \text{ т.е. } b_i^{p^{m_i}} = a_0^{s_i} \in A_0 = \langle a_0 \rangle. \quad (12.2)$$

Из (1) следует, что для любого  $\bar{x} \in \overline{G}$  справедливо разложение

$$\bar{x} = \bar{b}_1^{-t_1} \cdots \bar{b}_r^{-t_r}$$

где  $0 \leq t_i < p^{m_i}$ ,  $i = \overline{0, r}$ ,  $m_0 = m$ . Следовательно,

$$x = b_1^{t_1} \cdots b_r^{t_r} a_0^{t_0}, \quad x \in G. \quad (12.3)$$

Покажем, что можно так подобрать  $b_i$ , что разложение (12.3) будет однозначно для каждого  $x \in G$ . Для этого, учитывая, что  $m_i \leq m$ , возведём обе части равенства (12.2) в степень  $p^{m-m_i}$ :

$$e = b_i^{p^m} = a_0^{s_i p^{m-m_i}}.$$

Так как порядок элемента  $a_0$  равен  $p^m$ , то из последнего равенства следует, что  $p^m \mid s_i p^{m-m_i}$ . Поэтому, учитывая (12.2), получим

$$s_i = p^{m_i} t_i, \quad b_i^{p^{m_i}} = a_0^{t_i p^{m_i}}. \quad (12.4)$$

Далее, заметим, что элемент  $a_i = b_i a_0^{-t_i} \in \langle b_i \rangle = b_i A_0$ . Покажем, что его порядок равен  $p^{m_i}$ . В самом деле, имеем:

$$b_i^{p^{m_i}} \cdot a_0^{-t_i p^{m_i}} = a_0^{t_i p^{m_i}} \cdot a_0^{-t_i p^{m_i}} = e,$$

то есть  $a_i^{p^{m_i}} = e$ . Следовательно,  $ord(a_i) = p^c$ ,  $c \leq m_i$ . Так как  $b_i = a_0^{t_i} a_i$ , то

$$b_i^{p^c} = a_i^{p^c} a_0^{t_i p^c} = a_0^{t_i p^c} \in \langle a_0 \rangle.$$

Следовательно,  $\bar{b}_i^{p^c} = \bar{e}$ , где  $c \leq m_i$ . Отсюда и из определения группы  $\bar{A}_i = \langle \bar{b}_i \rangle$  следует, что  $c = m_i$  и  $\text{ord}(a_i) = p^{m_i}$ , т. е.  $a_i$  — также образующий элемент группы  $\langle b_i \rangle$ . Поэтому, заменив в (12.3)  $b_i$  на  $a_i$ , получим:

$$x = a_1^{t_1} a_2^{t_2} \cdots a_r^{t_r} a_0^{t_0}, \quad 0 \leq t_i < p^{m_i}, \quad i = \overline{0, r} \quad (12.5)$$

Покажем, что элемент  $x \in G$  однозначно определён разложением (12.5). Для этого достаточно доказать, что если

$$a_1^{v_1} a_2^{v_2} \cdots a_r^{v_r} a_0^{v_0} = e, \quad v_i < p^{m_i}, \quad (12.6)$$

то  $v_i = 0$ ,  $i = \overline{0, r}$ .

Действительно, применяя к обеим частям (12.6) естественный гомоморфизм  $G \rightarrow \bar{G}$ , получим:

$$\bar{a}_1^{-v_1} \bar{a}_2^{-v_2} \cdots \bar{a}_r^{-v_r} = \bar{e} \quad (12.7)$$

Из индуктивного предположения следует, что  $\bar{a}_i^{-v_i} = \bar{e}$ , то есть  $a_i^{v_i} \in \langle a_0 \rangle = A_0$ . Так как  $a_i \notin A_0$ , то  $v_i = 0$ ,  $i = \overline{1, r}$ . Но тогда из (12.6) следует, что  $v_0 = 0$ . Теорема полностью доказана.  $\square$

### Лемма 12.1.

Пусть  $G$  — некоторая группа,  $g \in G$  и  $\text{ord}(g) = n_1 n_2 \cdots n_k$ , где  $\text{НОД}(n_i, n_j) = 1$  при  $i \neq j$ . Тогда  $g$  единственным образом представляется в виде  $g = g_1 g_2 \cdots g_k$ , где  $g_i$  удовлетворяют следующим условиям:

1.  $g_i g_j = g_j g_i$ ;
2.  $\text{ord}(g_i) = n_i$ ;
3.  $g_i = g^{t_i}$ .

### Доказательство.

Доказательство будем вести индукцией по  $k$ .

Пусть  $k = 2$ . Тогда, согласно условию леммы, имеем:  $\text{ord}(g) = mn$ ,  $\text{НОД}(m, n) = 1$ . Из  $\text{НОД}(m, n) = 1$  следует, что при некоторых  $u, v \in \mathbb{Z}$  выполняется соотношение  $um + vn = 1$ .

## Глава 12. Строение конечных групп

Положим  $g_1 = g^{vn}$ ,  $g_2 = g^{mu}$ . Очевидно, что  $g_1g_2 = g_2g_1 = g$ .  
Укажем, что  $\text{ord}(g_1) = m$ ,  $\text{ord}(g_2) = n$ . Из определения  $g_1$  и  
 $g_2$  следует, что

$$g_1^m = (g^{vn})^m = (g^{mn})^v = e, \quad g_2^n = (g^{mu})^n = (g^{mn})^u = e.$$

Поэтому  $m_1 = \text{ord}(g_1) \mid m$  и  $n_1 = \text{ord}(g_2) \mid n$ . С другой стороны, поскольку  $g = g_1g_2 = g_2g_1$ , то  $g^{m_1n_1} = e$ , следовательно,  $\text{ord}(g) = mn \mid m_1n_1$ . Отсюда, учитывая, что  $\text{НОД}(m, n_1) = \text{НОД}(n, m_1) = 1$ , получим  $m \mid m_1$  и  $n \mid n_1$ . Таким образом,  $\text{ord}(g_1) = m$ ,  $\text{ord}(g_2) = n$  и  $g = g_1g_2$ .

Покажем, что компоненты  $g_1$  и  $g_2$  определены однозначно.  
Допустим, что

$$\begin{aligned} g = g_1g_2 &= h_1h_2, & \text{ord}(g_1) &= \text{ord}(h_1) = m, \\ \text{ord}(g_2) &= \text{ord}(h_2) = n \end{aligned} \tag{12.8}$$

Напомним, что  $g_1g_2 = g_2g_1$ ,  $h_1h_2 = h_2h_1$ , причём  $g_1$  и  $g_2$  — некоторые степени элемента  $g$ . Из (12.8) следует:

$$\begin{aligned} h_1g &= h_1(h_2h_1) = (h_1h_2)h_1 = gh_1, \\ h_2g &= h_2(h_1h_2) = (h_2h_1)h_2 = gh_2. \end{aligned}$$

Поэтому  $g_1h_1 = h_1g_1$  и  $g_2h_2 = h_2g_2$ .

Из соотношения (12.8) вытекает, что

$$w = g_1^{-1}h_1 = g_2h_2^{-1} \tag{12.9}$$

Покажем, что  $w = e$ . Пусть  $s$  — порядок элемента  $w$ . Из (12.9) имеем:

$$\begin{aligned} w^m &= (g_1^{-1}h_1)^m = (g_1^{-1})^mh_1^m = e, \\ w^n &= (g_2h_2^{-1})^n = g_2^n(h_2^{-1})^n = e. \end{aligned}$$

Поэтому  $s \mid m$  и  $s \mid n$ . Так как  $\text{НОД}(m, n) = 1$ , то  $s = 1$ , и  $w = e$ . Следовательно, из (12.9) получим  $g_1 = h_1$ ,  $g_2 = h_2$ . База индукции доказана.

Допустим, что справедливость леммы доказана при  $k \geq 2$ , и пусть  $\text{ord}(g) = n_1 n_2 \cdots n_k n_{k+1}$ ,  $\text{НОД}(n_i, n_j) = 1$  при  $i \neq j$ . Положим  $n_1 n_2 \cdots n_k = m$ ,  $n_{k+1} = n$ . Очевидно, что  $m$  и  $n$  удовлетворяют условиям базы индукции. Следовательно, справедливы соотношения

$$g = ab, ab = ba, \text{ord}(a) = m, \text{ord}(b) = n_{k+1}, a = g^s, b = g^{t_{k+1}}.$$

По предположению индукции, для элемента  $a$  справедливо утверждение леммы, поэтому

$$a = g_1 g_2 \cdots g_k, \text{ord}(g_i) = n_i, g_i g_j = g_j g_i, g_i = a^{n_i} = g^{t_i}, i = \overline{1, k}.$$

Следовательно,

$$\begin{aligned} g = ab &= g_1 \cdots g_k g_{k+1}, g_i = g^{t_i}, g_i g_j = g_j g_i, g_{k+1} = b, \\ \text{ord}(g_i) &= n_i, i = \overline{1, k+1}. \end{aligned}$$

Тем самым лемма полностью доказана.  $\square$

### Теорема 12.2.

Пусть  $G$  — абелева группа и  $|G| = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$  — каноническое разложение числа  $|G|$  в произведение простых сомножителей. Тогда

$$G = S_1 \times S_2 \times \cdots \times S_k,$$

где  $|S_i| = p_i^{t_i}$ ,  $i = \overline{1, k}$ . Подгруппа  $S_i$  называется сильвской  $p_i$ -подгруппой группы  $G$ .

### Доказательство.

Рассмотрим  $S_i = \{g \in G : \text{ord}(g) = p_i^k, k = \overline{1, t_i}\}$ . Очевидно, что  $S_i < G$ ,  $S_i \cap S_j = \langle e \rangle$  при  $i \neq j$ . С другой стороны,  $\text{ord}(g) | |G| = p_1^{t_1} \cdots p_k^{t_k}$  для любого  $g \in G$  и, следовательно,  $\text{ord}(g) = p_1^{s_1} \cdots p_k^{s_k}$ ,  $0 \leq s_i \leq t_i$ ,  $i = \overline{1, k}$ . Согласно лемме 12.1, элемент  $g$  однозначно представляется в виде  $g = g_1 g_2 \cdots g_k$ , где  $\text{ord}(g_i) = p_i^{s_i}$ , и поэтому  $g_i \in S_i$ . Таким образом,  $G \subset \prod_{i=1}^k S_i$  и,

следовательно,  $G = \prod_{i=1}^k S_i$ .

Покажем, что  $|S_i| = p_i^{t_i}$ . В самом деле, по Теореме 12.1, каждая  $S_i \neq \langle e \rangle$  является прямым произведением циклических подгрупп порядков  $p_i^{s_{i1}}, \dots, p_i^{s_{ir}}$ . Отсюда следует, что

$$|S_i| = p_i^{s_{i1} + \dots + s_{ir}} = p_i^{u_i}.$$

Но  $|G| = \prod |S_i| = \prod_{i=1}^k p_i^{u_i} = \prod_{i=1}^k p_i^{t_i}$ , следовательно,  $u_i = t_i$  и  $|S_i| = p_i^{t_i}$ .  $\square$

**Следствие 12.1.** Если  $p \mid n$ , то абелева группа порядка  $n$  содержит элемент порядка  $p$ .

**Теорема 12.3.**

Если конечная абелева группа  $G$  порядка  $p^n$  разложена двумя способами в прямое произведение своих циклических подгрупп:

$$G = A_1 \times A_2 \times \dots \times A_r = B_1 \times B_2 \times \dots \times B_s,$$

то  $r = s$  и  $|A_i| = |B_i|$  при некотором упорядочении групп  $B_1, \dots, B_s$ .

*Доказательство.*

Будем доказывать её индукцией по  $n$ . При  $n = 1$  теорема справедлива.

Пусть теорема верна для всех групп порядка меньше  $p^n$ ,  $n \geq 1$ . Упорядочим группы в порядке убывания их порядков, то есть будем считать, что  $|A_i| = p^{m_i}$ ,  $|B_j| = p^{n_j}$  и

$$\begin{aligned} m_1 &\geq m_2 \geq \dots \geq m_q > m_{q+1} = \dots = m_r = 1, \\ n_1 &\geq n_2 \geq \dots \geq n_t > n_{t+1} = \dots = n_s = 1. \end{aligned} \tag{12.10}$$

Далее рассмотрим множество  $G^p = \{g^p : g \in G\}$ . Очевидно, что  $G^p < G$  и  $|G^p| < |G|$ . С другой стороны, по условию теоремы, произвольный элемент  $g \in G$  может быть представлен в виде

$$g = a_1^{i_1} \cdots a_q^{i_q} a_{q+1}^{i_{q+1}} \cdots a_r^{i_r} = b_1^{j_1} \cdots b_t^{j_t} b_{t+1}^{j_{t+1}} \cdots b_s^{j_s}.$$

С учётом (10) отсюда получаем:

$$g^p = (a_1^p)^{i_1} \cdots (a_q^p)^{i_q} = (b_1^p)^{j_1} \cdots (b_{j_t}^p)^{j_t}.$$

Следовательно,  $A^p = \langle a_1^p \rangle \times \cdots \times \langle a_q^p \rangle = \langle b_1^p \rangle \times \cdots \times \langle b_{j_t}^p \rangle$ ,  
 $\text{ord}(a_i^p) = p^{m_i-1}$ ,  $\text{ord}(b_j^p) = p^{m_j-1}$ .

Так как  $|G^p| < |G|$ , то из индуктивного предположения следует, что  $q = t$ ,  $m_i - 1 = n_i - 1$  ( $i = \overline{1, t}$ ).

Поскольку  $|A_{q+1} \times \cdots \times A_r| = p^{n-q}$ ,  $|B_{t+1} \times \cdots \times B_s| = p^{s-t}$ ,  
и  $|G| = p^{m_1+\cdots+m_q} p^{r-q} = p^{m_1+\cdots+m_q} p^{s-q}$ , то  $s = r$ .

Теорема полностью доказана.  $\square$

Из теорем (12.1) и (12.3) вытекает

**Теорема 12.4** (Основная теорема). *Всякая конечная абелева группа является прямым произведением своих примарных циклических подгрупп. Любые два таких разложения имеют одно и то же число множителей каждого порядка.*

**Упражнение 12.1.** Доказать, что  $\mathbb{Z}_{p \cdot q}^* = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ .

**Упражнение 12.2.** Описать строение групп  $\mathbb{Z}_{15}^*$ ,  $\mathbb{Z}_{21}^*$ ,  $\mathbb{Z}_{54}^*$ ,  $\mathbb{Z}_{72}^*$ .

## 12.2 Сопряжённые классы и элементы. Теорема Коши

Пусть  $G$  — конечная группа,  $H < G$ ,  $S \subset G$ ,  $S \neq \emptyset$ .

**Определение 12.1.** Множества  $S$  и  $S_1$  называются *сопряжёнными* по подгруппе  $H$ , если для некоторого  $x \in H$  выполняется условие  $S_1 = x^{-1}Sx = S^x$ .

Очевидно, что отношение сопряжённости множеств является отношением эквивалентности.

**Определение 12.2.** Нормализатором множества  $S$  по подгруппе  $H$  называется множество  $N_H(S) = \{x \in H : S^x = S\}$ .

Очевидно, что  $N_H < H$ , и если  $N_G(H) = H$ , то  $H$  — нормальный делитель группы  $G$ , то есть для любого  $g \in G$

$$g^{-1}Hg = H.$$

**Определение 12.3.** Централизатором множества  $S$  в подгруппе  $H$  называется множество  $Z_H(S) = \{x \in H : xs = sx \forall s \in S\}$ .

В частности,  $Z_G(G) = Z(G)$  — центр группы — множество всех элементов из группы  $G$ , перестановочных с каждым элементом данной группы  $G$ .

Легко убедиться, что  $Z(G) \triangleleft G$ .

**Определение 12.4.** Класс элементов, сопряжённых с данным элементом  $g$  группы  $G$ , есть множество

$$C(g) = \{g^x = x^{-1}gx : x \in G\}.$$

**Теорема 12.5.**

Число множеств в группе  $G$ , сопряжённых с данным множеством  $S$  по подгруппе  $H$ , равно индексу нормализатора множества  $S$  в  $H$ , то есть  $[H : N_H(S)]$ .

*Доказательство.*

Пусть  $N_H(S) = D$  и  $H = D + Dx_2 + \cdots + Dx_r$ . Наша задача подсчитать число различных элементов в множестве  $A = \{S^x : x \in H\}$ . Пусть  $S^x = S^y$ ,  $x, y \in H$ . Это значит, что  $x^{-1}Sx = y^{-1}Sy$  или  $yx^{-1}Sxy^{-1} = S$ . Следовательно,  $yx^{-1} \in D$ , а значит  $y \in Dx$ , то есть  $x$  и  $y$  принадлежат одному смежному классу группы  $H$  по подгруппе  $D$ .

С другой стороны, пусть  $x$  и  $y$  принадлежат одному смежному классу  $Dz$ . Следовательно,  $x = d_1z$ ,  $y = d_2z$ ,  $d_1, d_2 \in D$ . Отсюда имеем:

$$S^x = x^{-1}Sx = z^{-1}(d_1^{-1}Sd_1)z = z^{-1}Sz = S^z,$$

$$S^y = y^{-1}Sy = z^{-1}(d_2^{-1}Sd_2)z = z^{-1}Sz = S^z,$$

то есть  $S^x = S^y$ .

Таким образом, число различных элементов в множестве  $A$  совпадает с числом смежных классов в группе  $H$  по подгруппе  $D$ , то есть равно  $[H : D] = [H : N_H(S)]$ . Теорема полностью доказана.  $\square$

**Следствие 12.2.**

Любая конечная группа разбивается на непересекающиеся классы сопряжённых элементов, причём мощность каждого класса является делителем порядка группы.

**Доказательство.**

Свойство сопряжённости элементов является отношением эквивалентности на группе  $G$  и поэтому справедлива первая часть утверждения. Справедливость второй части следует из Теоремы 12.5, как частный случай — множество  $S$  состоит из одного элемента. Таким образом,

$$G = C_1(e) + C_2(g_2) + \cdots + C_t(g_t), \quad (12.11)$$

где  $C_i(g_i) = \{g_i^x : x \in G\}$ ,  $i = \overline{1, t}$  и  $C_1(e) = \{e\}$ ,  $C_i$  попарно не пересекаются, то есть

$$C_i \cap C_j = \emptyset \quad (i \neq j),$$

и их мощность равна

$$|C_i| = [G : N_G(g_i)] / |G|.$$

□

**Теорема 12.6.**

Если порядок группы есть степень простого числа, то центр этой группы отличен от единицы.

**Доказательство.**

Из условия теоремы и разбиения (12.11) группы  $G$  на непересекающиеся классы сопряжённых элементов следует:

$$|G| = 1 + |C_2| + \cdots + |C_t| = p^k, k \geq 1, \quad (12.12)$$

где  $|C_i| \mid p^k$  и, следовательно,  $|C_i| = p^{s_i}$ ,  $s_i \geq 0$ . Соотношение (2) позволяет сделать вывод, что, во-первых, некоторые  $|C_i|$  в (2) при  $i \geq 2$  должны обязательно равняться 1 и количество таких слагаемых должно быть кратно  $p$ . Но, если  $|C_i(g_i)| = 1$ ,

то  $C_i(g_i) = \{g^x : x \in G\} = \{g_i\}$ ,  $i \geq 2$ . Это означает, что для любых  $x \in G$ ,  $g_i x = x g_i$ . Поэтому  $g_i \in Z_G$ ,  $g_i \neq e$ ,  $i \geq 2$  и  $|Z_G| > 1$ .  $\square$

**Теорема 12.7** (Коши).

Если простое число  $p$  является делителем порядка группы  $G$ , то в  $G$  существует элемент порядка  $p$ .

**Доказательство.**

Пусть  $|G| = ps$ ,  $s \geq 1$ . Доказательство будем вести индукцией по порядку группы. Если  $s = 1$ , то теорема верна, поскольку в этом случае  $G$  — циклическая группа, порядка  $p$ .

Допустим, что мы доказали справедливость теоремы для всех групп, порядок которых меньше  $|G|$ , и будем доказывать её справедливость для группы  $G$ . Возможны два случая:

I. Существует  $H < G$  такая, что  $p \nmid [G : H]$ ,  $H \neq G$ ,  $H \neq \langle e \rangle$ . По теореме Лагранжа  $|G| = |H| \cdot [G : H]$ . Поэтому  $p \mid |H|$  и  $|H| < |G|$ . Из индуктивного предположения следует, что существует  $h \in H$  такое, что  $ord(h) = p$ . Поскольку  $h$ , естественно, является элементом группы  $G$ , то тем самым устанавливается справедливость теоремы.

II. Для любой собственной подгруппы  $H$  группы  $G$  выполняется условие

$$p \mid [G : H]. \quad (12.13)$$

Разобьём группу  $G$  на непересекающиеся классы сопряжённых элементов:  $G = C_1(e) + C_2(g_2) + \cdots + C_t(g_t)$ . Напомним, что  $C_1(e) = \{e\}$ ,  $C_i(g_i) = \{g_i^x : x \in G\}$ ,  $|C_i| \mid |G|$ ,  $i = \overline{1, t}$ . Следовательно,

$$ps = |G| = 1 + |C_2| + \cdots + |C_t| \quad (12.14)$$

и  $|C_i| = [G : N_G(g_i)]$ ,  $N_G(g_i) < G$ . Отсюда и условия (12.13) следуют, что если  $|C_i| \neq 1$ , то  $p \mid |C_i|$ . Поэтому число слагаемых  $|C_i|$  в (12.14), равных 1, должно быть кратно  $p$ . Но если  $|C_i| = 1$ , то соответствующий элемент  $g_i$  принадлежит центру

группы  $G$ . Таким образом мы установили, что центр  $Z(G)$  группы  $G$  имеет порядок, кратный простому числу  $p$ . Но  $Z(G)$  — абелева группа, следовательно существует элемент  $a \in Z(G)$  такой, что  $\text{ord}(a) = p$ . Теорема Коши полностью доказана.  $\square$

## 12.3 Двойные классы смежности. Теоремы Силова

*Определение 12.5.* Пусть  $H < G$ ,  $K < G$ ,  $x \in G$ . Множество  $HxK = \{hxk : k \in K, h \in H\}$  называется *двойным смежным классом*.

Нетрудно доказать, что два двойных смежных класса либо совпадают, либо не пересекаются. Любой элемент  $x \in HxK$ , поэтому группу  $G$  можно представить в виде объединения непересекающихся двойных смежных классов:

$$G = Hx_1K + Hx_2K + \cdots + Hx_mK, x_1 = e. \quad (12.15)$$

Разложение (12.15) обычно называют *разложением группы по двойному модулю*  $(H, K)$ .

Очевидно, что  $HxK \supset Hxk$  и  $HxK \supset hxK$  для любых  $k \in K$  и  $h \in H$ . Следовательно, двойной смежный класс является объединением некоторого числа левых смежных классов группы  $G$  по подгруппе  $H$  и объединением некоторого числа правых смежных классов группы  $G$  по подгруппе  $K$ .

**Лемма 12.2.**

Если

$$HxK = Ha_1 + \cdots + Ha_s = b_1K + \cdots + b_mK - \quad (12.16)$$

разложение двойного смежного класса на соответствующие левые и правые смежные классы и  $x^{-1}Hx \cap K = D$ , то  $s = [K : D]$ ,  $m = [x^{-1}Hx : D]$ .

*Доказательство.*

Разложим группу  $A = x^{-1}Hx$  на правые смежные классы по подгруппе  $D$ :

$$A = D + c_2D + \cdots + c_tD, [A : D] = r. \quad (12.17)$$

Покажем, что

$$AK = K + c_2K + \cdots + c_rK = C. \quad (12.18)$$

В самом деле, если  $g \in AK$ , то  $g = ak$ , где  $a \in A$ ,  $k \in K$ . Но из (12.17) следует, что  $a = c_id$ , следовательно,  $g = c_idk = c_ik' \in C$ . С другой стороны, если  $g \in c_iK$ , где  $c_i \in A$ , то, естественно, что  $g \in AK$ . И наконец, установим, что  $c_iK \cap c_jK = \emptyset$  при  $i \neq j$ . Пусть  $g = c_ik_1 = c_jk_2$ . Отсюда следует, что  $c_i^{-1}c_j = k_1k_2^{-1} \in A \cap K = D$ , то есть  $c_j \in c_iD$ . Согласно (12.17) это означает, что  $i = j$ .

Далее заметим, что поскольку  $xG = G$  для любого  $x \in G$ , то из (12.18) получим:  $xAK = HxK = xK + x_2c_2K + \cdots + x_rK$ . Сравнивая полученное разложение с разложением (12.16), получим  $r = [x^{-1}Hx : D] = m$ .

Аналогично доказывается, что  $[K : D] = s$ . Разложим  $K$  на левые смежные классы по подгруппе  $D$ :

$$K = D + Du_2 + \cdots + Du_t, [K : D] = t.$$

Далее заметим, что поскольку  $D < A$ , то

$$AK = A + Au_2 + \cdots + Au_t,$$

то есть

$$x^{-1}HxK = x^{-1}Hx + xHxu_2 + \cdots + x^{-1}Hxu_t. \quad (12.19)$$

Умножив обе части (12.19) на  $x$ , получим:

$$HxK = Hx + Hxu_2 + \cdots + Hxu_t.$$

Откуда следует, что  $t = s$ . Лемма полностью доказана. □

**Лемма 12.3.**

Пусть  $T \triangleleft G$ ,  $\mathfrak{A} = \{K: T \triangleleft K < G\}$  и  $\overline{\mathfrak{A}} = \{\overline{K} < G/T = \overline{G}\}$ .  
Тогда

1. Отображение  $\varepsilon: \mathfrak{A} \rightarrow \overline{\mathfrak{A}}$ , определённое правилом

$$\varepsilon(K) = \overline{K} = K/T,$$

является биекцией.

2.  $K \triangleleft G$  тогда и только тогда, когда  $\overline{K} \triangleleft \overline{G}$ .

3.  $[G : K] = [G/T : K/T]$ .

*Доказательство.*

1. Пусть  $K_1, K_2 \in \mathfrak{A}$  и  $K_1 \neq K_2$ . Рассмотрим разложение  $K_1$  и  $K_2$  на смежные классы по нетривиальному нормальному делителю  $T$ :

$$K_1 = T + u_2T + \cdots + u_rT, \quad K_2 = T + v_2T + \cdots + v_sT.$$

Так как  $K_1 \neq K_2$ , то  $u_iT \neq v_jT$  для некоторых  $i$  и  $j$ . Отсюда следует, что

$$\overline{K}_1 = K_1/T = \{\overline{e}, \overline{u_2}, \dots, \overline{u_r}\} \neq \overline{K}_2 = K_2/T = \{\overline{e}, \overline{v_2}, \dots, \overline{v_s}\}.$$

Таким образом, отображение  $\varepsilon$  инъективно.

С другой стороны, это отображение сюръективно, поскольку если

$$\overline{K} = \{T, u_2T, \dots, u_rT\},$$

то  $K = T + u_2T + \cdots + u_rT < G$  и  $\varepsilon(K) = \overline{K}$ .

2. Пусть  $T \triangleleft K \triangleleft G$  и

$$\overline{K} = K/T = \{T, u_2T, \dots, u_rT\} = \{\overline{e}, \overline{u_2}, \dots, \overline{u_r}\},$$

$\overline{G} = \{\overline{e}, \overline{g_2}, \dots, \overline{g_s}\} = G/T$ . Если  $\overline{g} = gT$  — произвольный элемент из  $G/T$ ,  $\overline{u} = uT$  — произвольный элемент из  $K/T$ , то

$\bar{g}^{-1}\bar{u}\bar{g} = (g^{-1}T)(uT)(gT) = (g^{-1}ug)T = u'T \in \bar{K}$ . Следовательно,  $\bar{K} \triangleleft \bar{G}$ .

Пусть теперь  $\bar{K} = K/T \triangleleft G/T = \bar{G}$ . Согласно определению нормального делителя это означает, что  $\bar{g}^{-1}\bar{u}\bar{g} \in \bar{K}$  для любых  $\bar{g} \in \bar{G}$  и  $\bar{u} \in \bar{K}$ . Отсюда получаем, что существуют такие  $t_1, t_2, t_3, t_4 \in T$ , что справедливо соотношение:  $g^{-1}t_1ut_2gt_3 = u_1t_4$ ,  $g \in G$ ,  $u, u_1 \in K$ . Поскольку  $T \triangleleft K$ , то  $t_1u = ut'_1$  для некоторого  $t'_1 \in T$ . Следовательно,  $g^{-1}ut'_1t_2gt_3 = u_1t_4$ , то есть  $g^{-1}ut''gt_3 = u_1t_4$ . Так как  $T \triangleleft G$ , то  $t''g = g\tilde{t}$  для некоторого  $\tilde{t} \in G$ . Таким образом  $g^{-1}ug\tilde{t}t_3 = u_1t_4$ . Из последнего соотношения следует, что  $g^{-1}ug = u_1t \in K$ . Так как  $g$  и  $u$  были соответственно произвольные элементы из  $G$  и  $K$ , то тем самым мы установили, что  $K \triangleleft G$ . Вторая часть леммы полностью доказана.

3. Справедливость третьей части, учитывая конечность группы, немедленно следует из теоремы Лагранжа.  $\square$

**Теорема 12.8** (Первая теорема Силова).

Пусть  $|G| = p^m s$ ,  $(s, p) = 1$ ,  $p$  — простое. 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  $p^{i+1}$ .

*Доказательство.*

Доказательство будем вести индукцией по  $i$ . Если  $i = 1$ , то согласно теореме Коши в  $G$  существует подгруппа порядка  $p$ .

Пусть  $\mathcal{P} < G$ ,  $|\mathcal{P}| = p^i$ ,  $m > i \geq 1$ . Разложим группу  $G$  по двойному модулю:  $G = \mathcal{P} + \mathcal{P}x_2\mathcal{P} + \cdots + \mathcal{P}x_s\mathcal{P}$ ,  $x_1 = e$ . Пусть  $b_k$  — число правых смежных классов по  $\mathcal{P}$  в двойном смежном классе  $\mathcal{P}x_k\mathcal{P}$ . Тогда  $\sum_{k=1}^s b_k = [G : \mathcal{P}]$ . Согласно Лемме 12.2  $b_k = [x_k^{-1}\mathcal{P}x_k : x_k^{-1}\mathcal{P}x_k \cap \mathcal{P}] = p^{t_k}$ ,  $t_k \geq 0$ . Так как  $b_1 = 1$ , то число  $b_k$ , равных 1, должно быть кратно  $p$ . Далее рассмотрим  $N = N_G(\mathcal{P}) = \{g \in G : g^{-1}\mathcal{P}g = \mathcal{P}\}$ ,  $\mathcal{P} \triangleleft N$ . Заметим, что если  $b_k = 1$ , то  $x_k \in N$  и весь смежный класс

$x_k \mathcal{P} = \mathcal{P} x_k \subset N$ . И наоборот, если  $x_k \in N$ , то  $b_k = 1$ . Следовательно, число  $b_k$ , равных 1, равно числу смежных классов группы  $N$  по  $\mathcal{P}$ , то есть  $[N : \mathcal{P}]$ . Так как  $\mathcal{P} \triangleleft N$ , то можно построить фактор-группу  $\bar{N} = N/\mathcal{P}$ . Из изложенного выше следует, что  $|N/\mathcal{P}| = [N : \mathcal{P}] = pt$ . По теореме Коши в  $N/\mathcal{P}$  существует подгруппа  $\bar{H}$  порядка  $p$ . Так как  $\langle \bar{e} \rangle \triangleleft \bar{H} < \bar{N}$  и по Лемме 12.3  $\bar{H} = H/\mathcal{P}$  и  $\mathcal{P} \triangleleft H$ , где  $\bar{e} = \mathcal{P}$ , то  $H < N$  и  $|H| = p \cdot |\mathcal{P}| = p^{i+1}$ . Тем самым теорема доказана.  $\square$

**Определение 12.6.** Максимальная группа порядка  $p^m$  группы  $G$  ( $G = p^m \cdot s$ ,  $(p, s) = 1$ ) называется *силовской  $p$ -подгруппой*.

**Теорема 12.9** (Вторая теорема Силова).

*Все силовские  $p$ -подгруппы конечной группы сопряжены.*

**Доказательство.**

Пусть  $\mathcal{P}_1$  и  $\mathcal{P}_2$  — две силовские подгруппы группы  $G$ . Разложим  $G$  по двойному модулю  $(\mathcal{P}_1, \mathcal{P}_2)$ :

$$G = \mathcal{P}_1 \mathcal{P}_2 + \mathcal{P}_1 x_2 \mathcal{P}_2 + \cdots + \mathcal{P}_1 x_s \mathcal{P}_2.$$

Так как  $|G| = p^t s$ ,  $(s, p) = 1$  и  $|\mathcal{P}_1| = p^s$ , то  $p \nmid [G : \mathcal{P}_i]$ . С другой стороны, по Лемме 12.2  $[G : \mathcal{P}_i] = \sum_{i=1}^s b_i$ , где

$$b_i = [x_i^{-1} \mathcal{P}_1 x_i : (x_i^{-1} \mathcal{P}_1 x_i) \cap \mathcal{P}_2] = p^{r_i}, \quad r_i \geq 0.$$

Следовательно, среди  $b_i$  хотя бы одно должно быть равно 1. Отсюда следует, что  $\mathcal{P}_2 = x_i^{-1} \mathcal{P}_1 x_i$ , то есть  $\mathcal{P}_1$  и  $\mathcal{P}_2$  сопряжены в  $G$ .  $\square$

**Теорема 12.10** (Третья теорема Силова).

*Число силовских  $p$ -подгрупп конечной группы делит порядок группы и сравнимо с единицей по модулю  $p$ .*

*Доказательство.*

Пусть  $\mathcal{P}_0$  — одна из силовских  $p$ -подгрупп,  $\mathcal{P}_1, \dots, \mathcal{P}_r$  — остальные. Рассмотрим множество

$$\{x^{-1}\mathcal{P}_i x : x \in \mathcal{P}_0, i = \overline{1, r}\} = M_1 + \cdots + M_t, t \leq r, \sum_{i=1}^t |M_i| = r,$$

$M_i$  — классы сопряжённых относительно  $\mathcal{P}_0$  групп  $\mathcal{P}_i$ . Рассмотрим  $N_i = N_G(\mathcal{P}_i) = \{g \in G : g^{-1}\mathcal{P}_i g = \mathcal{P}_i\}$ . Очевидно, что  $\mathcal{P}_i < N_i$ , но  $\mathcal{P}_j \not< N_i$  при  $i \neq j$ ,  $i = \overline{0, r}$ . Справедливость последнего утверждения следует из теоремы 12.9. Поэтому  $N_{\mathcal{P}_0}(\mathcal{P}_i) = N_i \cap \mathcal{P}_0 < \mathcal{P}_0$  и  $N_{\mathcal{P}_0}(\mathcal{P}_i) \neq \mathcal{P}_0$ . Поэтому, число групп, сопряжённых с  $\mathcal{P}_i$  относительно  $\mathcal{P}_0$ , равно  $|M_i| = [\mathcal{P}_0 : N_{\mathcal{P}_0}(\mathcal{P}_i)] = p^{t_i}$ ,  $t_i \geq 1$ . Следовательно,  $r = \sum_{i=1}^t p^{t_i}$ , а число силовских подгрупп равно  $1 + r \equiv 1 \pmod{p}$ .  $\square$

**Упражнение 12.3.** Найти все силовские подгруппы группы  $A_5$ .

**Упражнение 12.4.** Доказать, что если  $|G| = p^2q$ ,  $q > p > 2$  ( $p$  и  $q$  — простые), то  $G$  содержит нетривиальную нормальную подгруппу.

## Глава 13

# Конечные группы подстановок

### 13.1 Орбиты, стабилизаторы и их свойства. Лемма Бернсайда

Пусть  $\Omega = \{a_1, \dots, a_n\}$  и  $S^\Omega = \left\{ \begin{pmatrix} a_1 & \dots & a_n \\ a_{i_1} & \dots & a_{i_n} \end{pmatrix} \right\}$  — симметрическая группа всех подстановок на множестве  $\Omega$ . В дальнейшем, как правило, будем считать, что  $\Omega = \{1, 2, \dots, n\}$  и  $S^\Omega = S_n$ . Если  $\alpha \in \Omega$  и подстановка  $g \in G < S_n$  отображает  $\alpha$  в  $\beta$ , то будем записывать этот факт следующим образом:  $\beta = \alpha^g$ . В дальнейшем будем рассматривать только группы  $G < S^\Omega$ .

*Определение 13.1.* Множество  $\Delta \subset \Omega$  называется *инвариантным* относительно группы  $G$ , если  $\Delta = \Delta^G = \{\alpha^g : \alpha \in \Delta, g \in G\}$ .

Очевидно, что  $\emptyset$  и  $\Omega$  являются инвариантами для любой группы  $G < S_n$ .

**Пример 13.1.** Пусть  $n = 4$ . Рассмотрим группу

$$G = \{e, (12), (34), (12)(34)\}.$$

Эта группа имеет четыре инвариантных множества:  $\Delta_1 = \emptyset$ ,  $\Delta_2 = \Omega = \{1, 2, 3, 4\}$ ,  $\Delta_3 = \{1, 2\}$ ,  $\Delta_4 = \{3, 4\}$ .

**Определение 13.2.** Минимальное инвариантное множество  $\Delta \neq \emptyset$  группы  $G$  называется *орбитой* или *множеством транзитивности*.

Следует заметить, из определения орбиты следует, что любые две различные орбиты не пересекаются, их объединение есть множество  $\Omega$  и любая орбита  $\Delta$  может быть записана в виде  $\Delta = \alpha^G$ , где  $\alpha$  — произвольный элемент орбиты  $\Delta$ .

**Пример 13.2.** Группа  $G$  из предыдущего примера имеет две орбиты  $\Delta_3$  и  $\Delta_4$ .

**Пример 13.3.** Рассмотрим группу Клейна

$$\mathcal{K} = \{e, (12)(34), (13)(24), (14)(23)\} = \{e, g_2, g_3, g_4\}.$$

Для этой группы минимальное инвариантное множество совпадает с  $\Omega = \{1^g : g \in \mathcal{K}\} = \{1^e, 1^{g_2}, 1^{g_3}, 1^{g_4}\} = \{1, 2, 3, 4\}$ .

**Определение 13.3.** Группа  $G < S^\Omega$  называется *транзитивной*, если она имеет единственную орбиту, совпадающую с множеством  $\Omega$ .

**Упражнение 13.1.** Доказать, что если  $\Delta$  — орбита группы  $G < S_n$ , то  $\Delta^t$  — орбита группы  $t^{-1}Gt$ , где  $t \in S_n$ .

**Определение 13.4.** Пусть  $\Delta \subset \Omega$  и  $G_\Delta = \{g \in G : \alpha^g = \alpha, \forall \alpha \in \Delta\}$ . Очевидно, что  $G_\Delta \subset G$ . Если  $\Delta = \{\alpha\}$ , то группу  $G_\alpha$  называют *стабилизатором* элемента  $\alpha$ .

**Пример 13.4.**

$$G = A_4 = \{e, (123), (124), (134), (234), (132), (142), \\ (143), (243), (12)(34), (13)(24), (14)(23)\}$$

$$G_1 = \{e, (234), (243)\}$$

$$G_2 = \{e, (143), (134)\}$$

$$G_3 = \{e, (124), (142)\}$$

$$G_4 = \{e, (123), (132)\}$$

Для группы Клейна  $G_1 = G_2 = G_3 = G_4 = \langle e \rangle$ .

**Упражнение 13.2.** Доказать, что если  $\alpha^G = \beta^G$ , то группы  $G_\alpha$  и  $G_\beta$  сопряжены в  $G$ .

**Теорема 13.1.**

Порядок группы равен произведению порядка стабилизатора на длину соответствующей орбиты, то есть

$$|G| = |G_\alpha| \cdot |\alpha^G| \text{ для } \forall \alpha \in \Omega. \quad (13.1)$$

*Доказательство.*

Подсчитаем мощность орбиты  $\Delta(\alpha) = \alpha^G = \{\alpha^g : g \in G\}$ . Для этого заметим, что  $\alpha^g = \alpha^h$  тогда и только тогда, когда  $\alpha^{gh^{-1}} = \alpha$ . Это означает, что  $gh^{-1} \in G_\alpha$  или  $g \in G_\alpha h$ . Таким образом, число элементов в орбите  $\alpha^G$  равно числу различных смежных классов группы  $G$  по  $G_\alpha$ , то есть равно  $[G : G_\alpha]$ . Отсюда и из теоремы Лагранжа следует справедливость равенства (13.1)  $\square$

**Следствие 13.1.**

Для любых  $\alpha, \beta \in \Omega$  ( $\alpha \neq \beta$ ) справедливо равенство

$$[G : G_{\alpha\beta}] = |\alpha^G| \cdot |\beta^{G_\alpha}| = |\beta^G| \cdot |\alpha^{G_\beta}| \quad (13.2)$$

*Доказательство.*

Поскольку  $G_{\alpha\beta} < G_\alpha < G$ , то

$$[G : G_\alpha] = [G : G_\alpha] \cdot [G_\alpha : (G_\alpha)_\beta] = [G : G_\beta] \cdot [G_\beta : (G_\beta)_\alpha].$$

Отсюда и из формулы (13.1) следует справедливость формулы (13.2)  $\square$

**Теорема 13.2.**

Если  $P$  — силовская  $p$ -подгруппа группы  $G$  и  $p^k$  делит длину орбиты  $\alpha^G$ , то  $p^k$  делит длину орбиты  $\alpha^P$  группы  $P$ .

*Доказательство.*

Из определения силовской  $p$ -подгруппы следует, что

$$|P| = p^m \text{ и } ([G : P], p) = 1.$$

Далее заметим, что

$$\mathcal{P}_\alpha < G_\alpha < G, \quad \mathcal{P}_\alpha < \mathcal{P} < G.$$

Отсюда и из теоремы Лагранжа получим:

$$[G : \mathcal{P}_\alpha] = [G : G_\alpha] \cdot [G_\alpha : \mathcal{P}_\alpha] = [G : \mathcal{P}] \cdot [\mathcal{P} : \mathcal{P}_\alpha].$$

С учётом (13.1) из этих соотношений следует

$$|\alpha^G| \cdot [G_\alpha : \mathcal{P}_\alpha] = [G : \mathcal{P}] \cdot |\alpha^\mathcal{P}| \quad (13.3)$$

Поскольку  $([G : \mathcal{P}], p) = 1$  и по условию теоремы  $|\alpha^G| = p^k w$ , то из (13.3) вытекает, что  $p^k \mid |\alpha^\mathcal{P}|$ . Теорема доказана.  $\square$

### Теорема 13.3.

Если  $p^m$  – наибольшая степень простого числа  $p$ , делящая  $|\alpha^G|$ , то любая орбита группы  $\mathcal{P}$  наименьшей мощности, лежащая в орбите  $\alpha^G$ , имеет мощность  $p^m$ .

*Доказательство.*

Из (13.1) следует, что любая орбита  $\Delta_i$  группы  $\mathcal{P}$  имеет мощность, равную некоторой степени числа  $p$  ( $|\alpha^\mathcal{P}| = [\mathcal{P} : \mathcal{P}_\alpha]$ ), то есть  $|\Delta_i| = p^{r_i}$ , из теоремы 13.1 следует, что  $r_i \geq m$ . С другой стороны, так как  $\mathcal{P} < G$ , то орбита  $\alpha^G$  есть объединение некоторого числа орбит группы  $\mathcal{P}$ , следовательно,

$$|\alpha^G| = |\Delta_1| + \cdots + |\Delta_l|,$$

где  $\Delta_1, \dots, \Delta_l$  – орбиты группы  $\mathcal{P}$  и  $|\Delta_i| \leq |\Delta_{i+1}|$ ,  $i = \overline{1, l-1}$ . Откуда, учитывая, что  $|\Delta_i| = p^{r_i}$ , получаем

$$|\alpha^G| = p^{r_1} + p^{r_2} + \cdots + p^{r_l} = p^m w.$$

Так как  $p^{m+1} \nmid |\alpha^G|$ , то  $r_1 = m$  и  $|\Delta_1| = p^m$ . Теорема доказана.  $\square$

**Теорема 13.4.**

Пусть  $G$  - транзитивна и  $H < G_\alpha$  такова, что любая подгруппа  $V < G_\alpha$ , сопряженная с  $H$  в  $G$ , сопряжена с ней в  $G_\alpha$ . Тогда  $N_G(H) = N$  транзитивна на множестве  $\Phi = \{\beta: \beta^H = \beta\}$  (множество элементов, оставляемых каждым элементом группы  $H$  на месте).

**Доказательство.**

Во-первых, докажем, что  $\Phi$  инвариантное множество для группы  $N$ . В самом деле, поскольку  $H \triangleleft N$ , то для любого  $t \in N$  и любого  $h \in H$  найдётся  $h_1 \in H$  такое, что  $th = h_1t$ . Поэтому если  $\beta \in \Phi$ , то  $(\beta^t)^h = \beta^{h_1t} = (\beta^{h_1})^t = \beta^t$ . Следовательно,  $\beta^t \in \Phi$  для любого  $t \in N$ . Это означает, что  $\Phi^N = \Phi$ , то есть  $\Phi$  - инвариантное для  $N$  множество.

Покажем, что это минимальное инвариантное множество, то есть орбита группы  $N$ . Пусть  $\alpha$  и  $\beta$  – произвольные элементы из  $\Phi$ . Так как по условию теоремы группа  $G$  транзитивна, то найдётся  $g \in G$  такое, что  $\alpha = \beta^g$ . Рассмотрим группу  $g^{-1}Hg = V$ . Поскольку  $\alpha^V = (\alpha^{g^{-1}})^{Hg} = (\beta^H)^g = \beta^g = \alpha$ , то  $V < G_\alpha$ . Из условия теоремы следует, что при некотором  $a \in G_\alpha$  выполняется соотношение  $H = aVa^{-1}$ . Отсюда получаем  $V = aHa^{-1} = g^{-1}Hg$ . Следовательно,  $b = ga \in N$  и  $\beta^b = (\beta^g)^a = \alpha^a = \alpha$ . Тем самым установлена транзитивность группы  $N$  на множестве  $\Phi$ .  $\square$

**Упражнение 13.3.** Доказать, что если  $G$  – транзитивная группа, то  $N_G(G_\alpha)$  транзитивна на множестве точек, оставляемых на месте подстановками из  $G_\alpha$ .

**Упражнение 13.4.** Доказать, что если  $G$  – транзитивная группа и  $\mathcal{P}$  – силовская подгруппа группы  $G_\alpha$ , то  $N_G(\mathcal{P})$  транзитивна на множестве точек, оставляемых на месте подстановками из  $\mathcal{P}$ .

Пусть  $g \in G < S_\Omega$ . Обозначим через

$$\text{Fix}(g) = \{\alpha \in \Omega: \alpha^g = \alpha\}.$$

**Лемма 13.1** (Бернсайд).

Если  $t$  – число орбит группы  $G$ , то

$$\sum_{g \in G} |\text{Fix}(g)| = t|G|.$$

*Доказательство.*

Пусть  $\Omega_1, \dots, \Omega_t$  – орбиты группы  $G$ . Тогда  $\Omega_i \cap \Omega_j = \emptyset$  ( $i \neq j$ ),  $\bigcup_{i=1}^t \Omega_i = \Omega$ . Рассмотрим множество

$$M_i = \{(\alpha, g) : \alpha^g = \alpha, \alpha \in \Omega_i, g \in G\}.$$

Очевидно, что  $\sum_{i=1}^t |M_i| = \sum_{g \in G} |\text{Fix}(g)|$ . Это следует из того, что множество  $M_i$  определяет все циклы длины один элементов группы  $G$  на орбите  $\Omega_i$ : для данного  $g \in G$  пара  $(\alpha, g)$  принадлежит множеству  $M_i$  тогда и только тогда, когда  $\alpha^g = \alpha$ ,  $\alpha \in \Omega_i$ .

Покажем, что  $|M_i| = |G|$ . Из определения  $M_i$  имеем:

$$M_i = \bigcup_{\alpha \in \Omega_i} \{(\alpha, g) : g \in G, \alpha^g = \alpha\} = \bigcup_{\alpha \in \Omega_i} \{(\alpha, g) : g \in G_\alpha\}.$$

Следовательно,  $|M_i| = \sum_{\alpha \in \Omega_i} |G_\alpha|$ . Далее, заметим, что согласно (13.1)  $|G_\alpha| = |G|/|\alpha^G| = |G|/|\Omega_i|$ . Поэтому

$$|M_i| = \sum_{\alpha \in \Omega_i} |G|/|\Omega_i| = |G|.$$

Отсюда следует, что

$$\sum_{i=1}^t |M_i| = \sum_{g \in G} |\text{Fix}(g)| = t|G|.$$

□

**Упражнение 13.5.** Доказать, что в любой транзитивной группе степени  $n > 1$  существует элемент степени  $n$ , то есть элемент, в цикловой записи которого нет циклов длины один.

**Упражнение 13.6.** Доказать, что если  $p$  — простое и  $p \mid |G|$ , то в группе подстановок  $G$  существует элемент, в цикловой записи которого содержится цикл длины  $p$ .

**Упражнение 13.7.** Доказать, что  $\text{Fix}(h^{-1}gh) = (\text{Fix}(g))^h$  для любого  $h \in G$ .

## 13.2 Регулярные и полурегулярные группы

**Определение 13.5.** Группа называется *полурегулярной*, если для любого  $\alpha \in \Omega$  выполняется соотношение  $G_\alpha = \langle e \rangle$ .

Например, группа Клейна

$K = \{e, (12)(34), (13)(24), (14)(23)\}$  является полурегулярной.

**Определение 13.6.** Транзитивная полурегулярная группа называется *регулярной*.

Группа Клейна является регулярной.

**Теорема 13.5.**

Порядок полурегулярной группы делит её степень. Транзитивная группа регулярна тогда и только тогда, когда её порядок и степень равны.

*Доказательство.*

Если  $G$  полурегулярная, то  $|\alpha^G| = |G|$  для  $\alpha \in G$ , то есть все орбиты группы имеют одинаковую длину. Поскольку  $\Omega$  есть объединение непересекающихся орбит группы  $G$ , то  $|\Omega| = t|G|$ , где  $t$  — число орбит группы  $G$ .

Если  $G$  полурегулярна и транзитивна, то  $|\Omega| = |G|$ , то есть порядок группы и её степень совпадают. Пусть теперь  $|G| = |\Omega|$

и  $G$  транзитивна на  $\Omega$ , тогда  $\alpha^G = \Omega$  и из теоремы 13.1 предыдущего пункта следует, что  $G_\alpha = \langle e \rangle$  для любого  $\alpha \in G$ . Тем самым теорема полностью доказана.  $\square$

Заметим, что примеры регулярных групп дают регулярные представления произвольных групп. Если  $G$  — произвольная конечная группа, то положим  $\Omega = G$ , тогда

$$G^* = \left\{ \begin{pmatrix} e & g_2 & \dots & g_m \\ g & gg_2 & \dots & gg_m \end{pmatrix} \mid g \in G \right\} \subset S^G,$$

и группы  $G$  и  $G^*$  изоморфны (теорема Кэли).

### Теорема 13.6.

*Если централизатор группы  $G$  в  $S^\Omega$  транзитивен на  $\Omega$ , то  $G$  полурегулярна.*

*Доказательство.*

Пусть  $H = Z_{S^\Omega}(G) = \{z \in S^\Omega : zg = gz \forall g \in G\}$  и  $\alpha, \beta \in \Omega$ . Из условия теоремы следует, что существует  $z \in H$  такой, что  $\alpha^z = \beta$ . Отсюда вытекает, что  $G_\beta = G_{\alpha^z} = z^{-1}G_\alpha z = G_\alpha$ . Так как  $\alpha$  и  $\beta$  выбраны произвольно, то  $G_\alpha = \langle e \rangle$  и, следовательно,  $G$  полурегулярна.  $\square$

### Следствие 13.2.

*Любая абелева группа  $G$ , транзитивная на  $\Omega$ , регулярна и является своим собственным централизатором в  $S^\Omega$ .*

*Доказательство.*

Так как  $G$  абелева, то  $Z_G = Z_{S^\Omega}(G) > G$ . Отсюда из транзитивности  $G$  следует, что  $Z_G$  транзитивен на  $\Omega$ . Из теоремы 13.6 следует, что  $G$  — регулярная группа. С другой стороны, поскольку централизатор

$$Z = Z_{S^\Omega}(Z_G) = \{g \in S^\Omega : gz = zg \forall z \in Z_G\} > G$$

и, следовательно, транзитивен, то  $Z_G$  также регулярная подгруппа. Поэтому согласно теореме 13.5 имеем:  $|Z_G| = |G| = |\Omega|$ . Учитывая, что  $Z_G > G$ , получаем требуемый результат, а именно:  $Z_{S^\Omega}(G) = G$ .  $\square$

**Упражнение 13.8.** Доказать, что централизатор полурегулярной группы транзитивен.

**Упражнение 13.9.** Доказать, что если  $G$  транзитивна на  $\Omega$ , то  $Z = Z_{S\Omega}(G)$  — полурегулярная группа и

$$|Z| = |\{\beta^g = \beta : g \in G_\alpha\}|.$$

**Теорема 13.7.**

Если  $|G| = 2n$  и  $n = 2k+1$ ,  $k \geq 1$ , то  $G$  содержит нормальный делитель порядка  $n$ .

*Доказательство.*

Из теоремы Коши следует, что  $G$  содержит элемент  $a$  второго порядка. Так как  $G^*$  регулярная группа, то соответствующая подстановка  $a^* = \begin{pmatrix} e & g_2 & \dots & g_{2n} \\ a & ag_2 & \dots & ag_{2n} \end{pmatrix}$  в группе  $G^*$  состоит из  $n$  независимых транспозиций. Так как  $n$  нечётно, то  $a^*$  — нечётная подстановка, и, следовательно, в  $G^*$  есть нечётные подстановки. Следовательно, множество всех чётных подстановок  $N^*$  группы  $G^*$  является подгруппой и эта подгруппа имеет индекс 2 и является нормальной. Искомый нормальный делитель  $N$  исходной группы  $G$  — это соответствующий образ группы  $N^*$ .  $\square$

### 13.3 Блоки и импримитивные группы

Пусть  $G < S^\Omega$  и  $\Delta \subset \Omega$ .

**Определение 13.7.** Множество  $\Delta$  называется блоком группы  $G$ , если для любого  $g \in G$  либо  $\Delta^g = \Delta$ , либо  $\Delta^g \cap \Delta = \emptyset$ .

Очевидно, что  $\emptyset, \Delta = \{\alpha\}, \Omega$  являются блоками. Эти блоки будем называть *тривиальными*. Если  $H < G$ , то если  $\Delta$  — блок  $G$ , то, естественно,  $\Delta$  будет блоком и для  $H$ .

**Утверждение 13.1.**

Если  $\Delta_1$  и  $\Delta_2$  — блоки группы  $G$ , то  $\Delta_1 \cap \Delta_2$  также блок.

*Доказательство.*

Пусть  $\Delta = \Delta_1 \cap \Delta_2$  и  $\Delta \cap \Delta^g \neq \emptyset$ . Это означает, что существуют  $\alpha, \beta \in \Delta$  такие, что  $\beta = \alpha^g$ . Из определения  $\Delta$  следует, что  $\beta \in \Delta_1 \cap \Delta_1^g$  и  $\beta \in \Delta_2 \cap \Delta_2^g$ . Отсюда, согласно определению блока, получим:  $\Delta_1^g = \Delta_1$ ,  $\Delta_2^g = \Delta_2$  и  $\Delta^g = \Delta_1^g \cap \Delta_2^g = \Delta$ . Следовательно,  $\Delta$  — блок группы  $G$ .  $\square$

**Утверждение 13.2.**

Если  $H < G$ ,  $g \in G$  и  $\Delta$  — блок группы  $H$ , то  $\Delta^g$  — блок группы  $g^{-1}Hg$ .

*Доказательство.*

Пусть  $h \in H$ . Допустим, что  $\Delta^{g(g^{-1}hg)} \cap \Delta^g \neq \emptyset$ . Из этого соотношения следует, что  $\Delta^{hg} \cap \Delta^g \neq \emptyset$ . Отсюда следует, что  $\Delta^h \cap \Delta \neq \emptyset$ . Так как  $\Delta$  — блок группы  $H$ , то это означает, что  $\Delta^h = \Delta$ . Поэтому  $\Delta^{hg} = \Delta^g$  или  $\Delta^{g(g^{-1}hg)} = \Delta^g$ . Таким образом,  $\Delta^g$  — блок группы  $g^{-1}Hg$ .  $\square$

**Утверждение 13.3.**

Мощность блока транзитивной группы является делителем её степени.

*Доказательство.*

Пусть  $G$  — транзитивная на  $\Omega$  группа. Из Утверждения 13.2 следует, что если  $\Delta_0$  — блок группы  $G$ , то  $\Delta_0^g$  при любом  $g \in G$  также блок группы  $G$ . Два таких блока назовем сопряженными. Совокупность всех блоков группы  $G$ , сопряженных с данным блоком  $\Delta_0$ , образуют полную систему блоков  $\sum(\Delta_0)$ . Все блоки этой системы, очевидно, имеют одинаковую мощность, равную  $|\Delta_0|$ . Так как  $G$  — транзитивная группа, то  $\bigcup_{\Delta \in \sum(\Delta_0)} \Delta = \Omega$ . Следовательно,  $|\Omega| = |\Delta| \cdot |\sum(\Delta_0)|$ . Тем самым установлена справедливость утверждения 13.3.  $\square$

**Упражнение 13.10.** Доказать, что блоки группы

$$G = \langle (1 \ 2 \ \dots \ n) \rangle$$

являются классами вычетов по  $\text{mod } k$ , где  $k$  пробегает множество всех делителей  $n$ .

**Определение 13.8.** Транзитивная группа  $G$  называется *импримитивной*, если для неё существует по крайней мере один нетривиальный блок  $\Delta$ . Такой блок обычно называют *множеством импримитивности* группы  $G$ .

**Пример 13.5.**  $\mathcal{K} = \{e, (12)(34), (13)(24), (14)(23)\}$ ,  $\Delta_1 = \{1, 2\}$ ,  $\Delta_2 = \{3, 4\}$  — блоки группы  $\mathcal{K}$ , следовательно  $\mathcal{K}$  — импримитивная группа.

**Теорема 13.8.**

Если  $G$  транзитивная группа,  $N \neq \langle e \rangle$ ,  $N \triangleleft G$  и  $N$  — интранзитивная группа, то  $G$  импримитивна и орбиты группы  $N$  образуют полную систему блоков группы  $G$ .

**Доказательство.**

Пусть  $\Delta$  — орбита группы  $N$ . Тогда  $\Delta^g$  для любого  $g \in G$  — орбита группы  $g^{-1}Ng = N$ . Поскольку орбиты не пересекаются, а группа  $G$  по условию транзитивна, то  $\bigcup_{g \in G} \Delta^g = \Omega$ . Так

как  $N \neq \langle e \rangle$ , то каждая орбита группы  $N$  содержит более одной точки (все орбиты группы  $N$  имеют одинаковую длину, при воздействии на орбиты элементом  $g \in G$  орбиты переставляются) и, поскольку  $N$  интранзитивна,  $|\Delta| \neq |\Omega|$ . Из вышеизложенного следует, что орбиты группы  $N$  образуют полную систему блоков группы  $G$ .  $\square$

**Упражнение 13.11.** Пусть  $\bar{\Omega} = \{\Delta_1, \dots, \Delta_k\}$  — нетривиальная полная система блоков импримитивной группы  $G$  и  $\bar{g}$  — подстановка на  $\bar{\Omega}$ , индуцированная подстановкой  $g \in G$ :

$$\bar{g} = \begin{pmatrix} \Delta_1 & \dots & \Delta_k \\ \Delta_1^g & \dots & \Delta_k^g \end{pmatrix}.$$

Доказать, что  $\bar{G} = \{\bar{g}: g \in G\} < S^{\bar{\Omega}}$  и отображение  $\varphi: G \rightarrow \bar{G}$ , определённое по правилу  $\varphi(g) = \bar{g}$ , является гомоморфизмом группы  $G$  на  $\bar{G}$ .

**Упражнение 13.12.** Доказать, что группа  $\bar{G}$  из предыдущей задачи транзитивна на  $\bar{\Omega}$ .

**Теорема 13.9.**

Если  $G$  транзитивна на  $\Omega$  и  $\alpha \in \Delta \subset \Omega$ , то множество  $\psi = \bigcap_{g \in \{g \in G: \alpha \in \Delta^g\}} \Delta^g$  является блоком группы  $G$ .

*Доказательство.*

Пусть  $h \in G$  и  $\psi \cap \psi^h \neq \emptyset$ . Возможны следующие случаи:

I. Элемент  $\alpha \in \psi^h = \bigcap_{g \in \{g \in G: \alpha \in \Delta^g\}} \Delta^{gh}$ , т.е.  $\alpha \in \Delta^{gh}$ . Очевидно, что

$$\{g \in G: \alpha \in \Delta^g\} \supset \{g \in G: \alpha \in \Delta^{gh}\}.$$

Следовательно,  $\psi^h \supseteq \psi$ . Так как  $|\psi^h| = |\psi|$ , то  $\psi^h = \psi$ .

II.  $\beta \in \psi \cap \psi^h$ ,  $\beta \neq \alpha$ . Из транзитивности  $G$  следует, что найдётся  $v \in G$  такое, что  $\alpha^v = \beta$ . Это означает, что  $\alpha \in \psi^{v^{-1}} \cap \psi^{hv^{-1}}$ . Следовательно, мы пришли к случаю I, из которого следует, что  $\psi^{v^{-1}} = \psi^{hv^{-1}}$ . Отсюда немедленно вытекает, что  $\psi^h = \psi$ .

Теорема полностью доказана.  $\square$

**Теорема 13.10** (Критерий импримитивности).

Транзитивная группа  $G < S^\Omega$  импримитивна тогда и только тогда, когда существует группа  $H$  такая, что при некотором  $\alpha \in \Omega$  выполняются следующие условия:

$$G_\alpha < H < G, H \neq G_\alpha, H \neq G \quad (13.4)$$

*Доказательство.*

**Необходимость.** Пусть  $G$  импримитивна,  $\psi$  — нетривиальный блок группы  $G$  и  $\alpha \in \psi$ . Рассмотрим подгруппу  $H$  группы  $G$ , определённую следующим образом:

$$H = \{h \in G: \psi^h = \psi\}.$$

Очевидно, что  $H \neq G$ . Поскольку  $\psi \neq \Omega$  и  $G$  транзитивна на  $\Omega$ , то существует  $g \in G$  такой, что  $\psi^g \neq \psi$ . Поскольку  $\psi$  — блок, то из  $\alpha^g = \alpha$  следует, что  $\psi^g = \psi$ . Это означает, что  $G_\alpha < H$ . С другой стороны, так как  $|\psi| > 1$ , а  $G$  транзитивна, то найдутся  $\beta \in \psi$ ,  $\beta \neq \alpha$  и  $h \in G$  такие, что  $\alpha^h = \beta$ . Отсюда следует, что  $\psi^h = \psi$ , то есть  $h \in H$ , но  $h \notin G_\alpha$ . Таким образом,  $G_\alpha < H < G$ ,  $H \neq G_\alpha$ .

**Достаточность.** Пусть подгруппа  $H$  удовлетворяет условию (13.4) и  $\psi = \alpha^H$ . Покажем, что  $\psi$  — блок группы  $G$ . Допустим, что  $\psi \cap \psi^g \neq \emptyset$  и  $\beta \in \psi \cap \psi^g$ ,  $g \in G$ . Тогда найдутся такие  $h, h_1 \in H$ , что  $\beta = \alpha^h = \alpha^{h_1 g}$ . Отсюда следует, что  $h_1 gh^{-1} \in G_\alpha$  и поскольку,  $G_\alpha < H$ , то  $g \in H$ . Из определения  $\psi$  следует, что  $\psi^g = \alpha^{Hg} = \alpha^H$ , то есть  $\psi$  есть блок группы  $G$ . Далее, так как  $G_\alpha \neq H$ ,  $G_\alpha < H$ , то  $|\psi| > 1$ . С другой стороны, поскольку мы установили, что из равенства  $\psi = \psi^g$  следует, что  $g \in H \neq G$ , то найдётся  $g' \in G$  такой, что  $\psi^{g'} \neq \psi$ . Поэтому  $\psi \neq \Omega$ . Таким образом,  $\psi$  — нетривиальный блок группы  $G$  и, следовательно,  $G$  импримитивна.  $\square$

**Упражнение 13.13.** Доказать, что если  $G$  регулярна на  $\Omega$  группа и  $|\Omega|$  — составное число, то  $G$  импримитивна.

## 13.4 Примитивные группы. Кратная транзитивность

**Определение 13.9.** Группа называется *примитивной*, если она имеет только тривиальные блоки.

**Утверждение 13.4.**

Если  $\Delta$  — собственное подмножество множества  $\Omega$  и  $G$  примитивна на  $\Omega$ , то для любых двух различных элементов  $\alpha$  и  $\beta$  из  $\Omega$  найдётся элемент  $g \in G$  такой, что  $\alpha \in \Delta^g$ ,  $\beta \notin \Delta^g$ .

**Доказательство.**

По теореме 13.9 предыдущего пункта  $\psi = \bigcap_{g \in \{g \in G : \alpha \in \Delta^g\}} \Delta^g$  — блок для  $G$ . Поскольку по условию  $|\Delta| < |\Omega|$ , а группа  $G$  при-

митивна на  $\Omega$ , получаем, что  $\psi = \{\alpha\}$ . Поэтому хотя бы для одного  $g \in G$   $\beta \notin \Delta^g$ . В противном случае мощность блока  $\psi$  была бы больше единицы.  $\square$

**Упражнение 13.14.** Пусть  $\alpha \in \Omega$ ,  $|\Omega| > 1$ . Доказать, что транзитивная группа  $G$  примитивна тогда и только тогда, когда  $G_\alpha$  — максимальная подгруппа группы  $G$ .

**Упражнение 13.15.** Доказать, что если группа  $G \neq \langle e \rangle$  примитивна на  $\Omega$ , то  $G$  транзитивна на  $\Omega$ .

**Упражнение 13.16.** Доказать, что транзитивная группа простой степени примитивна.

Пусть  $\Delta$  — инвариантное множество группы  $G < S^\Omega$ ,  $\Delta \subset \Omega$ . В частности,  $\Delta$  может быть орбитой группы  $G$ . Определим на множестве  $\Delta$  группу подстановок

$$G^\Delta = \{g^\Delta : g \in G\} < S^\Delta$$

следующим образом. Если  $g \in G$  и  $\alpha, \beta \in \Delta$ , то  $\alpha^{g^\Delta} = \beta$  в том и только в том случае, если  $\alpha^g = \beta$ .

Очевидно, что соответствие  $\varphi(g) = g^\Delta$  является гомоморфизмом группы  $G$  на  $G^\Delta$ . Группу  $G^\Delta$  называют *составляющей* группы  $G$  на множестве  $\Delta$ . Если  $\varphi$  — изоморфизм, то  $|G^\Delta| = |G|$  и составляющая  $G$  называется *точной*.

### Теорема 13.11.

Пусть  $G$  транзитивна на  $\Omega$ ,  $V < G$  и  $\Delta$  — орбита группы  $V$ . Тогда, если  $V^\Delta$  примитивна на  $\Delta$  и  $|\Omega| < 2|\Delta|$ , то  $G$  примитивна на  $\Omega$ .

### Доказательство.

Пусть  $\psi$  — произвольный блок  $G$ , следовательно, он является и блоком для группы  $V$ . Поскольку  $\Delta$  — орбита  $V$ , то есть  $\Delta^V = \Delta$ , то  $\Delta$  также блок группы  $V$ . Для  $g \in G$ ,  $\Phi = \Delta \cap \psi^g$  — блок группы  $V$ , возможно, совпадающий с пустым множеством.

Из определения группы  $V^\Delta$  вытекает, что  $\Phi$  будет блоком и для группы  $V^\Delta$ . Напомним, что  $\alpha^v = \alpha^{v^\Delta}$ , для любого  $\alpha \in \Delta$  и, кроме того, если  $\Phi^v = \Phi$ , то  $\Phi^{v^\Delta} = \Phi^v = \Phi$ .

Далее, так как  $V^\Delta$  примитивна на  $\Delta$ , то возможны следующие случаи:

1.  $\Phi = \Delta$ , то есть  $\psi^g \supset \Delta$ , для некоторого  $g \in G$ . Отсюда и из условия теоремы следует, что  $|\psi| = |\psi^g| \geq |\Delta| > \frac{|\Omega|}{2}$  и  $|\psi|$  делит  $|\Omega|$ . Поэтому  $|\psi| = |\Omega|$  и  $\psi = \Omega$  — тривиальный блок.
2.  $|\Phi| \leq 1$  при любом  $g \in G$ . Из транзитивности группы  $G$  следует, что число  $T$  блоков группы  $G$  сопряжённых с  $\psi$  и таких, что  $|\psi^g \cap \Delta| \leq 1$ , будет не менее  $|\Delta| > \frac{|\Omega|}{2}$ . С другой стороны  $|T| \cdot |\psi| = |\Omega|$ , поэтому  $T = |\Omega|$ ,  $|\psi| = 1$  и, следовательно,  $\psi$  — тривиальный блок.

□

**Упражнение 13.17.** Пусть  $G > C$ ,  $G > D$  и  $G = \langle C, D \rangle$ . Доказать, что если  $C$  примитивна на  $\Gamma \subset \Omega$ ,  $C < G_{\Omega \setminus \Gamma}$ ,  $D$  примитивна на  $\Delta \subset \Omega$ ,  $D < G_{\Omega \setminus \Delta}$ , то  $G$  примитивна на  $\Omega$ .

**Теорема 13.12.**

Если  $G$  примитивна на  $\Omega$ ,  $\alpha, \beta \in \Omega$ ,  $\alpha \neq \beta$ , то либо  $G_\alpha \neq G_\beta$ , либо  $G$  — регулярная группа простой степени.

**Доказательство.**

Рассмотрим возможные случаи.

(а) Пусть  $G_\alpha \neq \langle e \rangle$  для некоторого  $\alpha \in \Omega$  и

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

Ранее было доказано, что  $N_G(G_\alpha) = N$  транзитивен на  $\Phi$ . Допустим, что  $G_\alpha = G_\beta$  при  $\alpha \neq \beta$ . Тогда  $\alpha, \beta \in \Phi$  и из транзитивности  $N$  следует, что  $N > G_\alpha$ ,  $N \neq G_\alpha$ . Отсюда и из примитивности группы  $G$  следует, что  $N = G$ ,  $\Phi = \Omega$  и  $G_\alpha = \langle e \rangle$ . Пришли к противоречию с условием  $G_\alpha \neq \langle e \rangle$ . Следовательно,  $G_\alpha \neq G_\beta$ .

(b) Пусть  $G_\alpha = \langle e \rangle$  для каждого  $\alpha \in \Omega$ . Тогда  $G$  — регулярная группа и, следовательно, её степень есть простое число.  $\square$

### Следствие 13.3.

*Если  $G$  примитивна на  $\Omega$  и  $\alpha, \beta \in \Omega$ ,  $\alpha \neq \beta$ , то либо  $G = \langle G_\alpha, G_\beta \rangle$ , либо  $G$  — регулярная группа простой степени.*

*Доказательство.*

Предположим, что  $\langle G_\alpha, G_\beta \rangle \neq G$ . Откуда следует, что  $G_\beta < \langle G_\alpha, G_\beta \rangle < G$ . Так как по условию  $G$  — примитивна, то либо  $G = \langle G_\alpha, G_\beta \rangle$ , либо  $\langle G_\alpha, G_\beta \rangle = G_\beta$ . Так как  $\alpha$  и  $\beta$  — произвольны, то из  $\langle G_\alpha, G_\beta \rangle = G_\beta$  следует, что  $G_\alpha = \langle e \rangle$  для любого  $\alpha \in \Omega$ . Следовательно,  $G$  — регулярная группа простой степени.  $\square$

**Упражнение 13.18.** Пусть  $N \triangleleft G$ ,  $N \neq \langle e \rangle$  и  $N$  транзитивна. Доказать, что если существует такой нетривиальный нормальный делитель  $H$  группы  $G$  ( $H \triangleleft G$ ,  $H \neq \langle e \rangle$ ), что  $N < H$ , то  $G$  примитивна на  $\Omega$ .

**Упражнение 13.19.** Доказать, что если степень примитивной группы чётная и больше 2, то порядок группы делится на 4.

**Определение 13.10.** Группа  $G$  называется  $m$ -транзитивной на  $\Omega$ , если для любых двух упорядоченных кортежей

$$(\alpha_1 \dots \alpha_m)$$

и

$$(\beta_1 \dots \beta_m)$$

множества  $\Omega$  существует элемент  $g \in G$  такой, что

$$\alpha_i^g = \beta_i, \quad i = \overline{1, m}.$$

### Теорема 13.13.

*Если  $|\Omega| = n$ ,  $n > 1$ , то группа  $S_n$   $n$ -транзитивна, а группа  $A_n$  —  $(n - 2)$ -транзитивна, но не  $(n - 1)$ -транзитивна.*

*Доказательство.*

Для  $S_n$  утверждение очевидно, его справедливость следует из определения группы  $S_n$ . Далее заметим, что одна из подстановок

$$\begin{pmatrix} \alpha_1 & \dots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \dots & \beta_{n-2} & \beta_{n-1} & \beta_n \end{pmatrix},$$

$$\begin{pmatrix} \alpha_1 & \dots & \alpha_{n-2} & \alpha_n & \alpha_{n-1} \\ \beta_1 & \dots & \beta_{n-2} & \beta_{n-1} & \beta_n \end{pmatrix}$$

является чётной. Следовательно, группа  $A_n$  является  $(n-2)$ -транзитивной. Эта группа не может быть  $(n-1)$ -транзитивной, так как в этом случае она была бы  $n$ -транзитивной и совпадала с  $S_n$ , а это не так.  $\square$

**Теорема 13.14.**

Пусть  $G$  транзитивна на  $\Omega$  и  $m \geq 2$ . Тогда  $G$  является  $m$ -транзитивной тогда и только тогда, когда для некоторого  $\alpha \in \Omega$  группа  $G_\alpha$   $(m-1)$ -транзитивна на  $\Omega \setminus \{\alpha\}$ .

*Доказательство.*

**Необходимость** очевидна.

**Достаточность.** Пусть  $G$  транзитивна на  $\Omega$ , а группа  $G_\alpha$   $(m-1)$ -транзитивна на  $\Omega \setminus \{\alpha\}$ . Покажем, что для любого  $\beta \neq \alpha$  группа  $G_\beta$  транзитивна на  $\Omega \setminus \{\beta\}$ . Действительно, из транзитивности  $G$  следует, что  $\beta = \alpha^g$  для некоторого  $g \in G$ . Поэтому  $G_\beta = G_{\alpha^g} = g^{-1}G_\alpha g$ . Пусть  $(\alpha_1 \dots \alpha_{m-1})$  и  $(\beta_1 \dots \beta_{m-1})$  — два произвольных упорядоченных подмножества из  $\Omega \setminus \{\beta\}$ . Очевидно, что  $\alpha_i^{g^{-1}} \neq \alpha$ ,  $\beta_i^{g^{-1}} \neq \alpha$  для  $i = \overline{1, m-1}$ . Из  $(m-1)$ -транзитивности группы  $G_\alpha$  на  $\Omega \setminus \{\alpha\}$  следует, что существует  $g_\alpha \in G_\alpha$  такой, что  $\alpha_i^{g^{-1}g_\alpha} = \beta_i^{g^{-1}}$  для  $i = \overline{1, m-1}$ . Следовательно,  $\alpha_i^{g^{-1}g_\alpha g} = \beta_i$  для  $i = \overline{1, m-1}$ . Это означает, что группа  $G_\beta$  транзитивна на  $\Omega \setminus \{\beta\}$ .

Пусть теперь даны произвольные упорядоченные подмножества  $(\alpha_1 \dots \alpha_m)$  и  $(\beta_1 \dots \beta_m)$  множества  $\Omega$ . Пользуясь транзитивностью  $G$ , выберем  $a \in G$  так, чтобы  $\alpha_1^a = \beta_1$ . Далее, воспользуемся  $(m-1)$ -транзитивностью группы  $G_{\beta_1}$  и

найдём  $h \in G_\beta$  такой, что  $(\alpha_i^a)^h = \beta_i$ ,  $i = \overline{2, m}$ . Очевидно, что  $(\alpha_i^a)^h = \beta_i$  для всех  $i = \overline{1, m}$ . Тем самым установлена транзитивность группы  $G$ .  $\square$

### Теорема 13.15.

*Транзитивная группа  $G$  является дважды транзитивной тогда и только тогда, когда, для любого  $g \in G \setminus G_\alpha$  выполняется условие*

$$G = G_\alpha + G_\alpha g G_\alpha \quad (13.5)$$

*Доказательство.*

**Необходимость.** Пусть  $G$  дважды транзитивна и  $g, h \in G \setminus G_\alpha$ . Тогда, если  $\alpha^h = \beta$ ,  $\alpha^g = \gamma$ , то  $\gamma \neq \alpha$ ,  $\beta \neq \alpha$ . Из предыдущей теоремы следует, что  $G_\alpha$  транзитивна на  $\Omega \setminus \{\alpha\}$ , поэтому существует  $k \in G_\alpha$  такой, что  $\beta^k = \gamma$ . Следовательно,  $\alpha^{hk} = \gamma = \alpha^g$ . Отсюда вытекает, что  $hkg^{-1} \in G_\alpha$ , то есть  $h = g_\alpha g k^{-1} \in G_\alpha g G_\alpha$ . Так как  $h$  произвольный элемент из  $G \setminus G_\alpha$ , то это означает, что  $G \setminus G_\alpha \subseteq G_\alpha g G_\alpha$ . С другой стороны, поскольку  $\alpha^g \neq \alpha$ , то  $G_\alpha g G_\alpha \cap G_\alpha = \emptyset$  и поэтому  $G_\alpha g G_\alpha = G \setminus G_\alpha$  и  $G = G_\alpha + G_\alpha g G_\alpha$ .

**Достаточность.** Пусть выполняется условие (13.5)  $G$  – транзитивная на  $\Omega$  группа и  $\beta, \gamma \in \Omega \setminus \{\alpha\}$ . Из транзитивности  $G$  следует, что существуют  $h_1$  и  $h_2$  из  $G$  такие, что  $\alpha^{h_1} = \beta$ ,  $\alpha^{h_2} = \gamma$ . Очевидно, что  $h_1, h_2 \notin G_\alpha$  и, следовательно, согласно (13.5)  $h_2 \in G_\alpha h_1 G_\alpha$ . Поэтому для некоторых  $k_1, k_2 \in G_\alpha$   $h_2 = k_1 h_1 k_2$ . Отсюда получаем  $\gamma = \alpha^{h_2} = \alpha^{k_1 h_1 k_2} = \alpha^{h_1 k_2} = \beta^{k_2}$ . Таким образом, группа  $G_\alpha$  транзитивна на  $\Omega \setminus \{\alpha\}$  и, следовательно,  $G$  – дважды транзитивна.  $\square$

**Упражнение 13.20.** Доказать, что если  $G$  дважды транзитивна, то она примитивна.

### Теорема 13.16.

*Если  $G$  – транзитивная на  $\Omega$  группа и  $G_\alpha$  имеет  $t$  орбит на  $\Omega$ , то*

$$\sum_{g \in G} |\text{Fix}(g)|^2 = t \cdot |G|, \quad (13.6)$$

при этом транзитивная группа  $G$  дважды транзитивна тогда и только тогда, когда

$$\sum_{g \in G} |\text{Fix}(g)|^2 = 2 \cdot |G|. \quad (13.7)$$

*Доказательство.*

I. Пусть

$$M = \{(g, \alpha, \beta) : \alpha \in \Omega, \beta \in \Omega, g \in G_\alpha \cap G_\beta\},$$

$$M_g = \{(g, \alpha, \beta) : \alpha^g = \alpha, \beta^g = \beta\}.$$

Очевидно, что

$$|M_g| = |\{(\alpha, \beta) : \alpha^g = \alpha, \beta^g = \beta\}| = |\text{Fix}(g) \times \text{Fix}(g)| = |\text{Fix}(g)|^2.$$

С другой стороны  $M = \bigcup_{g \in G} M_g$  и, следовательно,

$$|M| = |\text{Fix}(g)|^2. \quad (13.8)$$

Далее, пусть  $T_\alpha = \{(g, \alpha, \beta) : g \in G_\alpha, \beta^g = \beta, \beta \in \Omega\}$ . Эти множества удовлетворяют следующим условиям:

(a)  $T_\alpha \cap T_\gamma = \emptyset$ , если  $\alpha \neq \gamma$ ;

(b)  $\bigcup_{\alpha \in \Omega} T_\alpha = M$ ;

(c)  $|T_\alpha| = |T_\gamma|$ .

Справедливость свойств (a) и (b) следует из определений множеств  $M$  и  $T_\alpha$ . Докажем справедливость условия (c). Так как  $G$  — транзитивная группа, то существует  $g_0 \in G$  такой, что  $\alpha^{g_0} = \gamma$ ,  $g_0^{-1}G_\alpha g_0 = G_{\alpha^{g_0}} = G_\gamma$ . Поэтому, если  $(g, \alpha, \beta) \in T_\alpha$ , то  $(\beta^{g_0})^{g_0^{-1}g_0} = \beta^{gg_0} = \beta^{g_0}$  и отсюда следует, что  $(g_0^{-1}g_0, \alpha^{g_0} = \gamma, \beta^{g_0}) \in T_\gamma$ . Таким образом,  $|T_\gamma| \geq |T_\alpha|$ , а поскольку  $\alpha$  и  $\gamma$  — произвольные элементы из  $\Omega$ , то отсюда следует, что  $|T_\alpha| = |T_\gamma|$ .

Из (a), (b) и (c) вытекает, что

$$|M| = |\Omega| \cdot |T_\alpha|. \quad (13.9)$$

С другой стороны,

$$|T_\alpha| = |\{(g, \beta) : g \in G_\alpha, \beta^g = \beta\}| = \sum_{g \in G_\alpha} |\text{Fix}(g)|$$

и по лемме Бернсайда

$$|T_\alpha| = t \cdot |G_\alpha|. \quad (13.10)$$

Из (13.8), (13.9) и (13.10) получаем:  $\sum_{g \in G} |\text{Fix}(g)|^2 = |\Omega| \cdot t \cdot |G_\alpha|$ .

Но из транзитивности  $G$  следует, что  $|\Omega| = [G : G_\alpha] = \frac{|G|}{|G_\alpha|}$  и поэтому  $\sum_{g \in G} |\text{Fix}(g)|^2 = t \cdot |G|$ .

II. Если  $G$  дважды транзитивна, то  $G_\alpha$  транзитивна на  $\Omega \setminus \{\alpha\}$  и имеет две орбиты на  $\Omega$  и, следовательно, (13.7) справедливо.

Пусть  $G$  транзитивна и выполняется (13.7) то есть  $G_\alpha$  имеет две орбиты на  $\Omega$ . Одна орбита это  $\{\alpha\}$ , следовательно другая –  $\Omega \setminus \{\alpha\}$ . Таким образом  $G_\alpha$  транзитивна на  $\Omega \setminus \{\alpha\}$ , следовательно, группа  $G$  транзитивна на  $\Omega$ .  $\square$

### 13.5 Группы подстановок с регулярным нормальным делителем

*Определение 13.11.* Автоморфизмом конечной группы  $G$  называется взаимно однозначное отображение  $\phi : G \rightarrow G$  обладающее свойством гомоморфизма, т.е. для  $\forall g_1, g_2 \in G$ :

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2).$$

*Определение 13.12.* Группой автоморфизмов группы  $G$  называется множество всех автоморфизмов  $G$  и обозначается через  $\text{Aut}(G)$ .

Например, если  $G = F^*$ , где  $|F| = q = p^m$ , то

$$Aut(G) = \{\sigma_i | i = \overline{0, m-1}\}, \text{ где } \sigma_i(x) = x^{p^i}.$$

### Теорема 13.17.

Пусть  $N$  — конечная группа и  $G$  — группа автоморфизмов группы  $N$ , тогда  $G$  можно рассматривать как группу подстановок на множестве  $N^* = N \setminus \{e\}$  и справедливы следующие утверждения:

1. Если  $G$  транзитивная, то  $N$  — элементарная абелева группа для некоторого простого  $p$ .
2. Если  $G$  — дважды транзитивная, то либо  $|N| = 3$ , либо  $N$  — абелева 2-группа.
3. Если  $G$  — трижды транзитивная, то  $|N| = 4$
4.  $G$  не может быть четырежды транзитивной.

*Доказательство.*

1. Пусть  $p$  — простое число, делящее порядок  $N$ . Из теоремы Коши следует, что существует элемент  $a \in N$  порядка  $p$ . Из транзитивности  $G$  на множестве  $N \setminus \{e\}$  получаем, что для любого  $b = N^*$  найдётся  $g \in G$ , для которого  $a^g = b$ . При действии автоморфизма порядок элемента не меняется, поэтому любой неединичный элемент из  $N$  будет иметь порядок равный  $p$ , следовательно,  $N$  —  $p$ -группа. Докажем её абелевость. Центр  $Z(N)$  группы  $N$  отличен от единицы и для любого  $z \in Z(N)$  и любого  $a \in N$  верно соотношение  $za = az$ . Откуда немедленно следует, что  $z^g a^g = a^g z^g$  для любого  $g \in G$  и, так как  $a$  — произвольный элемент группы, то  $z^g \in Z(N)$ . В силу транзитивности группы  $G$  получаем  $\{z^g | g \in G\} = N^*$ . Таким образом  $Z(N)^G = Z(N) = N$ , то есть  $N$  — элементарная абелева  $p$ -группа.

2. Пусть группа  $G$  — дважды транзитивная и  $p > 2$ . Рассмотрим множество  $\Delta = \{x, x^{-1}\}$ , где  $x \in N^*$ , тогда  $\Delta^g = \{y, y^{-1}\}$ ,  $x^g = y$ ,  $(x^{-1})^g = y^{-1}$ ,  $g \in G$ . Докажем, что  $\Delta$  — блок группы  $G$ . Пусть  $\Delta^g \cap \Delta \neq \emptyset$ . Возможны следующие случаи:

- $y = x^{-1}$ , тогда  $(x^{-1})^g = y^{-1} = x$  и  $\Delta^g = \Delta$ .
- $y \neq x$   $y \neq x^{-1}$ , тогда  $(x^{-1})^g \neq y^{-1} \neq x$  и  $\Delta^g \cap \Delta = \emptyset$ .

Итак,  $\Delta$  — блок группы  $G$  и  $|\Delta| = N^*$ , поэтому

$$2 = |\Delta| = |N| - 1,$$

значит  $|N| = 3$ .

3. Пусть  $G$  трижды транзитивная, тогда  $|N^*| \geq 3$ , то есть  $|N| \geq 4$ . Из пункта 2 следует, что  $N$  — абелева 2-группа, то есть порядок любого неединичного элемента равен 2 или для любого  $x \in N$   $x = x^{-1}$ , следовательно,  $|N| = 2^m$ ,  $m \geq 2$ . Из первой теоремы Силова следует, что существует подгруппа  $H$  группы  $N$  такая, что  $|H| = 4$ . Пусть  $H = \{e, a, b, c\}$ ,  $or(a) = or(b) = or(c) = 2$ ,  $c = ab$ . Покажем, что  $\psi = \{a, b\}$  — блок группы  $G_c$ . Пусть  $g \in G_c$  и  $\psi^g = \{a^g, b^g\}$ , если  $\psi^g \cap \psi \neq \emptyset$ , то

- $a^g = b$ , тогда  $a = b^{g^{-1}} = (b^{-1})^g = b^g$  и  $\Delta^g = \Delta$ .
- $a^g = a$ , тогда  $(ab)^g = c = ab = a^g b^g = ab^g$ , то есть  $b^g = b$  и  $\Delta^g = \Delta$ .

Таким образом,  $\psi$  — блок группы  $G_c$ .

Но  $G_c$  — дважды транзитивная группа, следовательно, она примитивна, а значит  $|N^* \setminus \{c\}| = 2$ , поэтому  $|N| = 4$ .

4. Группа  $G$  не может быть четырежды транзитивной на  $N^*$ , так как в этом случае должно выполняться условие:  $|N| \geq 5$ . Но из пункта 3 следует, что  $|N| = 4$ . Противоречие.  $\square$

**Утверждение 13.5.**

Пусть  $G < S^\Omega$ ,  $N = \{e, v_1, v_2, \dots, v_m\} \triangleleft G$ ,  $N$  — регулярная и

$$G_\alpha^* = \left\{ g^* = \begin{pmatrix} v_1 & v_2 & \dots & v_m \\ g^{-1}v_1g & g^{-1}v_2g & \dots & g^{-1}v_mg \end{pmatrix} \middle| g \in G_\alpha \right\}.$$

Тогда группа подстановок  $G_\alpha$  на  $\Omega \setminus \{\alpha\}$  изоморфна группе подстановок  $G_\alpha^*$  на  $N^*$ .

*Доказательство.*

Определим отображение  $\varepsilon : G_\alpha \rightarrow G_\alpha^*$  по правилу

$$\varepsilon(g) = \begin{pmatrix} v_i \\ g^{-1}v_i g \end{pmatrix}, \quad i = \overline{1, m}, \quad \{v_1, v_2, \dots, v_m\} = N^* = N \setminus \{e\}.$$

Покажем, что  $\varepsilon$  — изоморфизм. Действительно,

$$\varepsilon(ab) = \begin{pmatrix} v_i \\ b^{-1}a^{-1}v_iab \end{pmatrix} = \begin{pmatrix} v_i \\ a^{-1}v_i a \end{pmatrix} \begin{pmatrix} a^{-1}v_i a \\ b^{-1}a^{-1}v_iab \end{pmatrix} = \varepsilon(a)\varepsilon(b).$$

Далее, если  $\varepsilon(a) = \varepsilon(b)$ , то  $a^{-1}v_i a = b^{-1}v_i b$ ,  $i = \overline{1, m}$ , следовательно,

$$ba^{-1}v_i ab^{-1} = v_i, \quad \forall i = \overline{1, m}.$$

Поскольку,  $a, b \in G_\alpha$ , то

$$\alpha^{v_i} = \alpha^{ba^{-1}v_i ab^{-1}} = \alpha^{v_i ab^{-1}},$$

значит  $ab^{-1} \in G_\alpha^{v_i}$ , следовательно  $ab^{-1} = e$ , то есть  $a = b$ . Таким образом,  $G_\alpha^*$  и  $G_\alpha$  изоморфны.

Определим отображение  $\psi : N^* \rightarrow \Omega \setminus \{\alpha\}$  следующим образом:  $\psi(v) = \beta$  тогда и только тогда, когда  $\alpha^v = \beta$  и  $v \in N^*$ . Докажем, что оно биективно, то есть взаимно однозначно. Из транзитивности  $N$  следует, что оно сюръективно. Если  $\alpha^v = \alpha^u$ , то  $\alpha^{v^{-1}u} = \alpha$ , то есть  $v^{-1}u \in N_\alpha$ . Из регулярности  $N$  вытекает, что  $v = u$ , то есть  $\psi$  — инъективное отображение, а значит и взаимно однозначное.

Осталось доказать, что если  $\varepsilon(g) = g^*$  и  $v^{g^*} = u$ , то  $\psi(v)^g = \psi(u)$  для  $\forall g \in G_\alpha$ . Из определения  $\psi$  и  $g^*$  имеем:

$$\begin{aligned} v^{g^*} &= g^{-1}vg = u, \quad \psi(v) = \beta, \quad \alpha^v = \beta, \quad \alpha^{gug^{-1}} = \beta, \\ \alpha^u &= \beta^g, \quad \psi(u) = \psi(v)^g. \end{aligned}$$

Тем самым утверждение полностью доказано.  $\square$

### Утверждение 13.6.

Пусть  $G$  —  $m$ -транзитивная группа подстановок степени  $n$  и  $N$  — её регулярный нормальный делитель, тогда

1. Если  $m = 2$ , то  $|N| = p^k$  для некоторого простого  $p$ .
2.  $m = 3$ , то  $|N| = 3$  или  $|N| = 2^k$ .
3.  $m = 4$ , то  $|N| = 4$ .
4.  $m$  не может быть больше 4.

### Доказательство.

Группа  $G_\alpha$  — транзитивная на  $\Omega \setminus \{\alpha\}$ . Из предыдущего утверждения следует, что  $G_\alpha$  — группа автоморфизмов группы  $N$ . Применяя теорему 13.17, получаем требуемое утверждение.  $\square$

**Определение 13.13.** Группа  $G$  называется *простой*, если она не содержит истинных нормальных делителей.

### Утверждение 13.7.

Пусть  $G$  — примитивная группа и любой нормальный делитель отличный от  $\langle e \rangle$  является нерегулярным, тогда  $G$  является простой группой, если  $G_\alpha$  — простая подгруппа.

### Доказательство.

Пусть  $N \triangleleft G$ ,  $N \neq \langle e \rangle$ . Из примитивности  $G$  следует, что  $N$  транзитивна. Рассмотрим  $N_\alpha = N \cap G_\alpha \triangleleft G_\alpha$ . Из простоты

$G_\alpha$  следует, что  $N_\alpha = \langle e \rangle$ , либо  $N_\alpha = G_\alpha$ . Если  $N_\alpha = \langle e \rangle$ , тогда в силу транзитивности  $N$  — регулярная, что противоречит условию. Пусть  $N_\alpha = G_\alpha$ . Из транзитивности  $N$  вытекает, что

$$|\Omega| = [N : N_\alpha] = [N : G_\alpha] = [G : G_\alpha], \quad \text{т.е. } |N| = |G|.$$

Таким образом,  $N = G$ , то есть  $G$  — простая группа.  $\square$

### Теорема 13.18.

Если  $|\Omega| = n \geqslant 5$ , то  $A_n$  — неабелева простая группа.

*Доказательство.*

Доказательство будем вести по индукции.

- Пусть  $n = 5$  и  $N \triangleleft A_5$ ,  $N \neq \langle e \rangle$ . Так как  $A_5$  — трижды транзитивная, то она дважды транзитивная, следовательно, примитивная, значит и  $N$  — транзитивная на  $|\Omega|$  и  $[N : N_\alpha] = |\Omega| = 5$ . Таким образом, 5 делит  $|N|$ . По теореме Коши существует элемент  $v \in N$  порядка 5. Пусть  $S = \langle v \rangle$  — силовская 5-подгруппа группы  $N$  и  $A_5$  ( $|A_5| = 60$ ). Не ограничивая общности, можно считать, что  $S = \langle v = (12345) \rangle$ . Если  $x = (123)$ , то  $x^{-1}vx = (132)(12345)(132) = (14532) \notin S$ . Таким образом  $S^x = x^{-1}Sx$  — другая силовская 5-подгруппа группы  $N$ . По второй теореме Силова  $S \not\triangleleft N$ . Из третьей теоремы Силова число силовских 5-подгрупп в группе  $N$  равно

$$T = [N : N_N(S)] = 1 + 5k, \quad k = 0, 1, \dots$$

Так как  $k \geqslant 1$  и  $T$  делит  $|N|$ , поэтому  $k = 1$  и  $T = 6$ , значит 30 делит порядок группы  $N$ . Заметим, что  $N$  содержит  $6(5 - 1) = 24$  элемента порядка 5 и, если  $|N| = 30$ , то в  $N$  будут только 6 элементов остальных порядков (1, 2, 3). В силу транзитивности  $N$  получаем соотношение  $30 = |N| = [N : N_\alpha][N_\alpha] = 5|N_\alpha|$ , то есть  $|N_\alpha| = 6 \quad \forall \alpha = 1, 2, 3, 4, 5$ . Поэтому каждое  $N_\alpha$  должно состоять из этих шести элементов, значит

$N_1 = N_2 = N_3 = N_4 = N_5$  или  $N = \langle e \rangle$ . Пришли к противоречию. Значит  $|N| = 60 = |A_5|$ , поэтому  $A_5$  — простая группа.

- Пусть теперь  $n \geq 6$  и  $A_{n-1}$  — простая группа. При  $n \geq 6$  группы  $A_n$  будет четырежды транзитивной и её степень больше 4. Из утверждения 13.6 следует, что любая нормальная подгруппа группы  $A_n$  нерегулярная (в противном случае степень  $A_n$  должна равняться 4.) Далее, если  $\alpha \in \{1, 2, \dots, n\}$ , то  $(A_n)_\alpha \cong A_{n-1}$ . Но группа  $A_{n-1}$  — простая, поэтому, применяя утверждение 13.7, получаем, что  $A_n$  тоже простая.

□

### Теорема 13.19.

$A_n$  ( $n \geq 5$ ) — единственная нормальная погруппа  $S_n$ .

#### Доказательство.

Пусть  $N \triangleleft S_n$  и  $H = (N \cap A_n) \triangleleft A_n$ . Так как  $A_n$  — простая, то  $H = \langle e \rangle$  либо  $H = A_n$ . С другой стороны  $[S_n : A_n] = 2$ . Если  $H = A_n$ , то  $A_n < N$  и из  $N \neq S_n$  следует, что  $N = A_n$ . Пусть теперь  $H = \langle e \rangle$ ,  $N \neq \langle e \rangle$ . Из определения  $H$  следует, что в группе  $N$  существует хотя бы одна нечётная подстановка. Так  $N \triangleleft S_n$  и  $A_n \triangleleft S_n$ , поэтому  $\langle A_n, N \rangle = S_n$  и  $N \cap A_n = \langle e \rangle$ , то  $NA_n = S_n$ , значит  $2|A_n| = S_n = |N||A_n|$ , откуда  $|N| = 2$ . Но  $N$  — транзитивная на  $\Omega$  и  $|N| = |\Omega||N_\alpha| = 5|N_\alpha| \geq 5$ . Противоречие. Теорема полностью доказана. □

**Упражнение 13.21.**  $G, H$  — транзитивные группы на  $\Omega$  и  $H < G$ , тогда для любого  $\alpha \in \Omega$  справедливо соотношение

$$G = G_\alpha H = HG_\alpha.$$

### Теорема 13.20.

Пусть  $G$  — примитивная на  $\Omega$  и  $N \triangleleft G$ ,  $N \neq \langle e \rangle$ ,  $N$  — абелева. Тогда  $N$  — единственная минимальная нормальная подгруппа группы  $G$  и  $\deg(G) = |N| = p^t$  ( $p$  — простое).

**Доказательство.**

Из примитивности  $G$  следует её транзитивность. Так как  $N$  — абелева, то она регулярная и  $Z_G(N) = N$ , следовательно,  $|\Omega| = |N|$ . Пусть  $M \triangleleft G$ ,  $M \neq \langle e \rangle$ , тогда  $(M \cap N) \triangleleft G$  и  $M \cap N$  — абелева группа. Допустим, что  $M \cap N = \langle e \rangle$ . Тогда для любых  $a \in M, b \in N$   $aba^{-1}b^{-1} \in M \cap N = \langle e \rangle$ , то есть  $ab = ba$ . Поэтому  $Z_G(N) > M$ , но  $Z_G(N) = N$ . Пришли к противоречию. Таким образом,  $M \cap N \neq \langle e \rangle$ .

Итак,  $(M \cap N) \triangleleft G$ ,  $M \cap N$  — абелева и транзитивная на  $\Omega$  подгруппа. Следовательно,  $M \cap N$  — регулярная на  $\Omega$  и  $|M \cap N| = |\Omega| = |N|$ . Отсюда получаем, что  $M > N$ , то есть  $N$  — минимальная нормальная подгруппа группы  $G$ .

Покажем, что  $|N| = p^t$ . Разложим  $N$  в прямое произведение своих силовских подгрупп:

$$N = S(p_1) \times \dots \times S(p_k), \quad |S(p_i)| = p_i^{t_i}, \quad |N| = p_1^{t_1} \dots p_k^{t_k}.$$

Так как  $N$  — абелева группа, то  $g^{-1}S(p_i)g = S(p_i)$  для любого  $g \in G$ , то есть  $S(p_i) \triangleleft G$ . Из минимальности  $N$  следует, что  $k = 1$  и, полагая  $t_1 = t$ , получаем  $|N| = p^t$ .

Теорема полностью доказана. □

## 13.6 Базисы симметрической и знакопеременной групп

Пусть  $G$  — конечная группа. Множество  $B = g_1, \dots, g_k$  будем называть базисом или системой образующих группы  $G$ , если  $G = \langle g_1, \dots, g_k \rangle$ , т.е. любой элемент  $g \in G$  может быть представлен в виде

$$g = a_1 \dots a_n, \text{ где } a_i \in B. \quad (13.11)$$

Например, если  $G = S_n = S_\Omega$  и  $\Omega = 0, 1, \dots, n - 1$ , то  $B_0 = \{(ij) \mid 0 \leq i \leq j \leq n - 1\}$  является базисом группы  $S_n$ . Очевидно, что  $|B_0| = \frac{n(n-1)}{2}$ . Если  $G = S_n$  и  $n \geq 3$ , то  $|B| \geq 2$  для любого базиса. Наша основная задача описать

базисы, состоящие из двух перестановок, как для группы  $S_n$ , так и для группы  $A_n$ .

### Лемма 13.2.

Для любого  $n \geq 2$  множество  $\{(0\ 1), (1\ 2), \dots, (n-2\ n-1)\}$  – базис группы  $S_n$ .

#### Доказательство.

Будем вести индукцию по  $n$ . Для  $n=2$  утверждение леммы очевидно справедливо. Пусть мы установили, что

$$\langle(0\ 1), \dots, (n-3\ n-2)\rangle \in S_{n-1}, \quad n \geq 3.$$

Если  $G = \langle(0\ 1), \dots, (n-3\ n-2), (n-2\ n-1)\rangle$ , то  $A_{n-1} < G < S_n$ , следовательно  $(0\ n-2)(n-2\ n-1)(0\ n-2) = (0\ n-1) \in G$ . Поэтому

$$\langle(0\ 1), (0\ 2), \dots, (0\ n-1)\rangle \subset G.$$

Но поскольку,  $(0\ i)(0\ j)(0\ i) = (i\ j)$  для любых  $i \neq j$ ,  $i, j \in \Omega$ , то  $B_0 \subset G$  и  $\langle B_0 \rangle = S_n = G$ .  $\square$

### Теорема 13.21.

Пусть  $n \geq 3$ ,  $k \in \Omega$ ,  $g = (01\dots n-1)$ ,  $h = (k\ k+1)(mod\ n)$ . Тогда  $\langle g, h \rangle = S_n$ .

#### Доказательство.

Из условий теоремы следует, что  $i^g \equiv i + 1(mod\ n)$ ,  $i^{g^{-1}} \equiv i - 1(mod\ n)$ ,  $i < n - 1$ . Поэтому  $i^{g^s} \equiv i + 1(mod\ n)$ ,  $i^{g^{-s}} \equiv i - 1(mod\ n)$  для любого  $s \in \mathbb{Z}$ . Отсюда вытекает, что

$$(ii+1) = g^{k-i}hg^{i-k} \in \langle g, h \rangle, \quad i = 0, 1, \dots, n-2.$$

Из Леммы 13.2 следует, что  $\langle g, s \rangle = S_n$   $\square$

### Лемма 13.3.

Множество  $B_1 = \{(ijk) | 0 \leq i < j < k \leq n-1\}$  базис группы  $A_n$ .

*Доказательство.*

Пусть  $g \in A_n$ . Тогда  $A_n$  может быть представлена в виде произведения четного числа транспозиций:

$$g = (i_1 \ j_1)(i_2 \ j_2) \dots (i_{2t} \ j_{2t}), t \geq 1 \quad (13.12)$$

Расставим скобки в (13.12) следующим образом:

$$g = [(i \ j_1)(i_2 \ j_2)] \dots [(i_{2t-1} \ j_{2t-1})(i_{2t} \ j_{2t})] = h_1 h_2 \dots h_t.$$

Если

$$\{i_{2k-1}, j_{2k-1}\} \cap \{i_{2k}, j_{2k}\} \neq 0,$$

то можно считать, что

$$h_k = (i_{2k-1} \ j_{2k-1})(i_{2k} \ j_{2k}) = (i_{2k-1} \ j_{2k-1})(i_{2k-1} \ j_{2k}),$$

но тогда  $h_k = (i_{2k-1} \ j_{2k-1} \ j_{2k})$  — цикл длины 3.

Если  $(i_{2k-1} \ j_{2k-1}) \cap (i_{2k} \ j_{2k}) = 0$ , то

$$\begin{aligned} h_k &= [(i_{2k-1} \ j_{2k-1})(j_{2k-1} \ i_{2k})][(i_{2k} \ j_{2k-1})(i_{2k} \ j_{2k})] = \\ &= (i_{2k-1} \ i_{2k} \ j_{2k-1})(i_{2k} \ j_{2k-1} \ j_{2k}). \end{aligned}$$

Тем самым  $h_k$  — есть произведение двух циклов. Тем самым справедливость Леммы установлена.  $\square$

**Упражнение 13.22.** Убедиться, что

$$\langle(012)\rangle = A_3 \text{ и } \langle(0 \ 1 \ 2), (1 \ 2 \ 3)\rangle = A_4.$$

**Лемма 13.4.**

Если  $n \geq 3$ , то  $\langle\{(0 \ 1 \ i), i = 2, \dots, n-1\}\rangle = A_n$

*Доказательство.*

Пусть  $H = \langle\{(0 \ 1 \ i) | i = 2, \dots, n-1\}\rangle \subset A_n$ . Так как  $(0 \ 1 \ j)^2 = (0 \ j \ 1) \in H$ , то  $(0 \ 1 \ i)(0 \ j \ 1) = (1 \ i \ j) \in H$ . Следовательно,  $(1 \ i \ j)(1 \ k \ j) = (i \ j \ k) \in H$ . Таким образом любой 3-цикл является элементом группы  $H$ . Согласно Лемме 13.3  $H = A_n$ .  $\square$

**Лемма 13.5.**

$$\langle (0 \ 1 \ 2), \dots, (n-3 \ n-2 \ n-1) \rangle = A_n \text{ при } n \geq 3.$$

*Доказательство.*

Индукцией по  $n$ . Если  $n = 3, 4$ , то утверждение леммы верно, что следует из упражнения 13.22. Пусть  $n > 4$ ,

$$H = \langle (0 \ 1 \ 2), \dots, (n-3 \ n-2 \ n-1) \rangle,$$

и предполагается, что мы уже установили, что

$$\langle (0 \ 1 \ 2), \dots, (n-4 \ n-3 \ n-2) \rangle = A_{n-1} < H.$$

Тогда  $(1 \ n-2)(0 \ n-3) \in A_{n-1}$ , следовательно,

$$(1 \ n-2)(0 \ n-3)(n-3 \ n-2 \ n-1)(1 \ n-2)(0 \ n-3) = (0 \ 1 \ n-1) \in H.$$

Таким образом  $\{(1 \ 2 \ i) | i = 0, \dots, n-1\} \in H$ . Поэтому, из леммы 13.4 следует,  $H = A_n$ .  $\square$

**Теорема 13.22.**

Пусть  $g = (01 \dots n-1)$ ,  $h = (k \ k+1 \ k+2)$ ,  $k \in \Omega$  (сложение по модулю  $n$ ). Тогда если  $n$ -четное (нечетное), то  $\langle g, h \rangle = S_n(A_n)$ .

*Доказательство.*

Рассмотрим 3-цикл  $(i \ i+1 \ i+2)$ ,  $i = 0, \dots, n-3$ . Легко убедиться, что  $(i \ i+1 \ i+2) = g^{k-i}hg^{i-k}$ . Следовательно,  $\{(i \ i+1 \ i+2) | i = 0, \dots, n-3\} \subset \langle g, h \rangle$ . По этому  $\langle g, h \rangle > A_n$ . Далее, если  $n$ -четное, то  $g$  — нечетная подстановка и в этом случае  $\langle g, h \rangle = S_n$ . В противном случае,  $\langle g, h \rangle = A_n$ .  $\square$

**Лемма 13.6.**

Пусть  $n \geq 3$ ,  $k \in \{2, \dots, n-1\}$ ,

$$\mathcal{B} = \{g_i = (i \ i+1 \ \dots \ i+k-1) \mid i = \overline{0, 2, \dots, n-k}\}.$$

Тогда  $\langle \mathcal{B} \rangle = S_n(A_n)$ , если  $k$  — четное (нечетное).

*Доказательство.*

Если  $k = 2$  или  $k = 3$ , то лемма справедлива при любом  $n \geq 3$ . Этот факт следует соответственно из леммы 13.2 и леммы 13.5. Далее доказательство будем вести индукцией по  $r = n - k$ .

I. База индукции  $r = n - k = 1$ ,  $k \geq 4$ ,  $n \geq 5$ . В этом случае  $\mathcal{B} = \{g_0 = (0\ 1\ 2\ \dots\ k-1), g_1 = (1\ 2\ \dots\ k)\}$  и пусть  $H = \langle \mathcal{B} \rangle$ . Непосредственной проверкой убеждаемся, что

$$g_1 g_0^{-1} = (1\ 2\ \dots\ k)(0\ k-1\ k-2\ \dots\ 2\ 1) = (0\ k-1\ k) \in H$$

$$g_1^2 = \begin{pmatrix} 1 & 2 & 3 & \dots & k-2 & k-1 & k \\ 3 & 4 & 5 & \dots & k & 1 & 2 \end{pmatrix},$$

$$g_1^{-2} = \begin{pmatrix} 1 & 2 & 3 & \dots & k-2 & k-1 & k \\ k-1 & k & 1 & \dots & k-4 & k-3 & k-2 \end{pmatrix}.$$

Отсюда получаем

$$g_1^{-2}(0\ k-1\ k)g_1^2 = (0\ 1\ 2) \in H.$$

Из теоремы 13.22 следует, что

$$\langle g_0, (0\ 1\ 2) \rangle = S_k = S_{n-1}(A_{n-1}) \subset H.$$

Поэтому

$$\{(0\ 1\ i) \mid i = \overline{2, n-2}\} \subset H.$$

С другой стороны

$$(0\ 1\ k-1)^{-1}(0\ k-1\ k)^{-1}(0\ 1\ k-1) = (0\ 1\ k).$$

Таким образом,  $\{(0\ 1\ i) \mid i = \overline{2, n-1}\} \subset H$ . И из леммы 13.4 следует, что  $A_n \leq H$ . Поэтому  $H = S_n$ , если  $k$  — четное и  $H = A_n$ , если  $k$  — нечетное.

II. Итак, пусть мы установили справедливость леммы для  $r = n - k$ , где  $r \geq 1$ ,  $k > 3$ . Это индуктивное допущение означает, что

$$H = \langle g_0, g_1, \dots, g_{n-k} \rangle = S_n(A_n),$$

если  $k$  — четное (нечетное). Рассмотрим

$$G = \langle g_0, g_1, \dots, g_{n-k}, g_{n+1-k} \rangle$$

и покажем, что  $G = S_{n+1}(A_{n+1})$ , если  $k$  — четное (нечетное).

Из индуктивного предположения следует, что  $A_n < H < G$ . Поэтому подстановки

$$(0\ 1\ 2), \dots, (0\ 1\ n-1) \in G,$$

$$f = (0\ n-k)(1\ n-1) \in G > A_n,$$

$$h = (n-2\ n-3\ \dots\ n-k+1) \in G > H.$$

Заметим, что  $\deg h = (n-3) - (n-k) + 1 = k-2$ , т.е.  $\deg h$  и  $\deg k$  — числа одной четности.

Далее рассмотрим подстановку

$$\begin{aligned} v = fhg_{n-k+1}f &= (0\ n-k+1)(1\ n-1)(n-2\ n-3\ \dots\ n-k+1) \cdot \\ &\quad \cdot (n-k+1\ n-k+2\ \dots\ n-1\ n)(0\ n-k+1)(1\ n-1). \end{aligned}$$

Непосредственной проверкой убеждаемся, что  $v = (0\ 1\ n)$ , следовательно,  $v \in G$ .

Учитывая, что  $A_n < G$ , получаем

$$\{(0\ 1\ i) \mid i = \overline{2, n}\} \subset G.$$

Следовательно, из леммы 13.4 получаем, что  $A_{n+1} < G$ . Поэтому  $G = S_{n+1}$ , если  $k$  четное или  $A_{n+1}$ , если  $k$  — нечетное.  $\square$

### Теорема 13.23.

Пусть  $n \geq 3$ ,  $k \in (0; n-1)$ ,  $m \in [0; n-1]$ ,

$$g = (0\ 1\ 2\ \dots\ n-1), \quad h = (m\ m+1\ \dots\ m+k-1).$$

Тогда, если  $n, k$  — четные (нечетные), то  $\langle g, h \rangle = S_n(A_n)$ .

*Доказательство.*

Для любого  $i = \overline{0, n-k}$  справедливо соотношение:

$$g_i = (i \ i+1 \ \dots \ i+k-1) = g^{m-i}hg^{i-m}. \quad (13.13)$$

Действительно,

$$\alpha^{g^{m-i}} = \alpha + m - i \pmod{n},$$

$$(\alpha + m - i + 1)^h = \alpha + m - i + 1 \pmod{n},$$

$$(\alpha + m - i + 1)^{g^{i-m}} = \alpha + m - i + 1 + i - m = \alpha + 1.$$

Здесь  $\alpha \in \{i, i+1, \dots, i+k-2\}$ , если  $\alpha = i+k-1$ , то полагаем  $\alpha+1 = i$ .

Из соотношения (13.13) и леммы 13.6 следует справедливость теоремы 13.22.  $\square$

**Упражнение 13.23.** Доказать, что

$$\begin{aligned} \langle (0 \ 1 \ \dots \ n-1), (k \ k+1 \ \dots \ n+1) \rangle &= \\ &= \begin{cases} S_n, & n \cdot k \text{ — четное;} \\ A_n, & n \cdot k \text{ — нечетное,} \end{cases} \text{ где } n-1 > k > 0. \end{aligned}$$

**Следствие 13.4.**

Если  $n \geq 3$ ,  $k \in (0, n-1)$ ,  $i \in [0, k-1]$ , то

$$\begin{aligned} \langle g = (0 \ 1 \ \dots \ k-1), h = (i \ k \ k+1 \ \dots \ n-1) \rangle &= \\ &= \begin{cases} S_n, & n \cdot k \text{ — четное;} \\ A_n, & n \cdot k \text{ — нечетное.} \end{cases} \end{aligned}$$

*Доказательство.*

Положим  $v = g^{-k+i+1}hg^{k-i-1}$ . Далее заметим, что если  $\alpha \in \{0, 1, \dots, k-1\}$ , то

$$\alpha^{g^{-k+i+1}} = \alpha - k + i + 1 = \beta, \quad \beta \neq i,$$

если  $\alpha \neq k-1$ . Поэтому  $\beta^h = \beta$ , если  $\alpha \neq k-1$ . Отсюда следует, что в этом случае

$$\beta^{g^{k-i-1}} = \beta + k - i - 1 = \alpha - k + i + 1 + k - i - 1 = \alpha.$$

Таким образом, если  $\alpha \neq k-1$ , то  $\alpha^v = \alpha$ . Если  $\alpha = k-1$ , то

$$\alpha^{g^{-k+i+1}} = i, \quad i^h = k, \quad k^{g^{k-i-1}} = k.$$

Далее очевидно, что

$$k^v = k^h = k + 1, \quad (k+i)^v = (k+i)^h = k + i + 1.$$

Наконец,

$$(n-1)^v = (n-1)^h = i^{g^{k-i+1}} = i + k - i + 1 = k - 1.$$

Следовательно,

$$v = (k-1 \ k \ \dots \ n-1) \in \langle g, h \rangle.$$

Заметим, что

$$\begin{aligned} v \cdot g &= (k-1 \ k \ \dots \ n-1)(0 \ 1 \ \dots \ k-1) = \\ &= (0 \ 1 \ k-1 \ \dots \ n-2 \ n-1) \in \langle g, h \rangle. \end{aligned}$$

Отсюда и из задачи 13.23 следует справедливость следствия.  $\square$

**Лемма 13.7.**

Пусть  $k \geq 2$ ,  $g_i = (\alpha_i \ \beta_i)$ ,  $i = \overline{1, k}$  и для любого

$$\langle g_1, \dots, g_k \rangle = S^\Omega,$$

где  $\Omega$  – множество элементов, переставляемых транспозициями  $g_i$ .

Тогда

$$\forall i = \overline{1, k-1} \quad \{\alpha_1, \beta_1, \dots, \alpha_i, \beta_i\} \cap \{\alpha_{i+1}, \beta_{i+1}\} \neq \emptyset.$$

*Доказательство.*

Индукция по  $k$ . Если  $k = 1$ , то лемма верна. Пусть  $k > 1$  и допустим, что  $\langle g_1, \dots, g_{k-1} \rangle = G$  — симметрическая группа на множестве тех элементов, которые переставляют транспозиции  $g_i$ ,  $i = \overline{1, k-1}$ . Пусть  $\Gamma = \{\gamma_1 \dots \gamma_t\}$  — множество всех таких элементов. Тогда цикл  $g = (\gamma_1 \dots \gamma_t) \in G = S_\Gamma$ . По условию леммы

$$\{\gamma_1, \dots, \gamma_t\} \cap \{\alpha_k, \beta_k\} \neq \emptyset.$$

Возможны следующие случаи:

$$1. |\{\gamma_1, \dots, \gamma_t\} \cap \{\alpha_k, \beta_k\}| = 1.$$

Пусть, для определенности,

$$\alpha_k = \gamma_i, \quad i = \overline{1, t}, \quad \beta_k = \gamma_{t+1} \notin \Gamma.$$

Тогда подстановки  $g = (\gamma_1 \dots \gamma_t)$  и  $h = (\gamma_i \gamma_{t+1})$  удовлетворяют условиям следствия, и, следовательно,

$$G = S^\Omega, \quad \Omega = \{\gamma_1, \gamma_2, \dots, \gamma_{t+1}\}.$$

$$2. |\{\gamma_1, \dots, \gamma_t\} \cap \{\alpha_k, \beta_k\}| = 2, \text{ т.е.}$$

$$\{\gamma_1, \dots, \gamma_t\} \cap \{\alpha_k, \beta_k\} = \{\alpha_k, \beta_k\}.$$

Но тогда  $\alpha_k \in \Gamma$  и  $\beta_k \in \Gamma$  и очевидно, что

$$G = S^\Gamma = \langle g_1, \dots, g_{k-1} \rangle = \langle g_1, \dots, g_{k-1}, g_k \rangle.$$

□

**Лемма 13.8.**

Пусть  $k \geq 1$ ,  $\{g_i = (\alpha_i \beta_i \gamma_i) \mid i = 1, \dots, k\} = \sum_k u$   
 $\{\alpha_1, \beta_1, \gamma_1, \dots, \alpha_i, \beta_i, \gamma_i\} \cap \{\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}\} \neq \emptyset, \quad i = \overline{1, k-1}$ .

Тогда, если  $\Gamma = \bigcup_{i=1}^k \{\alpha_i, \beta_i, \gamma_i\}$ , то  $G = \langle g_1, \dots, g_k \rangle = A^\Gamma$ .

*Доказательство.*

Если  $k = 1$ , то лемма верна. Допустим, что  $k > 1$  и предположим, что  $\langle \sum_{k-1} \rangle = A^{\Gamma_1} < G$ , где

$$\Gamma_1 = \bigcup_{i=1}^{k-1} \{\alpha_i, \beta_i, \gamma_i\} = \{\delta_1, \delta_2, \dots, \delta_t\}.$$

По условию,

$$\Gamma_1 \cap \{\alpha_k, \beta_k, \gamma_k\} \neq \emptyset.$$

Поэтому возможны следующие случаи:

1.  $\{\alpha_k, \beta_k, \gamma_k\} \subset \Gamma_1$ .

Тогда  $(\alpha_k, \beta_k, \gamma_k) \in A^{\Gamma_1}$ ,  $\Gamma_1 = \Gamma$  и  $G = A^\Gamma$ .

2.  $|\Gamma_1 \cap \{\alpha_k, \beta_k, \gamma_k\}| = 1$ .

Не ограничивая общности можно считать, что

$$\Gamma_1 \cap \{\alpha_k, \beta_k, \gamma_k\} = \alpha_k = \delta_t.$$

Положим  $\beta_k = \delta_{t+1}$ ,  $\gamma_k = \delta_{t+2}$ . Если  $t$  — нечетное, то подстановки  $g = (\delta_1 \dots \delta_t)$  и  $h = (\delta_t \delta_{t+1} \delta_{t+2})$  удовлетворяют условиям следствия. Поэтому

$$\langle g, h \rangle = A^\Gamma, \quad \Gamma = \Gamma_1 \cup \{\delta_{t+1}, \delta_{t+2}\}, \quad G \geq A^\Gamma.$$

Так как, с другой стороны, из определения  $G$  следует, что  $G \leq A^\Gamma$ , то  $G = A^\Gamma$ .

Пусть теперь  $t$  — четное. Тогда  $g = (\delta_2 \dots \delta_t) \in A^\Gamma$  и из следствия вытекает, что  $\langle g, (\delta_t \delta_{t+1} \delta_{t+2}) \rangle = A^{\Gamma \setminus \{\delta_1\}} < G$ .

Следовательно,  $\langle \{(\delta_1 \delta_2 \delta_3), \dots, (\delta_t \delta_{t+1} \delta_{t+2})\} \rangle < G$ .

Поскольку,  $(\delta_1 \delta_2 \delta_3) \in A^{\Gamma_1} < G$ , то по лемме 13.7

$$G = \langle (\delta_1 \delta_2 \delta_3), (\delta_2 \delta_3 \delta_4), \dots, (\delta_t \delta_{t+1} \delta_{t+2}) \rangle = A^\Gamma.$$

3.  $\Gamma_1 \cap \{\alpha_k, \beta_k, \gamma_k\} = \{\delta_i, \delta_j\}$ ,  $1 \leq i < j \leq t$ .

Пусть  $\alpha_k = \delta_i$ ,  $\beta_k = \delta_j$ ,  $\gamma_k = \delta_{t+1}$ . Если  $t$  — четное, то  $g = (\delta_1 \ \delta_2 \ \dots \ \delta_{j-1} \ \delta_{j+1} \ \dots \ \delta_t) \in A^{\Gamma_1}$  и из следствия вытекает, что

$$\langle g, (\delta_t \ \delta_j \ \delta_{t+1}) \rangle = A^\Gamma \leq G.$$

Пусть теперь  $t$  — нечетное. Тогда в силу индуктивного предположения  $t \geq 3$ . Если  $t = 3$ , то

$$(\delta_i \ \delta_j \ \delta_s) \in A^{\Gamma_1} < G, \ \delta_s \in \{\delta_i, \delta_j, \delta_4\}.$$

Поэтому,

$$\langle (\delta_i \ \delta_j \ \delta_s), (\delta_i \ \delta_j \ \delta_4) \rangle = A^\Gamma = A_4.$$

Если  $t > 3$ , то

$$g = (\delta_2 \ \delta_3 \ \dots \ \delta_{j-1} \ \delta_{j+1} \ \dots \ \delta_t) \in A^{\Gamma_1} < G.$$

Из следствия 13.4 получаем

$$\langle g, (\delta_i \ \delta_j \ \delta_{t+1}) \rangle = A^{\Gamma \setminus \{\delta_1\}} < G.$$

Отсюда следует, что

$$\{(\delta_i \ \delta_{i+1} \ \delta_{t+2}) \mid i = \overline{1, t-1}\} \subset G$$

и из предыдущей леммы получим  $G = A^\Gamma$ .

□

**Лемма 13.9.** Пусть  $n \geq 2$  и  $g$  — четная подстановка степени  $n+1$  и  $g \in S_\Gamma$ ,  $\Gamma = \{\alpha_1, \alpha_2, \dots, \alpha_{n+1}\}$ , причем для некоторого  $i \neq n+1$ ,  $\alpha_i^g = \alpha_{n+1}$ .

*Тогда*

$$1. G = \langle g, S^{\Gamma \setminus \{\alpha_{n+1}\}} \rangle = S^\Gamma.$$

$$2. \langle Mg, A^{\Gamma \setminus \{\alpha_{n+1}\}} \rangle = A^\Gamma.$$

*Доказательство.* Докажем эти соотношения.

1. Так как по условию  $\alpha_i^g = \alpha_{n+1}$ , то

$$\alpha_{i-1}^g = \alpha_j, \quad j \in \{1, 2, \dots, n\}$$

и

$$\alpha_j^{g^{-1}(\alpha_{i-1} \alpha_i)g} = \alpha_{i-1}^{(\alpha_{i-1} \alpha_i)g} = \alpha_i^g = \alpha_{n+1}.$$

Следовательно,  $g^{-1}(\alpha_{i-1} \alpha_i)g = (\alpha_{i-1} \alpha_{n+1})$ . Далее, поскольку

$$B = \{(\alpha_1 \alpha_2), (\alpha_1 \alpha_3), \dots, (\alpha_1 \alpha_n), (\alpha_i \alpha_{n+1})\}$$

удовлетворяет условиям леммы 13.7, то

$$\langle g, S^{\Gamma \setminus \{\alpha_{n+1}\}} \rangle = S^\Gamma.$$

2. Рассматривается система подстановок

$$\{(\alpha_1 \alpha_2 \alpha_3), \dots, (\alpha_{n-2} \alpha_{n-1} \alpha_n), (\alpha_{n-1} \alpha_n \alpha_1), \\ (\alpha_n \alpha_1 \alpha_2)\} \subset A^\Gamma.$$

Покажем, что

$$h = g^{-1}(\alpha_{i-2} \alpha_{i-1} \alpha_i),$$

где

$$g = (\alpha_j, \alpha_{k+i}, \alpha_k), \quad j \neq k, \quad j, k \in \{1, 2, \dots, n\}, \quad n \in G.$$

Здесь как и выше  $\alpha_{i-1}^g = \alpha_j$ .

Это следует из того, что подобные подстановки имеют одинаковую цикловую структуру, и справедливости следующих соотношений:

$$\alpha_j^{g^{-1}} = \alpha_{i-1}, \quad \alpha_{i-1}^{(\alpha_{i-2} \alpha_{i-1} \alpha_j)} = \alpha_i, \quad \alpha_i^g = \alpha_{n+1},$$

$$\text{т.е. } \alpha_j^h = \alpha_{n+1}.$$

$$\alpha_{n+1}^{g^{-1}} = \alpha_i, \quad \alpha_i^{(\alpha_{i-2} \alpha_{i-1} \alpha_j)} = \alpha_{i-2}, \quad \alpha_{i-2}^g = \alpha_k, \quad k \neq j.$$

Но система  $B' = B \cup \{(\alpha_j, \alpha_{n+1}, \alpha_k)\}$  удовлетворяет условиям леммы 13.8 и, следовательно,

$$\langle g, A^{\Gamma \setminus \{\alpha_{n+1}\}} \rangle = A^\Gamma.$$

□

### Лемма 13.10.

Пусть  $n > 3$ ,  $g = (0 \ 1 \ 2 \ \dots \ n-1)$ , и для  $\alpha_1, \alpha_2, \alpha_3$  из множества  $\Omega = \{0, 1, 2, \dots, n-1\}$  таких, что  $\alpha_1 < \alpha_2$  и  $\alpha_1 < \alpha_3$

$$h = (\alpha_1 \ \alpha_2 \ \alpha_3).$$

Тогда, если

$$НОД(\alpha_2 - \alpha_1, \alpha_3 - \alpha_1) = k,$$

то

$$(\alpha_1 \ \alpha_1 + k \ \alpha_1 + 2k) \in \langle g, h \rangle.$$

### Доказательство.

Пусть

$$\alpha_2 - \alpha_1 = k_1, \quad \alpha_3 - \alpha_1 = k_2.$$

Не ограничивая общности можно считать  $k_1 > k_2$ . Возможны следующие случаи:

1.  $k_1 = 2k_2$ .

Тогда НОД( $k_1, k_2$ ) =  $k_2 = k$  и

$$\alpha_1 + k = \alpha_1 + k_2 = \alpha_3, \quad \alpha_1 + 2k_2 = \alpha_1 + k_1 = \alpha_2.$$

Поэтому

$$(\alpha_1 \alpha_1 + k \alpha_1 + 2k) = (\alpha_1 \alpha_3 \alpha_2) = (\alpha_1 \alpha_2 \alpha_3)^{-1} \in \langle g, h \rangle.$$

Следовательно, в этом случае лемма верна.

2.  $k_1 \neq 2k_2$ .

Применяя алгоритм Евклида для вычисления

$$k = \text{НОД}(k_1, k_2),$$

будем иметь:

$$\begin{aligned} k_1 &= l_2 k_2 + k_3 & 1 \leq k_3 < k_2, \\ k_2 &= l_3 k_3 + k_4 & 1 \leq k_4 < k_3, \\ &\vdots & \vdots \\ k_{t-2} &= l_{t-1} k_{t-1} + k_t & 1 \leq k_t < k_{t-1}, \\ k_{t-1} &= l_t k_t & k_t = k, \quad t \geq 2. \end{aligned}$$

Рассмотрим подстановки

$$g_i = g^{-ik_2} h g^{ik_2} = (\alpha_1 + ik_2 \quad \alpha_1 + k_1 + ik_2 \quad \alpha_1 + (i+1)k_2),$$

где  $i = \overline{1, l_2}$ , и сложение осуществляется по модулю  $n$ .

Далее заметим, что подстановки  $\{g_1, g_2, \dots, g_{l_2}\}$  — удовлетворяют условиям леммы 13.8 и поэтому

$$\langle g_1, g_2, \dots, g_{l_2} \rangle = A^\Gamma < \langle g, h \rangle,$$

где  $\Gamma$  — множество элементов, переставляемых перестановками  $g_i$ . Отсюда следует, что, в частности,

$$v = (\alpha_1 \quad \alpha_1 + l_2 k_2 \quad \alpha_1 + l_2 k_2 + k_3) \in \langle g, h \rangle.$$

Поэтому

$$v' = g^{-k_3}vg^{k_3} = (\alpha_1 + k_3 \quad \alpha_1 + l_2k_2 + k_3 \quad \alpha_1 + l_2k_2 + 2k_3)$$

принадлежит  $\langle g, h \rangle$  и

$$w = (\alpha_1 + l_2k_2 \quad \alpha_1 + l_2k_2 + k_3 \quad \alpha_1 + l_2k_2 + 2k_3) \in \langle g, h \rangle.$$

Следовательно,

$$g^{l_2k_2}vg^{-l_2k_2} = (\alpha_1 \quad \alpha_1 + k_3 \quad \alpha_1 + 2k_3) \in \langle g, h \rangle.$$

Далее допустим, что мы уже доказали, что 3-цикл

$$d = (\alpha_1 \quad \alpha_1 + k_{m-1} \quad \alpha_1 + 2k_{m-1}) \in \langle g, h \rangle, \quad m > 3.$$

Отсюда следует вывод, что

$$\{h = (\alpha_1 \quad \alpha_1 + k_1 \quad \alpha_1 + k_2), (\alpha_1 \quad \alpha_1 + k_2 \quad \alpha_1 + k_3), \dots, (\alpha_1 \quad \alpha_1 + k_{m-1} \quad \alpha_1 + 2k_{m-1})\} \subset \langle g, h \rangle.$$

Из леммы 13.8 следует, что

$$c = (\alpha_1 \quad \alpha_1 + k_{m-2} \quad \alpha_1 + k_{m-1}) \in \langle g, h \rangle.$$

Рассмотрим следующие 3-циклы:

$$\begin{aligned} f_i &= g^{-ik_{m-1}}cg^{ik_{m-1}} = \\ &= (\alpha_1 + ik_{m-1} \quad \alpha_1 + k_{m-2} + ik_{m-1} \quad \alpha_1 + (i+1)k_{m-1}) \in \langle g, h \rangle, \\ i &= \overline{1, l_{m-1}}, \quad k_{m-1} = l_{m-1}k_{m-1} + k_m. \end{aligned}$$

Из определения  $\{f_i\}$  следует, что

$$\{f_i\} \subset \langle g, h \rangle$$

и система подстановок  $\{f_i\} \cup \{c\}$  — удовлетворяет условиям леммы 13.8. Поэтому

$$\langle\{f_i\} \cup \{c\}\rangle = A^\Gamma \langle g, h \rangle,$$

где  $\Gamma$  — множество элементов, переставляемых подстановками этой системы. Следовательно,

$$\begin{aligned}s &= (\alpha_1 \quad \alpha_1 + l_{m-1}k_{m-1} \quad \alpha_1 + k_{m-2}) = \\ &= (\alpha_1 \quad \alpha_1 + l_{m-1}k_{m-1} \quad \alpha_1 + l_{m-1}k_{m-1} + k_m) \in \langle g, h \rangle\end{aligned}$$

и

$$\begin{aligned}s' &= g^{-k_m} s g^{k_m} = \\ &= (\alpha_1 + k_m \quad \alpha_1 + l_{m-1}k_{m-1} + k_m \quad \alpha_1 + l_{m-1}k_{m-1} + 2k_m)\end{aligned}$$

также принадлежит группе  $\langle g, h \rangle$ . Отсюда следует, что группа  $\langle s, s' \rangle$  является подгруппой  $\langle g, h \rangle$ , а значит циклы

$$\begin{aligned}e &= (\alpha_1 + l_{m-1}k_{m-1} \quad \alpha_1 + l_{m-1}k_{m-1} + k_m \quad \alpha_1 + l_{m-1}k_{m-1} + 2k_m), \\ g^{l_{m-1}k_{m-1}} e g^{-l_{m-1}k_{m-1}} &= (\alpha_1 \quad \alpha_1 + k_m \quad \alpha_1 + 2k_m)\end{aligned}$$

принадлежат  $\langle g, h \rangle$  для любого  $m = 3, \dots, t$ .

В частности, при  $t = m$  получим, что цикл

$$(\alpha_1 \quad \alpha_1 + k_t \quad \alpha_1 + 2k_t) = (\alpha_1 \quad \alpha_1 + k \quad \alpha_1 + 2k) \in \langle g, h \rangle.$$

□

**Теорема 13.24.**

Пусть  $n \geq 4$  и

$$\alpha < \beta < \gamma, \quad \alpha, \beta, \gamma \in \Omega = \{0, 1, \dots, n-2\},$$

$$h = (\alpha \ \beta \ \gamma), \quad g = (0 \ 1 \ 2 \ \dots \ n-1).$$

Тогда если  $n$  — четное (нечетное), то

$$\langle g, h \rangle = S^\Omega (A^\Omega)$$

тогда и только тогда, когда

$$\text{НОД}(\beta - \alpha, \gamma - \beta, n) = 1.$$

*Доказательство.*

**Необходимость.**

Пусть  $\langle g, h \rangle = S_\Omega$  и  $\text{НОД}(\beta - \alpha, \gamma - \beta, n) = r > 1$ . Тогда  $\beta - \alpha = kr$ ,  $\gamma - \beta = mr$ ,  $n = n'r$ . Рассмотрим систему множеств

$$M_i = \{i, i + r, \dots, i + (n' - 1)r\}, \quad i = \overline{0, r - 1}.$$

Очевидно, что

$$M_i^g = \{i + 1, i + 1 + r, \dots, (i + 1) + (n' - 1)r\} = M_{i+1}, \quad i \neq r - 1,$$

$$M_{r-1}^g = M_0.$$

Так как

$$\alpha \equiv \beta \equiv \gamma \pmod{r},$$

то  $\alpha = i_0 + jr$ ,  $\beta = i_0 + sr$ ,  $\gamma = i_0 + tr$ ,  $j < s < t$ . Таким образом,

$$(\alpha \ \beta \ \gamma) = (i_0 + jr \ i_0 + sr \ i_0 + tr).$$

Следовательно,  $M_i^h = M_i$  для любого  $i = \overline{0, r - 1}$ . Из вышеизложенного следует, что множества  $M_0, \dots, M_{r-1}$  являются нетривиальными блоками группы  $\langle g, h \rangle = S_n (A_n)$ . Но поскольку,  $S_n (A_n)$  — примитивные группы, мы пришли к противоречию.

**Достаточность.**

I. Пусть  $\beta - \alpha = \gamma - \beta = k$ .

- Если  $k = 1$ , то  $h = (\alpha \ \alpha+1 \ \alpha+2) \dots (n-1)$  удовлетворяет условию теоремы 13.23 и получим требуемый результат.

2.  $k > 1$ . Так как  $\text{НОД}(k, n) = 1$ , то существуют целые  $m$  и  $t$  такие, что  $mk = 1 + tn$ . Поскольку

$$n = (\alpha \ \beta \ \gamma) = (\alpha \ \alpha + k \ \alpha + 2k),$$

то

$$\begin{aligned} h_j &= g^{-jk}hg^{jk} = \\ &= (\alpha + jk \ \alpha + (j+1)k \ \alpha + (j+2)k) \in \langle g, h \rangle, \\ &\quad j = 1, 2, \dots, 2m-2. \end{aligned}$$

В частности,

$$h_{m-2} = (\alpha + (m-2)k \ \alpha + (2m-1)k \ \alpha + mk),$$

$$h_{2m-2} = (\alpha + (2m-2)k \ \alpha + (2m-1)k \ \alpha + 2mk).$$

Т.к.  $mk = 1 + tn$ , то

$$\alpha + mk = \alpha + 1 + tn \equiv \alpha + 1 \pmod{n},$$

$$\alpha + 2mk - \alpha + 2 + 2tn \equiv \alpha + 2 \pmod{n}.$$

Отсюда следует, что подстановки

$$h = (\alpha \ \alpha + k \ \alpha + 2k), h_1, \dots, h_{m-2}, \dots, h_{2m-2}$$

согласно лемме 13.8 эти перестановки порождают знакопеременную группу. Следовательно,

$$(\alpha \ \alpha + 1 \ \alpha + 2) \in \langle h, h_1, \dots, h_{2m-2} \rangle$$

и по теореме 13.23

$$\langle g, h \rangle = S_n (A_n).$$

II. Пусть  $\beta - \alpha \neq \gamma - \beta$  и  $\text{НОД}(n, r) = r \geq 1$ .

Так как  $\text{НОД}(\beta - \alpha, \gamma - \beta, n) = 1$ , то  $\text{НОД}(n, r) = 1$ . С другой стороны,

$$\text{НОД}(\beta - \alpha, \gamma - \beta) = \text{НОД}(\beta - \alpha, \gamma - \alpha) = r.$$

Поэтому по лемме 13.10 цикл

$$v = (\alpha \alpha + r \alpha + 2r) \in \langle g, h \rangle.$$

Поскольку  $\text{НОД}(n, r) = 1$ , то мы пришли к случаю I.2 и, следовательно,  $\langle g, h \rangle = S_n (A_n)$ .

□

**Теорема 13.25** (С. Пикар). Для любого  $n \geq 3$  и любой  $g \in S_n (g \neq e)$  найдется  $h \in S_n$  такая, что  $\langle g, h \rangle = S_n$ .

*Исключение*

$$g \in K_4 \setminus \{e\} = \{(1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3), \}.$$

**Теорема 13.26.** Для любого  $n \geq 4$  и любой  $g \in A_n, g \neq e$ , найдется  $h \in A_n$  такая, что  $\langle g, h \rangle = A_n$ .

**Упражнение 13.24.** Пусть  $n = 2k, k \geq 4$ ,  $g = (0 \ 1 \ 2 \dots n-1)$ ,  $h = (2 \ 4 \ 6 \dots 2k \ 3 \ 5 \dots 2k-1 \ 1)$ .

Доказать, что  $\langle g, h \rangle = S_n$ .

**Упражнение 13.25.** Пусть  $n = 2k+1, k > 2$ ,  $g = (0 \ 1 \ 2 \dots n-1)$ ,  $h = (1 \ k+2 \ 3k+4 \dots i \ i+k+1 \dots k \ 2k+1 \ k+1 \ 2k+3)$ .

Доказать, что  $\langle g, h \rangle = A_n$ .

## Глава 14

# Эллиптические кривые

### 14.1 Общие понятия и канонические уравнения

Рассмотрим многочлен  $f(x, y)$  от двух переменных степени  $m$  с коэффициентами из поля  $F$ . Уравнение  $f(x, y) = 0$  задаёт алгебраическую кривую  $A_f$ .

Точка  $(x_0, y_0) \in A_f$  называется *неособой*, если хотя бы одна из частных производных  $\frac{\partial f}{\partial x}$  или  $\frac{\partial f}{\partial y}$  в этой точке не обращается в 0.

Если все точки  $A_f$  неособые, то алгебраическая кривая  $A_f$  называется *гладкой*.

*Определение 14.1.* Эллиптической кривой  $\mathcal{E}$  над полем  $F$  называется гладкая кривая, задаваемая уравнением вида:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (14.1)$$

*Определение 14.2.* Две эллиптические кривые называются *изоморфными*, если при допустимой замене координат

$$x = u^2X + r, \quad y = u^3Y + u^2sX + t, \quad u, s, t \in F \quad (14.2)$$

раскрывая скобки и приводя подобные слагаемые, уравнение одной кривой можно привести к уравнению другой.

**Задача 14.1.** Доказать, что множество всех допустимых замен является группой относительно операции композиции преобразований.

**Утверждение 14.1.** Если характеристика поля  $F$  отлична от 2, то эллиптическая кривая, задаваемая уравнением (14.1), изоморфна кривой с уравнением

$$Y^2 = X^3 + \alpha X^2 + \beta X + \gamma \quad \alpha, \beta, \gamma \in F \quad (14.3)$$

*Доказательство.* В левой части уравнения (14.1) выделим полный квадрат:

$$\left(y + \frac{ax + b}{2}\right)^2 - \left(\frac{ax + b}{2}\right)^2 = x^3 + cx^2 + dx + e.$$

Раскроем второй квадрат в левой части полученного равенства, перед этим перенеся его направо:

$$\left(y + \frac{ax + b}{2}\right)^2 = x^3 + \left(c + \frac{a^2}{4}\right)x^2 + \left(d + \frac{ab}{2}\right)x + e + \frac{b^2}{4}.$$

Введём некоторые обозначения:

$$\alpha = c + \frac{a^2}{4}; \quad \beta_4 = d + \frac{ab}{2}; \quad \gamma = e + \frac{b^2}{4}.$$

В новых обозначениях полученное уравнение примет вид:

$$\left(y + \frac{ax + b}{2}\right)^2 = x^3 + \alpha x^2 + \beta x + \gamma.$$

Сделаем замену:

$$X = x; \quad Y = y + \frac{ax + b}{2}.$$

Отметим, что данная замена допустима (сравнить с (14.2)). Очевидно, эта замена приводит к уравнению (14.3)  $\square$

**Утверждение 14.2.** Если характеристика поля  $F$  отлична от 2 и 3, то эллиптическая кривая, задаваемая уравнением (14.1), изоморфна кривой с уравнением

$$Y^2 = X^3 + aX + b \quad a, b \in F \quad (14.4)$$

*Доказательство.* В силу того, что по условию утверждения характеристика поля не равна двум, то эллиптическая кривая изоморфна кривой с уравнением (14.3). В (14.3) сделаем замену переменных (очевидно, она допустима):

$$Y = Y; \quad X = X - \frac{\alpha}{3}.$$

Получим:

$$Y^2 = \left(X - \frac{\alpha}{3}\right)^3 + \alpha \left(X - \frac{\alpha}{3}\right)^2 + \beta \left(X - \frac{\alpha}{3}\right) + \gamma.$$

Раскроем скобки:

$$\begin{aligned} Y^2 = X^3 - \alpha X^2 + \frac{\alpha^2}{3} X - \frac{\alpha^3}{27} + \alpha X^2 - \frac{2\alpha^2}{3} X + \frac{\alpha^3}{9} + \\ + \beta X - \frac{\alpha\beta}{3} + \gamma. \end{aligned}$$

Приведя подобные слагаемые, получим

$$Y^2 = X^3 + \left(\beta - \frac{\alpha^2}{3}\right) X + \frac{2\alpha^3}{27} - \frac{\alpha\beta}{3} + \gamma.$$

Окончательно, полагая

$$a = \beta - \frac{\alpha^2}{3}; \quad b = \frac{2\alpha^3}{27} - \frac{\alpha\beta}{3} + \gamma,$$

приходим к уравнению (14.4) □

**Утверждение 14.3.** Если характеристика поля  $F$  равна 2, то кривая (14.1) изоморфна или кривой вида

$$Y^2 + XY = X^3 + \beta_2 X^2 + \beta_6, \quad \beta_i (i = 2, 6) \in F \quad (14.5)$$

или кривой вида

$$Y^2 + \beta_3 Y = X^3 + \beta_4 X + \beta_6, \quad \beta_i (i = 3, 4, 6) \in F \quad (14.6)$$

*Доказательство.* Предположим, что в уравнении (14.1)  $a_1$  не равно нулю. В этом случае эллиптическая кривая изоморфна кривой, задаваемой уравнением (14.5). Действительно, разделим обе части уравнения на  $a^6$ . Получим

$$\begin{aligned} \left(\frac{y}{a^3}\right)^2 + \left(\frac{x}{a^2}\right)\left(\frac{y}{a^3}\right) + b\left(\frac{y}{a^3}\right) &= \\ &= \left(\frac{x}{a^2}\right)^3 + \frac{c}{a^2}\left(\frac{x}{a^2}\right)^2 + \frac{d}{a^4}\left(\frac{x}{a^2}\right) + \frac{e}{a^6}. \end{aligned}$$

Полагая  $X = \frac{x}{a^2}$ ,  $Y = \frac{y}{a^3}$  (эта замена допустима!), получаем

$$Y^2 + (X + c_3)Y = X^3 + c_2X^2 + c_4X + c_6.$$

Здесь  $c_3 = b$ ,  $c_2 = c/a^2$ ,  $c_4 = d/a^4$ ,  $c_6 = e/a^6$ . Делая допустимую замену  $X = X + c_3$ ,  $Y = Y$ , получаем

$$Y^2 + XY = X^3 + \beta_2X^2 + b_4X + b_6.$$

Где  $\beta_2 = c_3 + c_2$ ,  $b_4 = c_3^2 + c_4$ ,  $b_6 = c_2c_3^2 + c_4c_3 + c_6$ . Окончательно, производя допустимую замену  $X = X$ ,  $Y = Y + b_4$ , получим

$$Y^2 + XY = X^3 + \beta_2X^2 + b_6 + b_4^2.$$

Если положить  $\beta_6 = b_6 + b_4^2$ , то уравнение (14.1) получит вид (14.5).

Пусть теперь в уравнении (14.1) нет слагаемого вида  $xy$ . Тогда сделаем допустимую замену  $x = X + a_2$ ,  $y = Y$ . Легко проверить, что при такой замене уравнение (14.1) приводится к виду (14.6).  $\square$

## 14.2 Дискриминант эллиптической кривой над полем характеристики $p > 3$

Пусть  $\mathcal{E} : y^2 = x^3 + ax + b$  — ЭК над полем  $F = GF(p^4)$ ,  $p > 3$  и  $x_0 \in F$  — корень уравнения:

$$f(x) = x^3 + ax + b = 0. \quad (14.7)$$

Рассмотрим уравнение над полем  $F$ :

$$g(x) = u^2 - x_0 u - \frac{a}{3} = 0. \quad (14.8)$$

Пусть  $\alpha$  и  $\beta$  - его корни, возможно  $\alpha, \beta \notin F$ , но тогда  $\alpha, \beta \in F' \supset F$ , расширению поля  $F'$ . Фактически

$$F' = F[\alpha]/(g(\alpha)),$$

если  $g(x)$  - неприводим над  $F$ .

По теореме Виета:

$$\alpha + \beta = x_0, \quad (14.9)$$

$$\alpha\beta = -\frac{a}{3}. \quad (14.10)$$

Из (14.7) и (14.9) имеем:

$$(\alpha + \beta)^3 + a(\alpha + \beta) + b = 0.$$

Из последнего соотношения получим:

$$\alpha^3 + \beta^3 + (3\alpha\beta + a)(\alpha + \beta) + b = 0.$$

Откуда с учетом (14.10) будем иметь:

$$\begin{cases} \alpha^3 + \beta^3 = -b, \\ \alpha^3\beta^3 = -\frac{a^3}{27}. \end{cases}$$

Заметим, что  $a, b \in F$ , следовательно, по теореме Виета  $\alpha^3$  и  $\beta^3$  - это корни уравнения:

$$z^2 + bz - \frac{a^3}{27} = 0. \quad (14.11)$$

Из (14.11) получаем выражения  $\alpha^3$  и  $\beta^3$  через  $a$  и  $b$ :

$$\alpha^3 = -\frac{b}{2} + \sqrt{\frac{27b^2 + 4a^3}{108}}, \quad \beta^3 = -\frac{b}{2} - \sqrt{\frac{27b^2 + 4a^3}{108}}. \quad (14.12)$$

Таким образом, если  $\frac{27b^2 + 4a^3}{108}$  является квадратичным вычетом в поле  $F$ , то  $\alpha^3$  и  $\beta^3 \in F$ .

$D = 27b^2 + 4a^3$  - это дискриминант эллиптической кривой.

Далее из (14.12) будем иметь:

$$\alpha = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{D}{108}}}, \quad \beta = \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{D}{108}}}.$$

И окончательно, получим формулу Кардано:

$$x_0 = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{D}{108}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{D}{108}}}.$$

**Утверждение 14.4.** Если  $D = 0$ , то (14.7) разрешимо над  $F$  и имеет корни кратности  $r \geq 2$ .

**Доказательство.** Из  $D = 0$  следует, что если  $a = 0$  ( $b = 0$ ), то  $b = 0$  ( $a = 0$ ) и (14.7) примет вид:

$$x^3 = 0.$$

Корень этого уравнения  $x = 0$  имеет кратность 3.

Пусть  $a \neq 0$ ,  $b \neq 0$ . Тогда из  $D = 0$  имеем:

$$-\frac{a}{3} = \frac{9b^2}{4a^2}.$$

Это значит, что  $-\frac{a}{3}$  - квадратичный вычет, следовательно

$f'(x) = 3x^2 + a = 0$  имеет корень  $x = \sqrt{-\frac{a}{3}} = \pm \frac{3b}{2a}$  в поле  $F$ .

Покажем, что  $x_0 = \sqrt{-\frac{a}{3}} = -\frac{3b}{2a}$  является корнем многочлена  $f$ . Действительно:

$$-\frac{27b^3}{8a^3} - \frac{3b}{2} + b = -\frac{b(27b^2 + 4a^3)}{8a^3} = 0.$$

Таким образом,  $x_0$  - корень кратности  $\geq 2$ .

Покажем, что  $x_0$  имеет кратность ровно 2. Допустим, что  $x_0$  кратности 3. Тогда:

$$x^3 + ax + b = (x - x_0)^3 = x^3 - 3x^2x_0 + 3xx_0^2 - x_0^3.$$

Следовательно:

$$\begin{cases} -3x_0 = 0, \\ 3x_0^2 = a, \\ -x_0^3 = b. \end{cases}$$

Т.к. характеристика поля больше 3, то  $x_0 = 0$ , а значит  $a = b = 0$ . Пришли к противоречию.  $\square$

**Утверждение 14.5.** Если  $f(x) = x^3 + ax + b$  имеет кратный корень, то  $D = 0$ .

**Доказательство.** Если кратность  $r = 3$ , то из предыдущего утверждения следует, что  $a = b = 0$ , а значит и  $D = 0$ . Пусть  $r = 2$ , т.е.  $f(x)$  имеет вид:

$$(x - x_0)^2(x - x_1) = 0,$$

Раскроем скобки и приведем подобные:

$$x^3 - x^2(2x_0 + x_1) + x(x_0^2 + 2x_0x_1) - x_1x_0^2 = 0.$$

Отсюда получаем систему:

$$\begin{cases} 2x_0 + x_1 = 0, \\ x_0^2 + 2x_0x_1 = a, \\ -x_1x_0^2 = b. \end{cases}$$

Из этой системы имеем:

$$\begin{cases} x_1 = -2x_0, \\ a = -3x_0^2, \\ b = 2x_0^3. \end{cases}$$

Получаем,  $D = 4a^3 + 27b^2 = -108x_0^3 + 108x_0^3 = 0$ .  $\square$

### 14.3 Группа точек эллиптической кривой над полем характеристики $p > 3$

Пусть  $F$  — конечное поле характеристики  $p > 3$ . Рассмотрим уравнение

$$y^2 = x^3 + ax + b, \quad a, b \in F \quad (14.13)$$

Над полем  $F$  это уравнение определяет эллиптическую кривую. Обозначим через  $\mathcal{E}(a, b)$  множество (точек) всех решений уравнения (14.13) над полем  $F$ , дополненное бесконечно удалённой точкой  $\Theta$ .

**Пример 14.1.**  $F = \mathbb{Z}_7$ ,  $a = 1$ ,  $b = 0$ . Уравнение примет вид:  $y^2 = x^3 + x$ . Подставляя в левую часть этого уравнения элементы из  $\mathbb{Z}_7$ , получим:

$$\mathcal{E}(1, 0) = \{(0; 0), (1; \pm 3), (3; \pm 3), (-2; \pm 2), \Theta\}.$$

**Пример 14.2.**  $F = \mathbb{Z}_7$ ,  $a = b = 1$ . Уравнение (14.13) примет вид:  $y^2 = x^3 + x + 1$ .

$$\mathcal{E}(1, 1) = \{(0; \pm 1), (2; \pm 2), \Theta\}.$$

На множестве  $\mathcal{E}(a, b)$  введём бинарную операцию «сложения» точек эллиптической кривой следующим образом:

1.  $\Theta + P = P + \Theta = P$  для любой точки  $P \in \mathcal{E}(a, b)$
2. Если  $P = (x; y)$ ,  $Q = (x; -y)$ , то  $P + Q = \Theta$ , то есть  $-P = (x; -y)$ .
3. Если  $P = (x_1; y_1)$ ,  $Q = (x_2; y_2)$  и  $x_1 \neq x_2$ , то

$$P + Q = R = (x_3; y_3),$$

где

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \quad (14.14)$$

4. Если  $P = (x_1; y_1)$  ( $y_1 \neq 0$ ), то  $P + P = 2P = (x_3; y_3)$ , где

$$\begin{cases} x_3 = \lambda^2 - 2x_1, \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases} \quad \lambda = \frac{3x_1^2 + a}{2y_1}. \quad (14.15)$$

*Замечание 14.1.* Если  $P = (x; 0) \in \mathcal{E}(a, b)$ , то  $P + P = \Theta$ , то есть  $P = -P$ .

**Утверждение 14.6.** Относительно введённой операции сложения точек множество  $\mathcal{E}(a, b)$  является аддитивной абелевой группой.

*Доказательство.* Покажем корректность введённой операции, то есть, что в результате сложения решений  $P = (x_1; y_1)$  и  $Q = (x_2; y_2)$  уравнения (14.13) мы снова получим некоторое решение (14.13) (либо  $\Theta$ ).

Рассмотрим случай  $x_1 \neq x_2$ . Пусть  $\mathcal{L}(P, Q)$  — множество точек из  $F \times F$ , удовлетворяющих уравнению

$$y = \lambda x + d, \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad d = y_1 - \lambda x_1 \quad (14.16)$$

Геометрически при  $F = \mathbb{R}$  условия (14.16) определяют прямую, проходящую через точки  $P$  и  $Q$ . Покажем, что существует точка  $R' = (x'; y') \in \mathcal{E}(a, b) \cap \mathcal{L}(P, Q)$ , причём  $R' \neq P$  и  $R' \neq Q$ . Подставляя координаты точки  $R = (x; \lambda x + d)$  в (14.13) получим уравнение

$$x^3 - \lambda^2 x^2 + (a - 2\lambda d)x + b - d^2 = 0. \quad (14.17)$$

Так как  $P$  и  $Q$  принадлежат пересечению  $\mathcal{L}(P, Q)$  и  $\mathcal{E}(a, b)$ , то  $x_1$  и  $x_2$  являются корнями уравнения (14.17). Но над полем уравнение третьей степени имеет три корня, и по теореме Виета их сумма равна  $\lambda^2$ . Поэтому существует корень  $x_3 \in F$  такой, что  $x_3 + x_1 + x_2 = \lambda^2$ . Таким образом,  $R' = (x_3; y'_3) \in \mathcal{E}(a, b)$ ,  $x_3 = \lambda^2 - x_1 - x_2$ ,  $y'_3 = \lambda x_3 + y_1 - \lambda x_1$ . Следовательно и точка  $R = (x_3; -y'_3) = (x_3; y_3)$  также принадлежит  $\mathcal{E}(a, b)$ , и тем

самым установлена корректность операции сложения точек эллиптической кривой  $\mathcal{E}(a, b)$ .

Свойство коммутативности введённой операции сложения следует из тождества

$$\frac{y_2 - y_1}{x_2 - x_1} x_1 - y_1 = \frac{y_2 - y_1}{x_2 - x_1} x_2 - y_2.$$

Существование нейтрального элемента и противоположной точки для каждой точки из  $\mathcal{E}(a, b)$  вытекает непосредственно из определения операции сложения точек.

Осталось проверить свойство ассоциативности операции сложения точек эллиптической кривой. Предоставляем это сделать читателю самостоятельно в качестве упражнения.  $\square$

Далее будем рассматривать группу  $\mathcal{E}(a, b)$  над полем  $\mathbb{Z}_p$ ,  $p$  — простое,  $p > 3$ . Один из основных вопросов, возникающих в криптографических приложениях группы  $\mathcal{E}(a, b)$  — это вычисление (оценка) её порядка. Для некоторых  $p$  эта задача решается весьма просто. Воспользуемся следующей теоремой о строении группы  $\mathcal{E}(a, b)$  над полем  $\mathbb{Z}_p$ .

**Теорема 14.1.** Над полем  $\mathbb{Z}_p$  группа  $\mathcal{E}_p(a, b)$  либо циклическая, либо  $\mathcal{E}_p(a, b) \cong \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}$ , где  $N_2 \mid N_1$  и  $N_2 \mid p - 1$ .

**Теорема 14.2.** Если  $p$  — простое и  $p \equiv 2 \pmod{3}$ , то при любом  $b \in \mathbb{Z}_p^*$  порядок группы  $\mathcal{E}_p(0, b)$  равен  $p + 1$  и эта группа циклическая.

**Доказательство.** По условию теоремы  $p = 3t + 2$ , поэтому из  $x_1^3 \equiv x_2^3 \pmod{p}$  следует, что  $x_1^{3t} \equiv x_2^{3t} \pmod{p}$ . Отсюда и из теоремы Ферма ( $x^{p-1} \equiv 1 \pmod{p}$ ) следует, что  $x_1^{-1} \equiv x_2^{-1} \pmod{p}$ , то есть  $x_1 \equiv x_2 \pmod{p}$ . Таким образом, отображение  $\psi: x \rightarrow x^3$  биективно на  $\mathbb{Z}_p$ . Поэтому среди элементов множества  $\{x^3 + b: x \in \mathbb{Z}_p^*, b \neq 0\}$  половина, то есть  $(p - 1)/2$ , является квадратичными вычетами. Это означает, что соответствующие точки  $(x; \pm\sqrt{x^3 + b}) \in \mathcal{E}_p(0, b)$ . Очевидно, что число таких точек равно  $p - 1$ . Из биективности отображения  $\psi$

следует, что точка  $(\sqrt[3]{-b}; 0)$  также принадлежит  $\mathcal{E}_p(0, b)$ . Следовательно, с учётом точки  $\Theta$  порядок группы  $\mathcal{E}_p(0, b)$  равен  $p - 1 + 1 + 1 = p + 1$ . Первая часть утверждения теоремы доказана.

Докажем цикличность группы  $\mathcal{E}_p(0, b)$ . Допустим обратное. Тогда из теоремы о строении группы  $\mathcal{E}_p(a, b)$  следует, что

$$\mathcal{E}_p(a, b) \cong \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2}, \quad p - 1 = N_2 t, \quad N_1 = N_2 s, \quad N_2 \neq 1. \quad (14.18)$$

Отсюда получаем  $N_1 N_2 = p + 1 = N_2 t + 2$ . Следовательно, справедливо соотношение:

$$N_2(N_1 - t) = 2.$$

Поскольку  $N_2 \neq 1$ , то, из полученного ранее соотношения, следует, что

$$N_2 = 2 \text{ и } N_1 = 2s.$$

Отсюда и из (14.18) вытекает, что группа  $\mathcal{E}_p(0, b)$  должна содержать подгруппу четвёртого порядка, изоморфную группе  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , то есть в этой группе имеются, по крайней мере, три элемента порядка 2. Но из первой части доказательства теоремы следует, что  $\mathcal{E}_p(0, b)$  содержит единственную точку второго порядка  $-P = (\sqrt[3]{-b}; 0)$ . (Напомним, что если  $Q = (x; y) \neq \Theta$ , и  $Q = -Q$ , то  $y = -y$ , то есть  $y = 0$ .) Пришли к противоречию. Теорема полностью доказана.  $\square$

**Теорема 14.3.** *Если  $p$  — простое,  $p \equiv 3 \pmod{4}$ , то при любом  $a \in \mathbb{Z}_p^*$  порядок группы  $\mathcal{E}_p(a, 0)$  равен  $p + 1$ . Более того,*

$$\mathcal{E}_p(a, 0) \cong \mathbb{Z}_{p+1}, \text{ если } \left(\frac{a}{p}\right) = 1 \text{ и}$$

$$\mathcal{E}_p(a, 0) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2, \text{ если } \left(\frac{a}{p}\right) = -1.$$

*Доказательство.* Из того, что  $p \equiv 3 \pmod{4}$  следует, что  $\left(\frac{-1}{p}\right) = -1$ . Это означает, что только одно из чисел любой пары  $\{y; -y\}$ ,  $y \in \mathbb{Z}_p^*$  будет являться квадратичным вычетом. Поэтому, если  $f(x) = x^3 + ax$  и  $\left(\frac{a}{p}\right) = 1$ , то для любой пары  $(x; -x)$ ,  $x \in \mathbb{Z}_p^*$  только одно из чисел  $f(x)$  или  $f(-x) = -f(x)$  будет квадратичным вычетом. Этой паре соответствуют две точки — либо  $(x; \pm\sqrt{f(x)})$ , либо  $(-x; \pm\sqrt{-f(x)})$ . Число таких точек будет равно

$$2 \cdot (p-1)/2 = p-1.$$

Заметим, что если  $\left(\frac{a}{p}\right) = 1$ , то условие  $f(x) = f(-x)$  будет выполняться только при  $x = 0$ . Поэтому единственной точкой второго порядка будет точка  $(0; 0)$ . Следовательно, как и в Теореме 14.2 группа  $\mathcal{E}_p(a, 0)$  будет циклической группой порядка  $p+1$  и, следовательно,  $\mathcal{E}_p(a, 0) \cong \mathbb{Z}_{p+1}$ .

Если  $\left(\frac{a}{p}\right) = -1$ , то уравнение  $f(x) = 0$  будет иметь три решения:  $0$  и  $\pm\sqrt{-\frac{1}{a}}$ . Поэтому группа  $\mathcal{E}_p(a, 0)$  будет содержать  $p-2$  точки вида  $(\pm x; \pm\sqrt{\pm f(x)})$  и точки  $(0; 0)$ ,  $(\sqrt{-\frac{1}{a}}; 0)$ ,  $(-\sqrt{-\frac{1}{a}}; 0)$ . Таким образом, и в этом случае порядок группы  $\mathcal{E}_p(a, 0)$  равен  $p+1$ . И поскольку число элементов второго порядка равно, по крайней мере, трём, то  $\mathcal{E}_p(a, 0) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2$ .  $\square$

#### 14.4 Порядок группы $\mathcal{E}_p(a, b)$ с нулевым дискриминантом

**Теорема 14.4.** Если  $4a^3 + 27b^2 = 0$ , то порядок группы  $\mathcal{E}_p(a, b)$  равен одному из чисел  $p$ ,  $p+1$  или  $p+2$ .

*Доказательство.* Из утверждения 14.4 следует, что уравне-

ние (14.13) будет иметь вид:

$$y^2 = (x - x_0)^2(x - x_1). \quad (14.19)$$

Очевидно, что точки  $M_0 = (x_0; 0)$ ,  $M_1 = (x_1; 0)$  принадлежат группе  $\mathcal{E}_p(a, b)$ . Подсчитаем число остальных точек.

В случае, когда  $x_0 = x_1$ , число точек  $\mathcal{E}_p(a, b)$ , отличных от  $M_0$ , равно числу решений уравнения

$$u^2 = x - x_1, \quad x \in \mathbb{Z}_p \setminus \{x_0\}. \quad (14.20)$$

Поскольку число квадратичных вычетов в  $\mathbb{Z}_p$  равно  $(p-1)/2$ , то уравнение (14.20) будет иметь  $p-1$  решений, отличных от  $M_0$ . Таким образом, общее число точек группы  $\mathcal{E}_p(a, b)$  в этом случае равно  $p-1+1+1=p+1$ .

Если  $x_1 \neq x_0$ , то число решений уравнения (14.19) отличных от  $M_0$  и  $M_1$ , равно числу решений уравнения

$$u^2 = x - x_1, \quad x \in \mathbb{Z}_p \setminus \{x_0, x_1\}. \quad (14.21)$$

Если  $\left(\frac{x_0-x_1}{p}\right) = 1$ , то есть  $x_0 - x_1$  — квадратичный вычет, то число решений уравнения (14.21) равно

$$2 \cdot \left( \frac{p-1}{2} - 1 \right) = p-3,$$

и, следовательно, порядок группы  $\mathcal{E}_p(a, b)$  равен  $p-3+2+1=p$ .

И наконец, если  $\left(\frac{x_0-x_1}{p}\right) = -1$ , то есть  $x_0 - x_1$  — квадратичный невычет, то число решений уравнения (14.21) равно

$$2 \cdot \frac{p-1}{2} = p-1.$$

Поэтому порядок группы  $\mathcal{E}_p(a, b)$  будет равен  $p-1+2+1=p+2$ .

□

## 14.5 Элементарные верхние и нижние оценки порядка группы $\varepsilon_p(a, b)$

Пусть, как и раньше, характеристика поля  $F$  больше 3 и  $N(p)$  — число решений уравнения (14.13). Справедливы следующие оценки.

**Теорема 14.5** (Постников А.Г.). *Если  $4a^3 + 27b^2 \neq 0$ , то*

$$\frac{3p+3}{2} \geq N(p) \geq \frac{p-3}{2}.$$

*Доказательство.* Пусть  $f(x) = x^3 + ax + b$ . Рассмотрим многочлен

$$F(x) = 2f(x)(f^{\frac{p-1}{2}}(x) + 1) + f'(x)(x^p - x).$$

Заметим, что  $f'(x) = 3x^2 + a \neq 0$ , поскольку  $4a^3 + 27b^2 \neq 0$ . Степень многочлена  $F(x)$  равна

$$3 + 3 \cdot \frac{p-1}{2} = \frac{3(p+1)}{2}.$$

Далее заметим, что

$$\mathbb{Z}_p = M_0 \cup M_1 \cup M_{-1},$$

где

$$M_0 = \{\alpha \in \mathbb{Z}_p : f(\alpha) = 0\},$$

$$M_1 = \left\{ \alpha \in \mathbb{Z}_p : \left( \frac{f(\alpha)}{p} \right) = 1 \right\},$$

$$M_{-1} = \left\{ \alpha \in \mathbb{Z}_p : \left( \frac{f(\alpha)}{p} \right) = -1 \right\}.$$

Очевидно, что  $|M_0| + |M_1| + |M_{-1}| = p$ . Поэтому

$$N(p) = 2|M_1| + |M_0| = 2p - (2|M_{-1}| + |M_0|). \quad (14.22)$$

Вычислим производную многочлена  $F(x)$ :

$$\begin{aligned} F'(x) &= 2f'(x)(f^{\frac{p-1}{2}}(x) + 1) + (p-1)f(x)f^{\frac{p-3}{2}}(x)f'(x) + \\ &+ f''(x)(x^p - x) - f'(x) = 2f'(x)(f^{\frac{p-2}{2}}(x) + 1) - f^{\frac{p-1}{2}}(x)f'(x) - \\ &- f'(x) + f''(x)(x^p - x) = f'(x)(f^{\frac{p-1}{2}}(x) + 1) + f''(x)(x^p - x). \end{aligned}$$

Заметим, что для  $\beta \in M_{-1}$ ,  $F'(\beta) = 0$ . Следовательно, каждый элемент  $\beta \in M_{-1}$  является корнем многочлена  $F(x)$  кратности не менее двух. С другой стороны, каждый корень  $\gamma \in M_0$  имеет кратность 1. И только элементы из  $M_{-1}$  и  $M_0$  являются корнями многочлена  $F(x)$ . Поэтому имеем:

$$2|M_{-1}| + |M_0| \leq \frac{3(p+1)}{2}. \quad (14.23)$$

Из (14.15) и (14.16) следует, что

$$N(p) \geq 2p - \frac{3(p+1)}{2} = \frac{p-3}{2}.$$

Нижняя оценка установлена. Для доказательства верхней оценки рассмотрим многочлен

$$H(x) = 2f(x)(f^{\frac{p-1}{2}}(x) - 1) - f'(x)(x^p - x).$$

Найдём производную многочлена  $H(x)$ :

$$H'(x) = f'(x)(f^{\frac{p-1}{2}}(x) - 1) - f''(x)(x^p - x).$$

Так как для любого  $\alpha \in M_1$   $H'(\alpha) = 0$ , то  $\alpha$  является корнем многочлена  $H(x)$  кратности не менее двух. С другой стороны, любой элемент  $\gamma \in M_0$  также является корнем многочлена  $H(x)$ . Поэтому из (14.23) следует, что

$$N(p) = 2|M_1| + |M_0| \leq \frac{3(p+1)}{2}.$$

Таким образом, теорема полностью доказана. □

## 14.6 Элементарное доказательство теоремы Хассе

В этом пункте мы докажем основную теорему об оценке числа точек эллиптической кривой — теорему Хассе.

**Теорема 14.6 (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*

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

### Параметризация.

Введём параметр  $t$  и вместо (14.13) будем рассматривать уравнение

$$y^2 = \frac{x^3 + ax + b}{t^3 + at + b}. \quad (14.24)$$

Решения этого уравнения будем искать в области рациональных функций над  $\mathbb{Z}_p$ , то есть если  $(x_0; y_0)$  — решение (14.24) то это означает, что

$$x_0 = \frac{P_1(t)}{Q_1(t)}, \quad y_0 = \frac{P_2(t)}{Q_2(t)}, \quad \text{где } P_i, Q_i \in \mathbb{Z}_p[t].$$

Уравнение (14.24) имеет четыре решения:

$$(t; \pm 1), \quad \left( t^p; \pm (t^3 + at + b)^{\frac{p-1}{2}} \right).$$

Для первой пары точек проверка этого факта очевидна. Справедливость проверки второй пары следует из того, что

$$(A + B)^p \equiv A^p + B^p \pmod{p},$$

$$\text{и } \forall a, b \in \mathbb{Z}_p \quad a^p \equiv a \pmod{p}, \quad b^p \equiv b \pmod{p}.$$

Определим операцию «сложения» решений аналогично операции сложения точек эллиптической кривой. Пусть  $(x_1; y_1)$  и  $(x_2; y_2)$  — некоторые решения. Найдём сначала промежуточное решение  $(x; y)$ , где  $y = \lambda x + d$ ,  $\lambda = (y_2 - y_1)/(x_2 - x_1)$ ,  $d = y_1 - \lambda x_1$ ,  $x_1 \neq x_2$ . Подставим  $y$  в (14.24) и получим

$$x^3 + ax + b - (\lambda(x - x_1) + y_1)^2(t^3 + at + b) = 0.$$

Так как два корня  $x_1$  и  $x_2$  этого уравнения известны, то по теореме Виета находим третий корень из соотношения  $x_1 + x_2 + x'_3 = \lambda^2(t^3 + at + b)$ .

Таким образом, получаем:

$$x'_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 (t^3 + at + b) - x_1 - x_2,$$

$$y'_3 = \lambda(x_3 - x_1) + y_1,$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Из симметрии (14.24) относительно  $y$  следует, что

$$(x_3; y_3) = (x'_3, -y'_3)$$

также будет решением. Это решение мы и будем считать суммой решений  $(x_1, y_1)$  и  $(x_2, y_2)$ .

Итак,

$$(x_1; y_1) + (x_2; y_2) = (x_3; y_3), \text{ где}$$

$$\begin{cases} x_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 (t^3 + at + b) - x_1 - x_2, \\ y_3 = \frac{y_2 - y_1}{x_2 - x_1} (x_1 - x_3) - y_1. \end{cases}$$

Если  $x_1 = x_2 = x$ ,  $y_1 = y_2 = y$ , то положим

$$\lambda = \frac{3x^2 + a}{2y(t^3 + at + b)}$$

и покажем, что, если  $(x; y)$  удовлетворяет уравнению (14.24), то  $(X; Y) = (x; y) + (x; y) = 2(x; y)$ , где

$$\begin{cases} X = \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x, \\ Y = \frac{3x^2 + a}{2y(t^3 + at + b)}(x - X) - y. \end{cases} \quad (14.25)$$

также является решением уравнения (14.24). Так как

$$y^2 = \frac{x^3 + ax + b}{t^3 + at + b},$$

то из (14.25) следует, что

$$Y = \frac{y(3x^2 + a)}{2(x^3 + ax + b)} \left( 3x - \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} \right) - y.$$

Введем обозначения  $A = 3x^2 + a$ ,  $B = x^3 + ax + b$ . В этих обозначениях будем иметь

$$X = \frac{A^2}{4B} - 2x, \quad Y = y \left[ \frac{3Ax}{2B} - \frac{A^3}{8B^2} - 1 \right]. \quad (14.26)$$

Нам нужно установить, что при  $x, y$ , удовлетворяющих (14.24), справедливо равенство:

$$Y^2 = \frac{X^3 + aX + b}{t^3 + at + b}. \quad (14.27)$$

Поскольку  $t^3 + at + b = \frac{x^3 + ax + b}{y^2}$ , то (14.27) равносильно

$$B \cdot Y^2 = X^3 + aX + b \cdot y^2.$$

В последнем равенстве, заменяя  $X$  и  $Y$  по формулам (14.26):

$$B \cdot \left[ \frac{3Ax}{2B} - \frac{A^3}{8B^2} - 1 \right]^2 = \left( \frac{A^2}{4B} - 2x \right)^3 + a \left( \frac{A^2}{4B} - 2x \right) + b.$$

После раскрытия скобок и приведения подобных членов получим:

$$3A^2x^2 - 32Bx^3 - 8aBx + 12ABx + 4Bb - 4B^2 - A^3 + A^2a = 0$$

Далее заметим, что справедливы тождества:

$$3A^2x^2 - A^3 + A^2a = A^2(3x^2 + a - A) = A^2(A - A) = 0$$

$$32Bx^3 + 8aBx - 12ABx - 4Bb + 4B^2 =$$

$$= B(32x^3 + 8ax - 12x(3x^2 + a) - 4b + 4(x^3 + ax + b)) = 0.$$

Следовательно,  $(X; Y)$  — решение уравнения (14.24).

*Замечание 14.2.* Напомним, что  $x, y, X, Y$  — это рациональные функции от переменной  $t$ .

Тем самым полностью показана корректность операции сложения решений (точек) уравнения (14.24).

Можно показать, что множество решений уравнения (2) с введённой операцией сложения точек и дополненное бесконечно удалённой точкой  $\Theta$  является группой.

Построение последовательности решений  $\xi_n = \{(x_n; y_n)\}$ .

Положим  $(x_0; y_0) = \left(t^p; (t^3 + at + b)^{(p-1)/2}\right)$ . Если решение  $(x_n; y_n)$  определено, то положим

$$(x_{n+1}; y_{n+1}) = (x_n; y_n) + (t; 1),$$

$$(x_{n-1}; y_{n-1}) = (x_n; y_n) + (t; -1).$$

Первое из этих равенств позволяет продолжать последовательность решений вправо, а второе — влево. Если в процессе построения последовательности  $\{(x_n; y_n)\}$  вправо получим, что  $(x_n; y_n) = (t; -1)$ , то вместо  $(x_{n+1}; y_{n+1})$  проставляем в последовательность символ  $\star$ , и полагаем

$$(x_{n+2}; y_{n+2}) = (t; 1)$$

идвигаемся вправо далее. Аналогично, если при движении влево получим решение  $(x_n; y_n) = (t; 1)$ , то вместо  $(x_{n-1}; y_{n-1})$  проставляем в последовательность символ  $*$ , полагаем

$$(x_{n-2}; y_{n-2}) = (t; -1)$$

идвигаемся далее.

Таким образом, получим вполне определённую последовательность  $\{\xi_i\}$ , состоящую из решений уравнения (14.24) и, возможно, содержащую символы  $*$ :

$$\dots, \xi_{-n}, \xi_{-n+1}, \dots, \xi_{-1}, \xi_0, \xi_1, \dots, \xi_n, \xi_{n+1} \dots,$$

$$\text{где } \xi_n = \begin{cases} (x_n; y_n), n \in \mathbb{Z}, \\ *. \end{cases}$$

**Построение последовательности  $d = \{d_n\}$ .**

Для любого  $n$ , если  $\xi_n = (x_n; y_n)$  — решение сравнения (14.24), то, не ограничивая общности, можно считать, что

$$x_n = P_n(t)/Q_n(t),$$

где

$$\text{НОД}(P_n(t), Q_n(t)) = 1$$

и старший коэффициент многочлена  $P_n(t)$  равен 1. Далее определим последовательность  $d = \{d_n\}$  следующим образом:

$$d_n = \begin{cases} 0, \text{ если } x_n \text{ не определено,} \\ \deg P_n \text{ в остальных случаях.} \end{cases}$$

Для доказательства теоремы Хассе нам потребуются следующие леммы.

#### Лемма 14.1.

Для любого  $n \in \mathbb{Z}$ , при котором элемент  $\xi_n$  последовательности  $\{\xi_i\}$  определён, выполняется неравенство

$$\deg P_n > \deg Q_n, \tag{14.28}$$

где  $\xi_n = (x_n; y_n)$ ,  $x_n(t) = P_n(t)/Q_n(t)$ .

*Доказательство.*

Будем рассматривать  $x_n(t)$  и  $y_n(t)$  как функции, определённые на множестве  $\mathbb{R}$ . Тогда неравенство (14.28) равносильно условию

$$x_n|_{\infty} = \lim_{t \rightarrow \infty} x_n(t) = \infty. \quad (14.29)$$

Если  $n = 0$ , то (14.29) выполняется, поскольку

$$(x_0; y_0) = \left( t^p; (t^3 + at + b)^{\frac{p-1}{2}} \right).$$

Пусть (14.29) справедливо для некоторого  $n \geq 0$  и элементы  $\xi_n, \xi_{n+1}$  отличны от  $\star$ , то есть  $\xi_{n+1} = (x_{n+1}; y_{n+1})$  и  $\xi_{n+1}$  является решением уравнения (14.29). Тогда

$$y_{n+1}^2 = \frac{x_{n+1}^3 + ax_{n+1} + b}{t^3 + at + b}, \quad (14.30)$$

где  $x_{n+1} = P_{n+1}/Q_{n+1}$ ,  $y_{n+1} = S_{n+1}/T_{n+1}$ . Поэтому если  $y_{n+1}|_{\infty} \neq 0$ , то  $\deg P_{n+1} - \deg Q_{n+1} \geq 1$  и, следовательно,  $x_{n+1}|_{\infty} = \infty$ .

Предположим, что  $y_{n+1}|_{\infty} = 0$ . Из (14.30) следует, что  $x_{n+1}|_{\infty} = c \neq \infty$ . По правилам построения последовательности  $\{\xi_i\}$  имеем:

$$(x_{n+1}; y_{n+1}) = (x_n; y_n) + (t; 1).$$

Отсюда получаем:

$$y_{n+1} = \left( \frac{1 - y_n}{t - x_n} \right) (t - x_{n+1}) - 1.$$

Так как по предположению  $y_{n+1}|_{\infty} = 0$ , то

$$\left( \frac{1 - y_n}{t - x_n} \right) (t - x_{n+1})|_{\infty} = 1.$$

Поскольку  $x_{n+1}|_\infty = c$ , то из последнего соотношения следует

$$\left| \frac{1-y_n}{1-\frac{x_n}{t}} \left( 1 - \frac{x_{n+1}}{t} \right) \right|_\infty = \left| \left( \frac{1-y_n}{1-\frac{x_n}{t}} \right) \right|_\infty = 1 \quad (14.31)$$

По индуктивному предположению  $x_n|_\infty = \infty$ , а значит  $y_n|_\infty \neq 0$ . Поэтому возможны следующие случаи.

А.  $y_n|_\infty = \infty$ . Из (14.31) получаем, что  $\frac{x_n}{t}|_\infty = \infty$ , к тому же

$$\left| \frac{\frac{1}{y_n} - 1}{\frac{1}{y_n} - \frac{x_n}{ty_n}} \right|_\infty = 1, \quad (14.32)$$

и, следовательно,  $\frac{x_n}{ty_n}|_\infty = 1$ . Но тогда

$$\left| \frac{y_n^2 t^2}{x_n^2} \right|_\infty = \left| \frac{t^2 (x_n^3 + ax_n + b)}{(t^3 + at + b)x_n^2} \right|_\infty = \left| \frac{\left( \frac{x_n}{t} \right)^3 + a \left( \frac{x_n}{t} \right) \frac{1}{t^2} + \frac{b}{t^3}}{\left( 1 + \frac{a}{t^2} + \frac{b}{t^3} \right) \left( \frac{x_n}{t} \right)^2} \right|_\infty = 1.$$

Из этого соотношения вытекает, что  $\frac{x_n}{t}|_\infty = 1$ . Пришли к противоречию с (14.32).

Б.  $y_n|_\infty = \varepsilon \neq 0$ . В этом случае из (14.31) немедленно следует, что  $\frac{x_n}{t}|_\infty = \varepsilon$ .

Так как по правилу сложения точек

$$x_{n+1} = -t - x_n + \left( \frac{1-y_n}{t-x_n} \right)^2 (t^3 + at + b),$$

и  $x_{n+1}|_\infty \neq \infty$  то, с учётом (14.31), получим с одной стороны

$$\left| \frac{x_{n+1}}{t} \right|_\infty = 0,$$

а с другой

$$\left| \frac{x_{n+1}}{t} \right|_\infty = \left[ -1 - \frac{x_n}{t} + \left( \frac{1-y_n}{1-\frac{x_n}{t}} \right)^2 \left( 1 + \frac{a}{t^2} + \frac{b}{t^3} \right) \right]_\infty = -\varepsilon \neq 0.$$

Пришли к противоречию. Следовательно,  $y_{n+1}|_\infty \neq 0$  и  $\deg P_{n+1} > \deg Q_{n+1}$ .

Аналогично проводится доказательство при  $n < 0$ .  $\square$

**Основная лемма.**

**Лемма 14.2.**

Для любого  $n \in \mathbb{Z}$  справедливо равенство

$$d_{n-1} + d_{n+1} = 2d_n + 2.$$

*Доказательство.*

Рассмотрим три произвольных элемента

$$\xi_{n-1}, \xi_n, \xi_{n+1}$$

последовательности  $\{\xi_i\}$ . Возможны следующие случаи.

1.  $\xi_n = \star, \xi_{n-1} = (t; -1), \xi_{n+1} = (t; 1)$ .

Согласно правилам построения последовательности  $\{\xi_i\}$  будем иметь:

$$x_{n-1} = t, d_{n-1} = 1, d_n = 0, x_{n+1} = t, d_{n+1} = 1.$$

Поэтому утверждение леммы в этом случае справедливо.

2.  $\xi_{n-1} = \star$ . Тогда  $(x_n; y_n) = (t; 1)$  и

$$(x_{n+1}; y_{n+1}) = (x_n; y_n) + (t; 1) = (t; 1) + (t; 1).$$

Отсюда, на основе правила (14.25) сложения точек, получим

$$x_{n+1} = -2t + \frac{(3t^2 + a)^2}{4(t^3 + at + b)} = \frac{(t^2 - a)^2 - 8bt}{4(t^3 + at + b)},$$

$$\text{НОД}(3t^2 + a, t^3 + at + b) = 1.$$

Таким образом,  $d_{n+1} = 4, d_n = 1, d_{n-1} = 0$ , и в этом случае утверждение леммы справедливо.

3.  $\xi_{n+1} = \star$ . Для этого случая будем иметь  $(x_n; y_n) = (t; -1)$ ,  $(x_{n-1}; y_{n-1}) = (t; -1) + (t; -1)$ . Следовательно, также как и в случае 2,

$$x_{n-1} = \frac{(t^2 - a)^2 - 8bt}{4(t^3 + at + b)}.$$

Поэтому  $d_{n-1} = 4$ ,  $d_n = 1$ ,  $d_{n+1} = 0$ , и утверждение леммы справедливо.

4. Основной случай.  $\xi_k \neq \star$ ,  $k = n-1, n, n+1, n \in \mathbb{Z}$ .

Пусть  $\xi_k = (x_k; y_k)$ ,  $x_k = \frac{P_k}{Q_k}$ ,  $\text{НОД}(P_k, Q_k) = 1$ , и согласно Лемме 14.1  $\deg P_k > \deg Q_k$ . Напомним, что  $x_n$  и  $y_n$  являются решением уравнения (14.24), то есть

$$y_n^2 = \frac{x_n^3 + ax_n + b}{t^3 + at + b} = \frac{P_n^3 + aP_nQ_n^2 + bQ_n^3}{Q_n^3(t^3 + at + b)}. \quad (14.33)$$

*Замечание 14.3.* Из (14.33) следует, что

$$\begin{aligned} y_n^2 Q_n^4 (t^3 + at + b)^2 &= Q_n (P_n^3 + aP_nQ_n^2 + bQ_n^3) \times \\ &\quad \times (t^3 + at + b) \in \mathbb{Z}_p[t]. \end{aligned}$$

Читателю предоставляется доказать в качестве упражнения, что

$$y_n Q_n^2 (t^3 + at + b) \in \mathbb{Z}_p[t]. \quad (14.34)$$

Далее, используя правила сложения точек, получим:

$$\begin{aligned} x_{n-1} &= -t - x_n + \frac{(y_n + 1)^2 (t^3 + at + b)}{(x_n - t)^2} = \\ &= -\frac{tQ_n + P_n}{Q_n} + \frac{(y_n + 1)^2 (t^3 + at + b) Q_n^2}{(tQ_n - P_n)^2}. \end{aligned}$$

После приведения к общему знаменателю получим:

$$x_{n-1} = \frac{-(tQ_n + P_n)(tQ_n - P_n)^2 + (y_n + 1)^2 (t^3 + at + b) Q_n^3}{Q_n (tQ_n - P_n)^2}. \quad (14.35)$$

Если в последнем соотношении раскрыть скобки и использовать соотношение (14.33), то придём к следующей формуле:

$$\begin{aligned} x_{n-1} &= \frac{(P_n + tQ_n)(P_n t + aQ_n) + 2bQ_n^2 + 2y_n Q_n^2 (t^3 + at + b)}{(tQ_n - P_n)^2} = \\ &= \frac{R}{(tQ_n - P_n)^2} = \frac{P_{n-1}}{Q_{n-1}}, \end{aligned} \quad (14.36)$$

где  $P_{n-1} = R/D_1$ ,  $Q_{n-1} = (tQ_n - P_n)^2/D_1$ ,  
 $D_1 = \text{НОД}(R, (tQ_n - P_n)^2)$ .

Эти действия корректны, так как из замечания следует, что  $R \in \mathbb{Z}_p[t]$ .

Аналогично для  $x_{n+1}$  имеем:

$$x_{n+1} = -t - x_n + \left( \frac{y_n - 1}{x_n - t} \right)^2 (t^3 + at + b).$$

Проведя соответствующие замены и преобразования, получим:

$$x_{n+1} = \frac{-(tQ_n + P_n)(tQ_n - P_n)^2 + (y_n - 1)^2 (t^3 + at + b) Q_n^3}{Q_n (tQ_n - P_n)^2} \quad (14.37)$$

$$\begin{aligned} x_{n+1} &= \frac{(P_n + tQ_n)(P_n t + aQ_n) + 2bQ_n^2 - 2y_n Q_n^2 (t^3 + at + b)}{(tQ_n - P_n)^2} = \\ &= \frac{S}{(tQ_n - P_n)^2} = \frac{P_{n+1}}{Q_{n+1}}, \end{aligned} \quad (14.38)$$

где  $P_{n+1} = S/D_2$ ,  $Q_{n+1} = (tQ_n - P_n)^2/D_2$ ,  
 $D_2 = \text{НОД}(S, (tQ_n - P_n)^2)$ .

Из (14.36) и (14.38) после элементарных преобразований получим

$$x_{n-1} \cdot x_{n+1} = \frac{P_{n-1} P_{n+1}}{Q_{n-1} Q_{n+1}} = \frac{(tP_n - aQ_n)^2 - 4bQ_n (tQ_n + P_n)}{(tQ_n - P_n)^2} \quad (14.39)$$

Разложим многочлен  $H(t) = (tQ_n - P_n)^2$  на неприводимые (над  $\mathbb{Z}_p$ ) множители:

$$H(t) = f_1^{r_1} f_2^{r_2} \cdots f_k^{r_k}, \quad \text{НОД}(f_i, f_j) = 1, \text{ при } i \neq j.$$

Из (14.36) и (14.38) следует, что

$$Q_{n-1} = f_1^{\alpha_1} f_2^{\alpha_2} \cdots f_k^{\alpha_k}, \quad Q_{n+1} = f_1^{\beta_1} f_2^{\beta_2} \cdots f_k^{\beta_k}, \quad (14.40)$$

для некоторых  $0 \leq \alpha_i, \beta_i \leq r_i$ .

**Замечание 14.4.** Будем говорить, что многочлен  $f^r$  строго делит многочлен  $G$  (обозначение:  $f^r \parallel G$ ), если  $f^r \mid G$ , но  $f^{r+1} \nmid G$ .

Если мы покажем, что для любого  $f^r = f_i^{r_i}$ ,  $i = \overline{1, k}$  выполняется условие

$$f^r \parallel Q_{n-1} Q_{n+1}, \quad (14.41)$$

то

$$cQ_{n-1} Q_{n+1} = (tQ_n - P_n)^2, \quad c \in \mathbb{Z}_p^*.$$

Но тогда (14.39) можно переписать следующим образом:

$$\frac{P_{n-1} P_{n+1}}{Q_{n-1} Q_{n+1}} = \frac{(tP_n - aQ_n)^2 - 4bQ_n(tQ_n + P_n)}{cQ_{n-1} Q_{n+1}}.$$

Отсюда следует справедливость равенства

$$cP_{n-1} P_{n+1} = (tP_n - aQ_n)^2 - 4bQ_n(tQ_n + P_n),$$

которое с учётом Леммы 14.1 и даёт требуемый результат:

$$\deg P_{n-1} + \deg P_{n+1} = 2 + 2 \deg P_n.$$

Для доказательства выполнения условия (14.41) рассмотрим следующие случаи:

I.  $f \mid R$ , но  $f \nmid S$ .

Из (14.36) и (14.38) следует

$$x_{n-1} = \frac{P_{n-1}}{Q_{n-1}} = \frac{P_{n-1}}{f^\sigma H_1}, \quad \text{где НОД}(f, P_{n-1}) = 1, \quad H_1 \mid H,$$

$$\text{НОД}(H_1, f) = 1, \quad 0 \leq \sigma < r;$$

$$x_{n+1} = \frac{P_{n+1}}{Q_{n+1}} = \frac{P_{n+1}}{f^r H_2}, \text{ где } H_2 \mid H, \text{ НОД}(H_2, f) = 1.$$

Таким образом,  $Q_{n-1} Q_{n+1} = f^{r+\sigma} H_1 H_2$  и

$$x_{n-1} x_{n+1} = \frac{P_{n-1} P_{n+1}}{f^{r+\sigma} H_1 H_2} = \frac{M}{H} = \frac{M}{f^r H_3},$$

то есть

$$P_{n-1} P_{n+1} H_3 = M f^\sigma H_1 H_2.$$

Поскольку,

$$\text{НОД}(P_{n-1}, f) = \text{НОД}(P_{n+1}, f) = \text{НОД}(H_i, f) = 1, i = \overline{1, 3},$$

то последнее соотношение справедливо только в случае, когда  $\sigma = 0$ . Следовательно,  $f^r \parallel Q_{n-1} Q_{n+1}$ .

II.  $f \nmid R$ , но  $f \mid S$ .

Этот случай рассматривается аналогично случаю I.

III.  $f \mid R$  и  $f \mid S$ .

Из (14.35) и (14.37) следует, что

$$f \mid (1 + y_n)^2 (t^3 + at + b) Q_n^3, \quad f \mid (1 - y_n)^2 (t^3 + at + b) Q_n^3.$$

(Под делимостью здесь понимается делимость соответствующего числителя рациональной функции.)

Поэтому

$$f \mid (1 + y_n) (t^3 + at + b) Q_n^3 \text{ и } f \mid (1 - y_n) (t^3 + at + b) Q_n^3$$

и, следовательно, (сложив почленно последние соотношения), получаем:

$$f \mid 2Q_n^3 (t^3 + at + b). \quad (14.42)$$

Так как  $f \mid Q_n t - P_n$ , а  $\text{НОД}(Q_n, P_n) = 1$ , то из (14.42) получим, что  $f \parallel t^3 + at + b$ .

Далее возможны следующие случаи.

A.  $f \nmid (y_n \pm 1)$ .

Тогда из (14.35) и (14.37), с учётом того, что  $f \mid (tQ_n - P_n)^2$  следует, что  $f \parallel R$  и  $f \parallel S$ . Поэтому

$$x_{n-1} = \frac{P_{n-1}}{f^{r-1}H_1}, \quad x_{n+1} = \frac{P_{n+1}}{f^{r-1}H_2}, \quad H = f^r \cdot H_3 = (tQ_n - P_n)^2;$$

$$\text{НОД}(H_i, f) = 1, \quad i = 1, 2, 3.$$

Таким образом, в этом случае  $Q_{n-1}Q_{n+1} = f^{2r-2}H_1H_2$  и

$$x_{n-1} \cdot x_{n+1} = \frac{P_{n-1}P_{n+1}}{f^{2r-2}H_1H_2} = \frac{M}{f^rH_3},$$

т.е.

$$P_{n-1}P_{n+1}H_3 = f^{r-2}H_1H_2M$$

$$\text{НОД}(H_i, f) = \text{НОД}(P_{n-1}, f) = \text{НОД}(P_{n+1}, f) = 1$$

Последнее соотношение возможно тогда и только тогда, когда  $r = 2$ . Следовательно,  $Q_{n-1}Q_{n+1} = f^2H_1H_2$  и

$$f^2 \parallel Q_{n-1}Q_{n+1}.$$

В.  $f \mid (y_n + 1)$ ,  $f \mid (y_n - 1)$

Из этих условий следует, что  $f \mid y_n$ , что невозможно. Таким образом, остается рассмотреть следующий случай.

С.  $f \mid y_n + 1$ ,  $f \nmid y_n - 1$  (случай  $f \nmid y_n + 1$ ,  $f \mid y_n - 1$  рассматривается аналогично).

Из (14.35) и (14.37) с учётом того, что  $f \parallel t^3 + at + b$  и  $f \nmid Q_n$  вытекает, что

$$f \parallel S, \quad f^{2l+1} \parallel (y_n + 1)^2(t^3 + at + b)Q_n^3.$$

С другой стороны, поскольку  $f \nmid y_n - 1$ , то

$$\begin{aligned} f^{2l} \parallel (y_n - 1)^2(y_n + 1)^2 &= (y_n^2 - 1)^2 = \\ &= \left(1 - \frac{x_n^3 + ax_n + b}{t^3 + at + b}\right)^2 = \frac{(t - x_n)^2(t^2 + tx_n + x_n^2 + a)^2}{(t^3 + at + b)^2} = \\ &= \frac{(tQ_n - P_n)^2(t^2 + tx_n + x_n^2 + a)}{Q_n^2(t^3 + at + b)^2} \end{aligned} \quad (14.43)$$

Так как  $f \mid (t - x_n) = (tQ_n - P_n) / Q_n$ , то

$$\begin{aligned} f \mid (t^2 + tx_n + x_n^2 + a) - (3t^2 + a) &= tx_n + x_n^2 - 2t^2 = \\ &= (x_n - t)(x_n + 2t). \end{aligned} \quad (14.44)$$

Отсюда, поскольку  $f \nmid t^3 + at + b$ , то  $f \nmid 3t^2 + a$ . Это следует из того, что  $4a^3 + 27b^2 \neq 0$ . Поэтому из (14.44) вытекает, что  $f \nmid t^2 + tx_n + x_n^2 + a$ . Тогда из (14.43) немедленно следует, что  $2l = r - 2$ ,

$$f^{r-2} \parallel (1 - y_n^2)^2, f^{r-1} \parallel (y_n + 1)^2 (t^3 + at + b) Q_n^3.$$

Поэтому из (14.35) следует, что

$$f^{r-1} \parallel R,$$

и, следовательно

$$x_{n-1} = \frac{P_{n-1}}{f \cdot H_1}, \quad x_{n+1} = \frac{P_{n+1}}{f^{r-1} \cdot H_2}, \quad \text{НОД}(H_i, f) = 1, \quad i = 1, 2.$$

Отсюда получаем, что

$$Q_{n-1} Q_{n+1} = H_1 H_2 f^r.$$

Поэтому

$$f^r \parallel Q_{n-1} Q_{n+1}$$

и основная лемма полностью доказана.  $\square$

### Лемма 14.3.

Если  $N$  – число решений уравнения (14.13), то  $d_{-1} = N + 1$ .

*Доказательство.*

Если

$$m = |\{k \in \mathbb{Z}_p : \left( \frac{k^3 + ak + b}{p} \right) = -1\}|,$$

$$n = |\{l \in \mathbb{Z}_p : l^3 + al + b = 0\}|,$$

то очевидно, что

$$N = 2(p - m) - n. \quad (14.45)$$

Далее определим  $d_{-1}$ . Согласно конструкции последовательности  $(x_n; y_n)$  имеем:

$$(X_{-1}; Y_{-1}) = (x_0; y_0) + (t; -1) = (t^p; (t^3 + at + b)^{\frac{p-1}{2}}) + (t - 1).$$

Поэтому,

$$x_{-1} = \frac{((t^3 + at + b)^{\frac{p-1}{2}} + 1)^2(t^3 + at + b)}{(t^p - t)^2} - t - t^p.$$

Из последнего соотношения после элементарных преобразований получим:

$$\begin{aligned} x_{-1} &= \frac{(t^3 + at + b)^p + 2(t^3 + at + b)^{\frac{p+1}{2}} +}{(t^p - t)^2} \\ &\quad \underline{+ t^3 + at + b - (t^p - t)(t^{2p} - t^2)} \end{aligned}$$

Или в эквивалентной форме.

$$x_{-1} = \frac{t^{2p+1} + (2(t^3 + at + b)^{\frac{p+1}{2}} - t^{p+2} + at^p + at + 2b)}{(t^p - t)^2}.$$

Откуда немедленно следует, что

$$x_{-1} = \frac{t^{2p+1} + R(t)}{(t^p - t)^2} \quad (14.46)$$

Поскольку  $p > 3$ , то из 14.46 следует, что

$$\deg(t^{2p+1} + R(t)) = 2p + 1.$$

После возможных сокращений будем иметь

$$x_{-1} = \frac{t^{2p+1} + R(t)}{(t^p - t)^2} = \frac{P_{-1}(t)}{Q_{-1}(t)}, \quad (P_{-1}(t), Q_{-1}(t)) = 1.$$

Определим  $d_{-1} = \deg P_{-1}(t)$ . Для этого нужно определить степень

$$\text{НОД}([(t^3 + at + b)^{\frac{p-1}{2}} + 1]^2(t^3 + at + b), (t^p - t)^2).$$

Обозначим  $f(t) = (t^3 + at + b)^{\frac{p-1}{2}} + 1$ .

В поле  $\mathbb{Z}_p$  многочлен  $(t^p - t)^2$  разлагается на линейные множители:

$$(t^p - t)^2 = t^2(t - 1)^2 \cdots (t - p + 1)^2.$$

Следовательно, если  $(t - k)^2 | f^2(t)$ , то  $(k^3 + ak + b)^{\frac{p-1}{2}} + 1 = 0$ , а это означает, что  $\left(\frac{k^3 + ak + b}{p}\right) = -1$ .

Заметим, что поскольку  $4a^3 + 27b^2 \neq 0$ , то

$$(t - k)^2 \nmid (t^3 + at + b).$$

Поэтому, если  $(t - k)|(t^3 + at + b)$ , то  $k^3 + ak + b = 0$ .

Следовательно,

$$\deg \left( [(t^3 + at + b)^{\frac{p-1}{2}} + 1]^2(t^3 + at + b), (t^p - t)^2 \right) = 2m + n.$$

Отсюда вытекает, что  $d_{-1} = 2p + 1 - 2m - n$ . С учетом (14.45) имеем, что  $d_{-1} = N + 1$ .  $\square$

#### Лемма 14.4.

Для любого целого  $n$  справедливо соотношение

$$d_n = n^2 - (N - p)n + p.$$

*Доказательство.*

При  $n = -1$  справедливость леммы следует из леммы 14.3.

При  $n = 0$  справедливость следует из определения  $d_0$ .

Предположим, что лемма верна для  $n$  и  $n + 1$  и докажем её для индекса  $n + 2$ . По лемме 14.2 имеем

$$d_n + d_{n+2} = 2d_{n+1} + 2$$

или

$$d_{n+2} = 2d_{n+1} - d_n + 2.$$

Используя индуктивное предположение, получим:

$$d_{n+2} = 2((n+1)^2 - (N-p)(n+1) + p) - n^2 + (N-p)n - p + 2.$$

Упрощая соотношение, получим

$$\begin{aligned} d_{n+2} &= 2(n+1)^2 - n^2 + 2 - (N-p)(n+2) + p = \\ n^2 + 4n + 4 - (N-p)(n+2) + p &= (n+2)^2 - (N-p)(n+2) + p. \end{aligned}$$

Аналогично проводится доказательство «в другую сторону». База индукции такая же, как и в предыдущем случае. И пусть

$$\begin{aligned} d_{-n} &= n^2 - (N-p)(-n) + p \\ d_{-n-1} &= (-n-1)^2 - (N-p)(-n-1) + p \end{aligned}$$

Тогда учитывая, что:

$$d_{-n-2} + d_{-n} = 2d_{-n-1} + 2,$$

будем иметь

$$\begin{aligned} d_{-n-2} &= 2((n+1)^2 - (N-p)(-n-1) + p) - n^2 + \\ + (N-p)(-n) - p + 2 &= 2(n+1)^2 - n^2 + 2 - (N-p)(-n-2) + p = \\ &= (-n-2)^2 - (N-p)(-n-2) + p. \end{aligned}$$

□

### Доказательство теоремы Хассе.

*Доказательство.* Из определения  $d_n$  и Леммы 14.4 следует, что  $d_n = n^2 - (N-p)n + p$  и

$$d_n \geq 0, \forall n \in \mathbb{Z},$$

$$d_n + d_{n+1} \neq 0, \forall n \in \mathbb{Z}.$$

Покажем, что дискриминант  $D = (N-p)^2 - 4p$  этого квадратного трёхчлена не положителен. Допустим противное, то есть пусть  $D > 0$ . Тогда трёхчлен имеет два различных корня  $\alpha$  и  $\beta$ . Возможны следующие варианты расположения чисел  $\alpha$  и  $\beta$  относительно  $n$  и  $n+1$  на числовой оси:

a)  $\alpha = n, \beta = n + 1 - \gamma, 0 < \gamma < 1$ .

Тогда по теореме Виета:  $\alpha + \beta = 2n + 1 - \gamma \notin \mathbb{Z}$ . Противоречие с тем, что  $\alpha + \beta = N - p \in \mathbb{Z}$ .

b)  $\alpha = n + \delta, \beta = n + 1, 0 < \delta < 1$ .

По теореме Виета:  $\alpha + \beta = 2n + 1 + \delta \notin \mathbb{Z}$ .

c)  $\alpha = n + \delta, \beta = n + 1 - \delta, 0 < \delta \leq \frac{1}{2}$ .

По теореме Виета:

$$\alpha\beta = (n + \delta)(n + 1 - \delta) = n^2 + n + \delta(1 - \delta) \notin \mathbb{Z}.$$

d)  $\alpha = n + \delta, \beta = n + 1 - \gamma, \frac{1}{2} \geq \delta > \gamma > 0$ .

По теореме Виета:  $\alpha + \beta = 2n + 1 + \delta - \gamma \notin \mathbb{Z}$ .

Таким образом, получаем, что  $(N - p)^2 - 4p \leq 0$ , то есть  $|N - p| \leq 2\sqrt{p}$ . Теорема Хассе доказана.  $\square$

В случае кривых над непростыми конечными полями формулу для числа точек на этих кривых можно получить с помощью теоремы Хассе—Вейля.

**Теорема 14.7** (Хассе—Вейль). *Пусть  $G$  — группа точек эллиптической кривой над полем  $GF(q)$ ;  $G_n$  — группа точек той же кривой над полем  $GF(q^n)$ . Тогда  $|G_n| = q^n + 1 - (\alpha^n + \beta^n)$ , где  $\alpha, \beta$  — корни уравнения  $x^2 + tx + q = 0$ ,  $t = q + 1 - |G|$ .*

Доказательство этой теоремы менее элементарно, чем доказательство теоремы Хассе, и поэтому оно здесь не приводится.

## 14.7 Эллиптические кривые над полем характеристики 3

Напомним, что общее уравнение эллиптической кривой (ЭК)  $\mathcal{E}$  над конечным полем имеет вид:

$$\mathcal{E}: y^2 + Axy + By = x^3 + Cx^2 + Dx + E. \quad (14.47)$$

Если характеристика поля  $\neq 2$ , то уравнение (14.47) заменой  $X = x$ ,  $Y = y + Ax/2 + B/2$  приводится к виду:

$$\mathcal{E} : Y^2 = X^3 + aX^2 + bX + c. \quad (14.48)$$

Сложение точек ЭК определяется стандартным образом. Как обычно полагаем, если  $(x, y) \in \mathcal{E}$ , то  $-(x, y) = (x, -y)$ . Если  $(x_1, y_1), (x_2, y_2) \in \mathcal{E}$  и  $x_1 \neq x_2$ , то полагаем  $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ , где

$$\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases} \quad (14.49)$$

$$\text{где } \lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Покажем, что  $(x_3, y_3) \in \mathcal{E}$ . Рассмотрим систему:

$$\begin{cases} y^2 = x^3 + ax^2 + bx + c, \\ y = \lambda x + d, \\ d = y_1 - \lambda x_1. \end{cases} \quad (14.50)$$

Т.к.  $y = \lambda x + d$  — это уравнение прямой, проходящей через точки  $(x_1, y_1)$  и  $(x_2, y_2)$ , то эти точки удовлетворяют системе (14.50). Подставляя  $y = \lambda x + d$  в первое уравнение системы (14.50), получим уравнение:

$$x^3 - (\lambda^2 - a)x^2 + (b - 2\lambda d)x + c - d^2 = 0. \quad (14.51)$$

Т.к.  $x_1$  и  $x_2$  — корни уравнения (14.51), то по теореме Виета это краинение имеет корень  $x_3 = \lambda^2 - a - x_1 - x_2$ . Из системы (14.50) следует, что точка  $(x_3, \tilde{y}_3)$  является решением этой системы. Здесь  $\tilde{y}_3 = \lambda x_3 + y_1 - \lambda x_1$ . Но тогда точка  $(x_3, -\tilde{y}_3) = (x_3, \lambda(x_1 - x_3) - y_1) = (x_3, y_3) \in \mathcal{E}$ .

В случае  $x_1 = x_2 = x$ ,  $y \neq 0$  полагаем

$$\lambda = -\frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}} = \frac{2ax + b}{2y} = \frac{-ax + b}{-y} = \frac{ax - b}{y},$$

где  $F(x, y) = y^2 - x^3 - ax^2 - bx - c$ . Тогда, если  $2(x, y) = (X, Y)$ , то полагаем:

$$\begin{cases} X = \lambda^2 - a - 2x = \lambda^2 + x - a, \\ Y = \lambda(x - X) - y, \end{cases} \quad (14.52)$$

$$\text{где } \lambda = \frac{ax - b}{y}.$$

Убедимся, что  $(X, Y) \in \mathcal{E}$ . Из (14.52) имеем:

$$\lambda y = ax - b, \quad X = \lambda^2 + x - a, \quad (14.53)$$

следовательно

$$X^2 = \lambda^4 + x^2 + a^2 - \lambda^2 x + \lambda^2 a + ax. \quad (14.54)$$

Из (14.53) и (14.54) получим:

$$\begin{aligned} Y^2 &= (\lambda x - \lambda X - y)^2 = \lambda^2 x^2 + \lambda^2 X^2 + y^2 + \lambda^2 x X + \lambda x y - \lambda X y = \\ &= y^2 + \lambda^2 X^2 + \lambda^2 x^2 + \lambda^2 x(\lambda^2 + x - a) + x(ax - b) - (ax - b)(\lambda^2 + x - a) = \\ &= y^2 + \lambda^2 X^2 + \lambda^2 x^2 + \lambda^4 x + \lambda^2 x^2 - a\lambda^2 x + ax^2 - bx - ax^2 - a\lambda^2 x + a^2 x + \\ &\quad + b\lambda^2 + bx - ab. \end{aligned}$$

Отсюда следует, что

$$Y^2 = y^2 + \lambda^2 X^2 - \lambda^2 x^2 + x(\lambda^4 + a\lambda^2 + a^2) + b\lambda^2 - ab. \quad (14.55)$$

С другой стороны из (14.53), имеем:

$$\begin{aligned} X^3 + aX^2 + bX + c &= X^2(\lambda^2 + x - a) + aX^2 + b(\lambda^2 + x - a) + c = \\ &= \lambda^2 X^2 + x(\lambda^4 + x^2 + a^2 - \lambda^2 x + \lambda^2 a + ax) + b\lambda^2 + bx - ab + c = \\ &= \lambda^2 X^2 - \lambda^2 x^2 + x(\lambda^4 + a^2 + a\lambda^2) + b\lambda^2 - ab + x^3 + ax^2 + bx + c. \end{aligned}$$

Учитывая, что  $(x, y) \in \mathcal{E}$  и, следовательно,  $y^2 = x^3 + ax^2 + bx + c$ , из (14.55) вытекает, что  $Y^2 = X^3 + aX^2 + bX + c$ , т.е.  $(X, Y) = 2(x, y) \in \mathcal{E}$ .

**Пример 14.3.** Рассмотрим ЭК  $\mathcal{E}$ , заданную уравнением

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

над полем  $F = GF(3^3) = \mathbb{Z}_3[\theta]/\theta^3 + 2\theta + 1$ . Сначала найдем все точки  $\mathcal{E}$ . Для этого построим следующие таблицы. Напомним, что элементы поля  $F$  можно рассматривать как многочлены степени не больше 2 с коэффициентами из поля  $\mathbb{Z}_3$ . С другой стороны, элементы  $F^*$  — это степени примитивного корня  $\theta$  многочлена  $x^3 - x + 1$ .

Таблица 13.1 строится на основе соотношения:  $\theta^3 = \theta - 1$ .

Таблица 13.1 представления элементов поля  
 $F = GF(3^3) = \mathbb{Z}_2(\theta^3)/\theta^3 - \theta + 1$  через степень примитивного корня  $\theta$ .

$\theta^3$	$\theta^4$	$\theta^5$	$\theta^6$	$\theta^7$	$\theta^8$
$\theta - 1$	$\theta^2 - \theta$	$-\theta^2 + \theta - 1$	$\theta^2 + \theta + 1$	$\theta^2 - \theta - 1$	$-\theta^2 - 1$

$\theta^9$	$\theta^{10}$	$\theta^{11}$	$\theta^{12}$	$\theta^{13}$
$\theta + 1$	$\theta^2 + \theta$	$\theta^2 + \theta - 1$	$\theta^2 - 1$	$-1$

$$\theta^{13+k} = -\theta^k, k = \overline{1, 13}.$$

Таблица 13.2 значений многочлена  $f(x) = x^3 + 2x + 1$ .

$x$	0	1	-1	$\theta$	$-\theta$	$\theta^2$	$-\theta^2$	$\theta^3$	$-\theta^3$	$\theta^4$
$f(x)$	1	1	1	0	-1	$\theta^3$	$\theta^{14}$	0	-1	$\theta$

$x$	$-\theta^4$	$\theta^5$	$-\theta^5$	$\theta^6$	$-\theta^6$	$\theta^7$	$-\theta^7$	$\theta^8$	$-\theta^8$
$f(x)$	$\theta^{22}$	$\theta^{22}$	$\theta^3$	$\theta^9$	$\theta^{16}$	$\theta$	$\theta^{22}$	$\theta^{14}$	$\theta^3$

$x$	$\theta^9$	$-\theta^9$	$\theta^{10}$	$-\theta^{10}$	$\theta^{11}$	$-\theta^{11}$	$\theta^{12}$	$-\theta^{12}$
$f(x)$	0	-1	$\theta^9$	$\theta^{16}$	$\theta^9$	$\theta^{16}$	$\theta^3$	$\theta^{14}$

Из таблиц 13.1 и 13.2 следует, что

$$\mathcal{E} : y^2 = x^3 + 2x + 1 \text{ над } F = GF(27).$$

$$\begin{aligned}\mathcal{E} = \{ & \Theta, (0, \pm 1), (1, \pm 1), (-1, \pm 1), (\theta, 0), (\theta^3, 0), (\theta^9, 0), \\ & (-\theta^2, \pm \theta^7), (-\theta^4, \pm \theta^{11}), (\theta^5, \pm \theta^{11}), (-\theta^6, \pm \theta^8), \\ & (-\theta^7, \pm \theta^{11}), (-\theta^{12}, \pm \theta^7), (\theta^8, \pm \theta^7), (-\theta^{10}, \pm \theta^8), (-\theta^{11}, \pm \theta^8) \}.\end{aligned}$$

$$\#\mathcal{E} = 1 + 3 + 2 \cdot 12 = 28.$$

По теореме Хассе—Вейля

$$N(1) = 7, \quad N(3) = 3^3 + 1 - (\alpha^3 + \beta^3) = 28,$$

$$t = q + 1 - N(1) = 3 + 1 - 7 = -3, \quad \alpha - \beta = q = 3, \quad \alpha + \beta = -3,$$

$$\alpha^3 + \beta^3 = (\alpha + \beta)[(\alpha + \beta)^2 - 3\alpha\beta] = -3[9 - 9] = 0.$$

Из описания группы  $\mathcal{E}$  следует, что  $\mathcal{E} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7$ . Действительно, так как  $\mathcal{E}$  содержит 3 элемента 2-го порядка, то силовская 2-группа  $P(2)$  группы  $\mathcal{E}$ , имеющая порядок 4 ( $\#\mathcal{E} = 28$ ) изоморфна  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Из основной теоремы об абелевой группе вытекает требуемый результат.

**Пример 14.4.** Определить порядок  $T$  точки  $M_1 = (-\theta^2, \theta^7)$ .

Порядок  $T \in \{2, 4, 7, 14\}$ .

Т.к.  $-M_1 = (-\theta^2, -\theta^7) \neq M_1$ , то  $T \neq 2$ .

Вычислим  $2M_1 = (x_2, y_2)$ . Из системы (14.52), учитывая, что  $a = 0, b = -1, x = \theta^2, y = \theta^7$ , находим:

$$\lambda = \frac{1}{\theta^7},$$

$$x_2 = \theta^{38} - \theta^2 = \theta^{12} - \theta^2 = \theta^2 - 1 - \theta^2 = -1,$$

$$y_2 = \theta^{19}(-\theta^2 + 1) - \theta^7 = \theta^8 - \theta^6 - \theta^7 = -\theta^2 - 1 - \theta^2 - \theta - 1 - \theta^2 + \theta + 1.$$

Таким образом,  $2M_1 = (-1, -1)$ . Но точка  $2M_1$  имеет порядок 7 следовательно,  $or(M_1) = T = 14$ .

**Пример 14.5.** Найти координаты точки

$$M_3 = (x_3, y_3) = (-\theta^4, \theta^{11}) + (\theta^8, \theta^7)$$

Из системы (14.14) следует, что

$$\begin{aligned} \lambda &= \frac{\theta^7 - \theta^{11}}{\theta^8 + \theta^4} = \frac{\theta^2 - \theta - 1 - \theta^2 - \theta + 1}{-\theta^2 - 1 + \theta^2 - \theta} = \\ &= \frac{\theta}{-\theta - 1} = -\frac{\theta}{\theta^9} = -\frac{1}{\theta^8} = \theta^5, \end{aligned}$$

$$\lambda^2 = \theta^{10}, \quad x_3 = \theta^{10} + \theta^4 - \theta^8 = \theta^2 + \theta + \theta^2 - \theta + \theta^2 + 1 = 1,$$

$$\begin{aligned} y_3 &= \theta^5(-\theta^4 - 1) - \theta^{11} = -\theta^9 - \theta^5 - \theta^{11} = \\ &= -\theta - 1 + \theta^2 - \theta + 1 - \theta^2 - \theta + 1 = 1, \end{aligned}$$

$$M_3 = (1, 1).$$

**Задача 14.2.** Доказать, что порядок группы ЭК  $y^2 = x^3 + a$  над полем  $F = GF(3^n)$  при любом  $a \in F$  равен  $3^n + 1$ .

**Задача 14.3.** Доказать, что порядок группы ЭК  $y^2 = x^3 + ax$  над полем  $F = GF(3^{2k+1})$  равен  $3^{2k+1} + 1$  при любом  $a \in F^*$ .

## 14.8 Эллиптические кривые над полем характеристики 2

### 14.8.1 Группа точек суперсингулярной кривой

Каноническое уравнение суперсингулярной кривой имеет вид:

$$y^2 + ey = x^3 + ax + b \tag{14.56}$$

Пусть  $P = (x_0, y_0)$  удовлетворяет уравнению (14.56). Покажем, что точка  $Q = (x_0, y_0 + e)$  также удовлетворяет (14.56).

Это следует из следующего соотношения:

$$(y_0 + e)^2 + e(y_0 + e) = y_0^2 + e^2 + ey_0 + e^2 = y_0^2 + ey_0.$$

Поэтому полагаем  $-(x_0, y_0) = (x_0, y_0 + e)$ .

**Замечание 14.1.**  $P = -P$  тогда и только тогда, когда  $e = 0$ . В этом случае  $\mathcal{E}$  - элементарная абелева 2-группа.

Далее, как и ранее, пусть

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad x_1 \neq x_2, \quad \lambda = \frac{y_1 + y_2}{x_1 + x_2}, \quad d = \lambda x_1 + y_1.$$

Точки  $P_1$  и  $P_2$  являются решением (14.56).

Подставим координаты точки  $P = (x, \lambda x + d)$  в (14.56). В результате получим:

$$(\lambda x + d)^2 + e(\lambda x + d) = x^3 + ax + b.$$

Раскрывая скобки и приводя подобные члены будем иметь:

$$x^3 + \lambda^2 x^2 + x(e\lambda + a) + d^2 + ed + b = 0. \quad (14.57)$$

Из выбора точки  $P$  следует, что  $x_1$  и  $x_2$  - корни уравнения (14.57). Поэтому из теоремы Виета следует, что  $x_3 = \lambda^2 + x_1 + x_2$  тоже корень уравнения (14.57). Таким образом  $P = (x_3, \lambda x_3 + d)$  удовлетворяет уравнению (14.56), а следовательно, и точка  $-P = (x_3, \lambda x_3 + d + e)$  также удовлетворяет уравнению (14.56). Положим  $P_1 + P_2 = -P$ .

Таким образом, если  $x_1 \neq x_2$ , то

$$\begin{cases} x_3 = \lambda^2 + x_1 + x_2, \\ y_3 = \lambda(x_1 + x_3) + y_1 + e, \quad \lambda = \frac{y_2 + y_1}{x_2 + x_1}. \end{cases} \quad (14.58)$$

Пусть теперь

$$x_0 = x_1 = x_2, \quad y_0 = y_1 = y_2, \quad 2(x_0, y_0) = (x, y), \quad e \neq 0,$$

$$f(x, y) = y^2 + ey + x^3 + ax + b.$$

Найдем

$$\lambda = \left. \frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}} \right|_{(x_0, y_0)} = \frac{x_0^2 + a}{e}.$$

Как и в предыдущем случае подставим координаты точки  $P = (x, \lambda x + d)$ ,  $d = \lambda x_0 + y_0$  в уравнение (14.56) и по теореме Виета найдем координаты точки  $P$ :

$$x = \lambda^2 + 2x_0 = \lambda^2, \quad y = \lambda(x + x_0) + y_0.$$

В качестве точки  $2(x_0, y_0)$  возьмем точку  $-P = (x, y+e)$ . Таким образом координаты  $(x, y)$  удвоенной точки  $(x_0, y_0)$  суперсингулярной эллиптической кривой вычисляются по формулам:

$$\begin{cases} x = \lambda^2 \\ y = \lambda(x_0 + x) + y_0 + e, \quad \lambda = \frac{x_0^2 + a}{e}. \end{cases} \quad (14.59)$$

**Упражнение 14.1.** Доказать, что если  $e \neq 0$ , то порядок суперсингулярной кривой — нечетное число.

**Упражнение 14.2.** Доказать, что если  $e = a = b = 1$ , то

$$2(x_0, y_0) = (x_0^4 + 1, x_0^4 + y_0^4).$$

*Решение.* Если  $e = a = b = 1$ , то  $\lambda = x_0^2 + 1$ ,  $\lambda^2 = x_0^4 + 1$ . Из (14.59) имеем:

$$y = (x_0^2 + 1)(x_0^4 + 1 + x_0) + y_0 + 1 = x_0^6 + x_0^2 + x_0^3 + x_0^4 + 1 + x_0 + y_0 + 1.$$

Так как,  $y_0^2 + y_0 = x_0^3 + x_0 + 1$ , то из последнего соотношения получим:

$$\begin{aligned} y &= (y_0 + x_0^3 + x_0 + 1) + (x_0^6 + x_0^2 + 1) + x_0^4 = \\ &= y_0^2 + y_0^4 + y_0^2 + y_0^2 + x_0^4 = x_0^4 + y_0^4. \end{aligned}$$

□

**Упражнение 14.3.** Описать группу точек эллиптической кривой  $\mathcal{E}_1$  над полем  $GF(2)$ , заданной уравнением:

$$\mathcal{E}_1 : y^2 + y = x^3 + x.$$

Ответ:  $\mathcal{E}_1 = \{(0, 0), (0, 1)(1, 0), (1, 1), \Theta\}$ ,  $|\mathcal{E}_1| = 5$ .

**Пример 14.6.** Найти порядок  $N_3$  кривой  $\mathcal{E}_1$  над полем  $GF(8)$ . Применим теорему Хассе—Вейля

$$N_3 = 2^3 + 1 - (\alpha^3 + \beta^3), \quad t = q + 1 - N_1 = 3 - 5 = -2, \quad q = 2,$$

$$\alpha^3 + \beta^3 = -t(t^2 - 3q) = 2(4 - 6) = -4,$$

$$N_3 = 9 + 4 = 13,$$

$$\mathcal{E}_1(GF(8)) = 13.$$

**Упражнение 14.4.** Найти порядок  $N_2$  кривой  $\mathcal{E}_1$  над полем  $GF(4)$ .

Ответ:  $\mathcal{E}_1(GF(4)) = \mathcal{E}_1(GF(2)) = 5$ .

**Упражнение 14.5.** Найти порядок  $N_4$  кривой  $\mathcal{E}_1$  над полем  $GF(16)$ .

Ответ:  $N_4 = 25$ .

**Пример 14.7.** Рассмотрим кривую:

$$\mathcal{E}_2 : y^2 + \theta y = x^3 + x + \theta + 1,$$

над полем  $F_4 = \{0, 1, \theta, \theta + 1\}$ ,  $(\theta^2 = \theta + 1)$ .

Составим таблицу:

$x$	0	0	0	0
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta y$	0	$\theta + 1$	0	$\theta + 1$
$x^3 + x + \theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$

$x$	1	1	1	1
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta y$	0	$\theta + 1$	0	$\theta + 1$
$x^3 + x + \theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$

\*

\*

$x$	$\theta$	$\theta$	$\theta$	$\theta$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta y$	0	$\theta + 1$	0	$\theta + 1$
$x^3 + x + \theta + 1$	0	0	0	0

\*

\*

$x$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta y$	0	$\theta + 1$	0	$\theta + 1$
$x^3 + x + \theta + 1$	1	1	1	1

Из таблицы получаем

$$\mathcal{E}_2 = \{\Theta, (0, 1), (0, \theta + 1), (1, 1), (1, \theta + 1), (\theta, 0), (\theta, \theta)\}.$$

Порядок  $|\mathcal{E}_2| = 7$ , т.е.  $\mathcal{E}_2$  — циклическая.

**Упражнение 14.6.** Найти порядок  $\mathcal{E}_2$  над полем  $GF(16)$ .

**Ответ:** Группа  $\mathcal{E}_2$  над  $GF(16)$  — циклическая порядка 21.

**Упражнение 14.7.** Описать группу точек кривой над полем  $F_4$

$$\mathcal{E}_3 : y^2 + (\theta + 1)y = x^3 + \theta x.$$

$x$	0	0	0	0
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + (\theta + 1)y$	0	$\theta$	$\theta$	0
$x^3 + \theta x$	0	0	0	*

$x$	1	1	1	1
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + (\theta + 1)y$	0	$\theta$	$\theta$	0
$x^3 + \theta x$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$

$x$	$\theta$	$\theta$	$\theta$	$\theta$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + (\theta + 1)y$	0	$\theta$	$\theta$	0
$x^3 + \theta x$	$\theta$	$\theta$	$\theta$	$\theta$

\* \*

$x$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + (\theta + 1)y$	0	$\theta$	$\theta$	0
$x^3 + \theta x$	0	0	0	0

\*

\*

Ответ:  $\mathcal{E}_3 = \{\Theta, (0, 0), (0, \theta + 1), (\theta, 1), (\theta, \theta), (\theta + 1, 0), (\theta + 1, \theta + 1)\}$ . Порядок  $|\mathcal{E}_3| = 7$ .

**Упражнение 14.8.** Найти порядок  $\mathcal{E}_3$  над полем  $GF(16)$  и  $GF(64)$ .

Ответ: 21, 49.

#### 14.8.2 Суперсингулярные кривые над полем нечетной степени

Пусть суперсингулярная кривая задана уравнением:

$$Y^2 + aY = X^3 + bX + c, \quad a \neq 0, \quad GF(2^m), \quad m \equiv 1 \pmod{2}. \quad (14.60)$$

Покажем, что в этом случае кривая (14.60) изоморфна эллиптической кривой, заданной уравнением:

$$y^2 + y = x^3 + ax + b, \quad a, b \in GF(2). \quad (14.61)$$

**Лемма 14.5.**

Если  $t$  — нечетное, то уравнение

$$y^2 + y = a \quad (14.62)$$

разрешимо в поле  $GF(2^m)$  тогда и только тогда, когда  $Tr(a) = 0$ .

*Доказательство.*

Необходимость: пусть  $y_0$  — решение уравнения (14.62). Тогда из свойств следа вытекает, что

$$Tr(y_0^2) + Tr(y_0) = Tr(y_0) + Tr(y_0) = Tr(a) = 0.$$

Достаточность: если  $Tr(a) = 0$ , то положим  $y_1 = \sum_{k=0}^{\frac{m-1}{2}} a^{2^{2k}}$ .

Из определения  $y_1$  следует, что  $y_1^2 = \sum_{i=0}^{\frac{m-3}{2}} a^{2^{2i+1}}$  и  $y_1^2 + y_1 = a$ . Следовательно,  $y_1$  — решение уравнения (14.62). Второе решение имеет вид  $y_2 = y_1 + 1$ .  $\square$

**Лемма 14.6.**

Если  $t$  — нечетное, то уравнение

$$y^4 + y = a \quad (14.63)$$

разрешимо в поле  $GF(2^m)$  тогда и только тогда, когда  $Tr(a) = 0$ .

*Доказательство.*

Необходимость следует из свойств следа.

Достаточность: так как  $Tr(a) = 0$ , то, согласно Лемме 14.5, уравнение (14.62) разрешимо в  $GF(2^m)$ . Это уравнение имеет два решения и, поскольку  $Tr(1) = 1$ , то для одного из решений след равен 0. Пусть  $x_0$  — это решение уравнения (14.62), для которого  $Tr(x_0) = 0$ . Тогда уравнение  $y^2 + y = x_0$  согласно Лемме 14.5 имеет решение. Пусть  $y_0$  — решение этого уравнения. Итак, из изложенного ранее имеем

$$x_0^2 + x_0 = a, \quad y_0^2 + y_0 = x_0.$$

Поэтому

$$(y_0^2 + y_0)^2 + y_0^2 + y_0 = y_0^4 + y_0 = a.$$

Следовательно,  $y_0$  — решение уравнения (14.63).  $\square$

**Лемма 14.7.**

Если  $m$  — нечетное, то для любого  $a \in GF(2^m)$  существуют такие  $y_0, z_0 \in GF(2^m)$ , что

$$y_0^2 + y_0 + a, z_0^4 + z_0 + a \in GF(2)$$

*Доказательство.*

Если  $Tr(a) = 0$ , то из Леммы 14.5 и Леммы 14.6 следует, что уравнения

$$y^2 + y = a, z^4 + z = a$$

разрешимы в  $GF(2^m)$ . Пусть  $y_0$  и  $z_0$  — их решения. Тогда

$$y_0^2 + y_0 + a = 0 \in GF(2), z_0^4 + z_0 + a = 0 \in GF(2).$$

Если  $Tr(a) = 1$ , то разрешимы уравнения

$$y^2 + y = a + 1, z^4 + z = a + 1.$$

Если  $y_0$  и  $z_0$  — их решения, то

$$y_0^2 + y_0 + a = 1 \in GF(2), z_0^4 + z_0 + a = 1 \in GF(2).$$

$\square$

**Теорема 14.8.** Если  $m$  — нечетное, то эллиптическая кривая над полем  $GF(2^m)$ , заданная уравнением

$$y^2 + ay = x^3 + bx + c, a, b, c \in GF(2^m), a \neq 0 \quad (14.64)$$

изоморфна эллиптической кривой, заданной уравнением

$$y^2 + y = x^3 + bx + c, b, c \in GF(2).$$

*Доказательство.* Во-первых, заметим, что в поле  $F = GF(2^m)$  для любого элемента  $\beta \in F$  существует  $\sqrt[3]{\beta}$ . Это следует из того, что если  $\xi$  — примитивный элемент поля, то  $\xi^{2^m-1} = 1$ . Следовательно  $\xi^{2^m} = \xi$  или  $\xi^{2^m+1} = \xi$ . Поэтому можно считать, что  $\sqrt[3]{\xi} = \xi^{\frac{2^m+1-1}{3}}$ . Тогда, если  $a \in GF(2^m)$ ,  $a \neq 0$ , то  $a = \xi^t$  и

$$\sqrt[3]{a} = (\sqrt[3]{\xi})^t = \xi^{\frac{2^m+1-1}{3}t} \pmod{2^m-1}.$$

Используя этот факт, сделаем следующую допустимую замену переменных в (14.64):

$$x = X, \quad y = aY.$$

В результате получим уравнение вида:

$$Y^2 + Y = a'X^3 + b'X + c', \quad a', b', c' \in GF(2). \quad (14.65)$$

Учитывая, что  $m$  — нечетное и  $\sqrt[3]{a}$  — однозначно определен в поле  $GF(2^m)$ , в результате замен  $X = x/\sqrt[3]{a'}, Y = y$ , уравнение (14.65) приобретает вид:

$$y^2 + y = x^3 + bx + c, \quad b, c \in GF(2^m). \quad (14.66)$$

Далее, применяя Лемму 14.7, выберем  $k \in GF(2^m)$  так, чтобы  $\alpha = k^4 + k + b \in GF(2)$ , а затем выберем  $l \in GF(2^m)$  так, чтобы  $\beta = l^2 + l + k^6 + bk^2 + c \in GF(2)$ . Теперь сделаем замену

$$Y = y + kx + l, \quad X = x + k^2.$$

Подставляя в (14.66) получим:

$$(y + kx + l)^2 + (y + kx + l) = (x + k^2)^3 + b(x + k^2) + c.$$

После раскрытия скобок формула приобретает вид:

$$y^2 + k^2x^2 + l^2 + y + kx + l = x^3 + k^2x^2 + k^4x + k^6 + bx + bk^2 + c.$$

Приведем подобные члены:

$$y^2 + y = x^3 + x(k^4 + k + b) + (k^6 + l^2 + l + bk^2 + c), \quad \text{т.е.}$$

$$y^2 + y = x^3 + \alpha x + \beta, \quad \alpha, \beta \in GF(2).$$

□

В зависимости от значений  $a$  и  $b$  получим четыре вида уравнений:

$$y^2 + y = x^3 + x + 1, \quad y^2 + y = x^3 + x, \quad y^2 + y = x^3 + 1, \quad y^2 + y = x^3.$$

Заметим, что кривые

$$y^2 + y = x^3, \quad y^2 + y = x^3 + 1$$

изоморфны. Действительно, производя в первом уравнении замену  $y = X + Y$ ,  $x = X + 1$ , получим:

$$Y^2 + X^2 + Y + X = X^3 + X^2 + X + 1 \text{ или } Y^2 + Y = X^3 + 1.$$

Таким образом, при нечетном  $m$  будем иметь три класса неизоморфных суперсингулярных кривых:

$$K_1 = \{\mathcal{E}_1 : Y^2 + Y = X^3\}, \quad K_2 = \{\mathcal{E}_2 : Y^2 + Y = X^3 + X\},$$

$$K_3 = \{\mathcal{E}_3 : Y^2 + Y = X^3 + X + 1\}.$$

**Теорема 14.9.** *Если  $m$  – нечетное, то порядок группы точек суперсингулярной эллиптической кривой  $\mathcal{E}$  над полем  $GF(2^m)$  равен или  $2^m + 1$ , или  $2^m \pm 2^{\frac{m+1}{2}} + 1$ .*

*Доказательство.* Воспользуемся теоремой Хассе–Вейля. Рассмотрим эллиптическую кривую  $\mathcal{E}_1$  над полем  $GF(2)$ , ее порядок равен  $N_{\mathcal{E}_1}(2) = 3$  и поэтому  $t = 2 + 1 - 3 = 0$ . По теореме Хассе–Вейля имеем:

$$N_1(2^m) = 2^m + 1 - (\alpha^m + \beta^m).$$

Так как  $m$  нечетное, то  $(\alpha + \beta)|(\alpha^m + \beta^m)$  и, поэтому,  $N_{\mathcal{E}_1}(2^m) = 2^m + 1$ .

Для кривой  $\mathcal{E}_2(GF(2)) = \{(0, 0), (0, 1), (1, 0), (1, 1), \Theta\} = 5$ . Следовательно,  $N = 5$ ,  $t = -2$ ,  $\alpha = -1 + \sqrt{i}$ ,  $\beta = -1 - \sqrt{i}$ , т.е.

$$\alpha = \sqrt{2} \left( \cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right),$$

$$\beta = \sqrt{2} \left( \cos \left( -\frac{3\pi}{4} \right) + i \sin \left( -\frac{3\pi}{4} \right) \right).$$

Поэтому

$$\begin{aligned} N_2(2^m) &= 2^m + 1 - 2^{\frac{m}{2}} \left( \cos \frac{3\pi m}{4} + i \sin \frac{3\pi m}{4} + \right. \\ &\quad \left. + \cos \frac{3\pi m}{4} - i \sin \frac{3\pi m}{4} \right) = 2^m + 1 - 2^{\frac{m}{2}+1} \cos \frac{3\pi m}{4} = \\ &= \begin{cases} 2^m + 1 + 2^{\frac{m+1}{2}}, & m = \pm 1 \pmod{8}, \\ 2^m + 1 - 2^{\frac{m+1}{2}}, & m = \pm 3 \pmod{8}. \end{cases} \end{aligned}$$

Для кривой  $E_3$ , аналогичным образом устанавливаем, что

$$N_3(2^m) = \begin{cases} 2^m + 1 - 2^{\frac{m+1}{2}}, & m = \pm 1 \pmod{8}, \\ 2^m + 1 + 2^{\frac{m+1}{2}}, & m = \pm 3 \pmod{8}. \end{cases}$$

□

### 14.8.3 Группа точек несуперсингулярной кривой

Напомним, что каноническое уравнение несуперсингулярной кривой имеет вид:

$$y^2 + xy = x^3 + ax^2 + b. \quad (14.67)$$

Пусть точка  $P = (x_0, y_0)$  удовлетворяет уравнению (14.67). Заметим, что тогда точка  $Q = (x_0, x_0 + y)$  также удовлетворяет уравнению (14.67). Действительно,

$$(x_0 + y_0)^2 + x_0(x_0 + y_0) = x_0^2 + y_0^2 + x_0^2 + x_0 y_0 = y_0^2 + x_0 y_0 = x_0^3 + a x_0^2 + b.$$

Положим,  $-P = Q$ , т.е.  $-(x_0, y_0) = (x_0, x_0 + y_0)$ . Заметим, что если  $x_0 = 0$ , то  $-P = P$ .

Пусть  $x_1 \neq x_2$ ,  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$  — решение уравнения (14.67). Как и в случае полей характеристики  $\neq 2$ , решим систему:

$$\begin{cases} y = \lambda x + d, \text{ где } \lambda = \frac{y_2 + y_1}{x_2 + x_1}, & d = y_1 + \lambda x_1, \\ y^2 + xy = x^3 + ax^2 + b. \end{cases} \quad (14.68)$$

Очевидно, что  $(x_1, y_1)$  и  $(x_2, y_2)$  удовлетворяют (14.68).

Найдем еще одно решение, решая уравнение:

$$(\lambda x + d)^2 + x(\lambda x + d) = x^3 + ax^2 + b.$$

После раскрытия скобок и приведения подобных членов получим:

$$x^3 + (\lambda^2 + \lambda + a)x^2 + xd + d^2 + b = 0. \quad (14.69)$$

Из теоремы Виета имеем:

$$x_1 + x_2 + x_3 = \lambda^2 + \lambda + a.$$

Следовательно,  $x_3 = \lambda^2 + \lambda + a + x_1 + x_2$ . Поэтому

$$y'_3 = \lambda x_3 + d = \lambda x_3 + y_1 + \lambda x_1 = \lambda(x_3 + x_1) + y_1.$$

Таким образом точка  $P'_3 = (x_3, y'_3)$  является решением (14.68).

Положим,  $P_1 + P_2 = -P'_3 = (x_3, y'_3 + x_3)$ .

В итоге получим:

$$\begin{cases} (x_1, y_1) + (x_2, y_2) = (x_3, y_3), \\ x_3 = \lambda^2 + \lambda + a + x_1 + x_2, \text{ где } \lambda = \frac{y_2 + y_1}{x_2 + x_1}, \\ y_3 = \lambda(x_3 + x_1) + x_3 + y_1. \end{cases} \quad (14.70)$$

Пусть  $P_1 = P_2$ ,  $P_0 = (x_0, y_0)$ ,  $x_0 \neq 0$ ,  $2P_0 = (x_1, y_1)$ .

$$f(x, y) = y^2 + xy + x^3 + ax^2 + b.$$

Положим:

$$\lambda = \left. \frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}} \right|_{\substack{x=x_0 \\ y=y_0}} = \frac{x_0^2 + y_0}{x_0} = x_0 + \frac{y_0}{x_0},$$

$$x_1 = \lambda^2 + \lambda + a, \quad y'_1 = \lambda(x_0 + x_1) + y_0,$$

$$\begin{aligned}
 y_1 &= \lambda x_0 + \lambda x_1 + y_0 + x_1 = \\
 &= \left( x_0 + \frac{y_0}{x_0} \right) x_0 + (\lambda + 1)x_1 + y_0 = \\
 &= x_0^2 + (\lambda + 1)x_1.
 \end{aligned}$$

Таким образом:  $2(x_0, y_0) = (x_1, y_1)$ , где

$$x_1 = \lambda^2 + \lambda + a, \quad y_1 = x_0^2 + (\lambda + 1)x_1, \quad \lambda = x_0 + \frac{y_0}{x_0}. \quad (14.71)$$

**Пример 14.8.** Найдем все точки эллиптической кривой над полем  $GF(2^2) = \mathbb{Z}_2(\theta)/(\theta^2 + \theta + 1) = F$ , заданной уравнением:

$$y^2 + xy = x^3 + x^2 + 1. \quad (14.72)$$

Выпишем элементы поля  $F$ :  $\{0, 1, \theta, \theta + 1 \mid \theta^2 = \theta + 1\}$ . Решение уравнения (14.72) найдем перебором, составляя следующую таблицу:

$x$	0	0	0	0
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + xy$	0	1	$\theta + 1$	$\theta$
$x^3 + x^2 + 1$	1	1	1	1

\*

$x$	1	1	1	1
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + xy$	0	0	1	1
$x^3 + x^2 + 1$	1	1	1	1

\*

\*

$x$	$\theta$	$\theta$	$\theta$	$\theta$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + xy$	0	$\theta + 1$	0	$\theta + 1$
$x^3 + x^2 + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$

\*

\*

$x$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + xy$	0	$\theta$	$\theta$	0
$x^3 + x^2 + 1$	$\theta$	$\theta$	$\theta$	$\theta$

\* \* \*

По таблице определим решения (14.72):

$$\mathcal{E}_1 = \{(0, 1), (1, \theta), (1, \theta + 1), (\theta, 1), (\theta, \theta + 1), (\theta + 1, 1), (\theta + 1, \theta)\}.$$

Эти точки, вместе с точкой  $\Theta$ , образуют группу порядка 8. Заметим, что элемент второго порядка в этой группе единственный. Это точка  $(0, 1)$ . Следовательно, эта группа циклическая.

Найдем последовательно порядок точки  $P_1 = (1, \theta)$ . По формулам (14.71) находим:

$$\lambda = 1 + \theta, \quad \lambda^2 = \theta^2 + 1 = \theta,$$

$$x_1 = \lambda^2 + \lambda + a = \theta + (1 + \theta) + 1 = 0, \quad y_1 = x_0^2 + (\lambda + 1)x_1 = 1.$$

Таким образом  $2(1, \theta) = (0, 1)$  и, следовательно, порядок точки  $P_1 = (1, \theta)$  равен 4. Найдем порядок точки  $(\theta, \theta + 1) = P_2$ . Пусть  $2P_2 = (x_1, y_1)$ . На основе (14.71) имеем:

$$\lambda = \theta + (\theta + 1)\theta^{-1} = \theta + (\theta + 1)(\theta + 1) = \theta + \theta^2 + 1 = 0,$$

$$x_1 = 1, \quad y_1 = \theta^2 + \theta = 1.$$

Итак,  $2P_2 = (1, 1)$ , т.е.  $or(P_2) \neq 4$ , следовательно,  $or(P_2) = 8$ . Убедимся, что  $4P_2 = (x_2, y_2) = (1, 1)$ . Действительно, согласно (14.71) имеем:

$$\lambda = 1 + 1 = 0, \quad x_2 = 1, \quad y_2 = x_0^2 + (\lambda + 1)x_2 = 1 + 1 = 0.$$

Следовательно, группа точек эллиптической кривой (14.72) над полем  $GF(4)$  — циклическая группа порядка 8, порожденная точкой  $(\theta, \theta + 1)$ .

Найдем сумму точек  $(\theta, \theta + 1) + (1, \theta + 1) = (x, y)$ . Согласно (14.70):

$$\lambda = 0, \quad x = 1 + \theta + 1 = \theta, \quad y = \theta + \theta + 1, \quad (x, y) = (\theta, 1).$$

**Упражнение 14.9.** Описать группу точек эллиптической кривой  $\mathcal{E}_2$ , заданной уравнением:

$$y^2 + \theta xy = x^3 + x^2 + \theta + 1.$$

*Решение.*

$x$	0	0	0	0
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta xy$	0	1	$\theta + 1$	$\theta$
$x^3 + x^2 + \theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$

\*

$x$	1	1	1	1
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta xy$	0	$\theta + 1$	0	$\theta + 1$
$x^3 + x^2 + \theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$

\*

\*

$x$	$\theta$	$\theta$	$\theta$	$\theta$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta xy$	0	$\theta$	$\theta$	0
$x^3 + x^2 + \theta + 1$	1	1	1	1

$x$	$\theta + 1$	$\theta + 1$	$\theta + 1$	$\theta + 1$
$y$	0	1	$\theta$	$\theta + 1$
$y^2 + \theta xy$	0	0	1	1
$x^3 + x^2 + \theta + 1$	0	0	0	0

\*

\*

$$\mathcal{E}_2 = \{\Theta, (0, \theta), (1, 1), (1, \theta + 1), (\theta + 1, 0), (\theta + 1, 1)\}.$$

Порядок  $\mathcal{E}_2$  равен 6, следовательно  $\mathcal{E}_2$  — циклическая группа.

□

**Упражнение 14.10.** Найти порядок группы точек над эллиптической кривой  $\mathcal{E}_1$  над полем  $GF(16)$ , используя теорему Хассе—Вейля.

Ответ:  $|\mathcal{E}_1(GF(16))| = 16$ .

**Упражнение 14.11.** Найти порядок группы точек над эллиптической кривой  $\mathcal{E}_2$  над полем  $GF(16)$ , используя теорему Хассе—Вейля.

Ответ:  $|\mathcal{E}_2(GF(16))| = 24$ .

**Упражнение 14.12.** Пусть

$$F = GF(2)[\theta]/(\theta^4 + \theta + 1) = \left\{ \sum_{i=0}^3 \alpha_i \theta^i \mid \alpha_i \in GF(2) \right\}.$$

Показать, что  $\theta$  — примитивный элемент и описать группу точек эллиптической кривой над полем  $F$ , заданной уравнением:

$$y^2 + xy = x^3 + \theta^4 x^2 + 1 = x^3 + (\theta + 1)x^2 + 1.$$

Ответ:  $(1, \theta^{13}), (\theta^3, \theta^{13}), (\theta^5, \theta^{11}), (\theta^6, \theta^{14}), (\theta^9, \theta^{13}), (\theta^{10}, \theta^8), (\theta^{12}, \theta^{12}), (1, \theta^6), (\theta^3, \theta^8), (\theta^5, \theta^3), (\theta^6, \theta^8), (\theta^9, \theta^{10}), (\theta^{10}, \theta), (\theta^{12}, \theta), (0, 1), \Theta$ .

**Упражнение 14.13.** Докажите, что если  $m$  — нечетное, то кривая (14.60) изоморфна некоторой кривой, у которой коэффициент при  $x^2$  в уравнении (14.60) является элементом поля  $GF(2)$ .

*Определение 14.3.* Две эллиптические кривые:

$$(\mathcal{E}_1) : y^2 + xy = x^3 + a_1 x^2 + b \text{ и } (\mathcal{E}_2) : y^2 + xy = x^3 + a_2 x^2 + b$$

называются скрученными, если  $Tr(a_1) \neq Tr(a_2)$ .

**Теорема 14.10.** Если  $\mathcal{E}_1$  и  $\mathcal{E}_2$  — скрученные над  $GF(2^m)$  и  $m$  — нечетное, то  $N_1(\mathcal{E}_1) + N_2(\mathcal{E}_2) = 2^{m+1} + 2$ .

*Доказательство.* Не ограничивая общности, можно считать, что  $\text{Tr}(a_1) = 0$ ,  $\text{Tr}(a_2) = 1$ . Очевидно, что точка  $(0, \sqrt{b})$  является общей точкой этих кривых, как и точка  $\Theta$ .

Если  $x \neq 0$ , то уравнения этих кривых можно привести к виду:

$$\begin{aligned}\mathcal{E}_1 : \frac{y^2}{x^2} + \frac{y}{x} &= x + \frac{b}{x^2} + a_1, \\ \mathcal{E}_2 : \frac{y^2}{x^2} + \frac{y}{x} &= x + \frac{b}{x^2} + a_2.\end{aligned}$$

Замена  $z = \frac{y}{x}$  приводит к уравнениям:

$$\begin{aligned}z^2 + z &= x + \frac{b}{x^2} + a_1, \\ z^2 + z &= x + \frac{b}{x^2} + a_2.\end{aligned}$$

Так как  $\text{Tr}(a_1) = 0$ ,  $\text{Tr}(a_2) = 1$ , первое уравнение разрешается, если  $\text{Tr}\left(x + \frac{b}{x^2}\right) = 0$ , а второе разрешается, если  $\text{Tr}\left(x + \frac{b}{x^2}\right) = 1$ .

Следовательно, для любого  $x \neq 0$  только одно из уравнений  $(\mathcal{E}_1)$  или  $(\mathcal{E}_2)$  имеет два решения. Таким образом, общее число точек с  $x \neq 0$  и лежащих на обеих кривых равно  $2(2^m - 1)$ , а, следовательно,  $N_1 + N_2 = (2^{m+1} - 2) + 2 + 2 = 2^{m+1} + 2$ .  $\square$

#### 14.8.4 Аномальные несуперсингулярные эллиптические кривые

Рассмотрим  $\mathcal{E}_a(n)$  ( $n$  - нечетное) — группу точек эллиптической кривой над полем  $GF(2^n)$ , заданную уравнением:

$$Y^2 + XY = X^3 + aX^2 + 1, \quad a \in GF(2). \quad (14.73)$$

Легко убедиться, что:

$$N_a(1) = \#\mathcal{E}_a(1) = 3 + (-1)^{2-a} = \begin{cases} 4, & \text{если } a = 0, \\ 2, & \text{если } a = 1. \end{cases}$$

Из теоремы Хассе—Вейля следует, что

$$N_1(n) = \#\mathcal{E}_1(n) = 2^n + 1 - (\alpha^n + \beta^n),$$

где  $\alpha, \beta$  — корни уравнения  $x^2 + x + 2 = 0$ , т.е.  $\alpha, \beta = \frac{-1 \pm i\sqrt{7}}{2}$ .

$$N_0(n) = \#\mathcal{E}_0(n) = 2^n + 1 - (\alpha^n + \beta^n),$$

где  $\alpha, \beta$  — корни уравнения  $x^2 - x + 2 = 0$ , т.е.  $\alpha, \beta = \frac{1 \pm i\sqrt{7}}{2}$ .

Заметим, что  $V_n = \alpha^n + \beta^n$  — целое число.

**Пример 14.9.** Покажем, что последовательность  $V_n$  (последовательность Люка) удовлетворяет рекуррентному соотношению:

$$V_{n+1} = t_a V_n - 2V_{n-1}, \quad t_0 = -1, \quad t_1 = 1, \quad n = 2, \dots$$

Действительно,

$$\begin{aligned} \alpha^{n+1} + \beta^{n+1} &= (\alpha + \beta)(\alpha^n + \beta^n) - \beta\alpha^n - \alpha\beta^n = \\ &= (\alpha + \beta)(\alpha^n + \beta^n) - \alpha\beta(\alpha^{n-1} + \beta^{n-1}) = t_a V_n - 2V_{n-1}. \end{aligned}$$

Для практического использования нужно выбирать кривые, у которых  $N_a(n) = pN(1)$ ,  $p$  — простое,  $p \geq 3$ .

**Утверждение 14.7.** Если  $N_a(n) = pN(1)$ , то группа  $\mathcal{E}_a(n)$  — циклическая.

*Доказательство.* При  $a = 1$ ,  $N_1(1)|N_1(n)$ ,  $|N_1(1)| = 2$  и, т.к.  $(2, p) = 1$ , то  $\mathcal{E}_1(n)$  — циклическая. Если  $a = 0$ , то  $\mathcal{E}_0(1) = \{(0, 1), (1, 0), (1, 1), \Theta\}$  — циклическая группа порядка 4. Это следует из того, что  $(0, 1)$  — единственный элемент  $\mathcal{E}_0(1)$ , имеющий порядок 2.

Так как  $N_0(n) = 4p$  и  $p \geq 3$ , то и в этом случае группа  $\mathcal{E}_0(1)$  — циклическая.  $\square$

Обозначим через  $P$  — циклическую подгруппу порядка  $p$  группы  $\mathcal{E}_a(n)$ . Будем называть эту подгруппу главной. Любая точка группы, отличная от  $\Theta$  имеет порядок  $p$ .

**Утверждение 14.8.** Для точки  $P = (x, y) \in \mathcal{E}_a(n)$  существует точка  $P_0 = (x_0, y_0)$  такая, что  $P = 2P_0$  тогда и только тогда, когда  $Tr(x) = Tr(a)$ .

*Доказательство.* Необходимость: пусть  $P = 2P_0$ , тогда согласно правилу удвоения точки  $x = \lambda^2 + \lambda + a$ . Откуда следует

$$Tr(x) = Tr(\lambda^2) + Tr(\lambda) + Tr(a) = Tr(\lambda) + Tr(\lambda) + Tr(a) = Tr(a). \quad (14.74)$$

Достаточность: если  $Tr(a) = Tr(x)$ , то  $Tr(x+a) = 0$ . Следовательно, существует  $\lambda \in F = GF(2^n)$  такое, что  $\lambda^2 + \lambda = a + x$ . Т.к. для  $c \in GF(2^n)$  существует единственное  $d = \sqrt{c}$ , то для данных  $\lambda, x$  и  $y$  найдем  $x_0$  такой, что  $y = x(\lambda + 1) + x_0^2$ . Откуда следует:

$$y^2 = x^2(\lambda^2 + 1) + x_0^4, \quad xy = x^2(\lambda + 1) + x_0^2x. \quad (14.75)$$

Из (14.75) получаем:

$$\begin{aligned} y^2 + xy &= x^2(\lambda^2 + \lambda) + x_0^4 + x_0^2x = \\ &= x^2(a + x) + x_0^4 + x_0^2x = \\ &= x^3 + ax^2 + x_0^4 + x_0^2x = x^3 + ax^2 + 1. \end{aligned}$$

Таким образом,  $1 = x_0^4 + x_0^2x$ . Положим  $y_0 = \lambda x_0 + x_0^2$ , т.е.  $\lambda = x_0 + \frac{y_0}{x_0}$ .

$$\begin{aligned} y_0^2 &= \lambda^2 x_0^2 + x_0^4 = (\lambda + x + a)x_0^2 + x_0^4 = \\ &= x_0^3 + y_0 x_0 + x_0^2 x + a x_0^2 + x_0^4 = \\ &= x_0^3 + y_0 x_0 + 1 + a x_0^2. \end{aligned}$$

Следовательно,

$$y_0^2 + x_0 y_0 = x_0^3 + a x_0^2 + 1.$$

Таким образом,

$$(x_0, y_0) \in \mathcal{E}_a(n), \quad x = \lambda^2 + \lambda + a, \quad y = x_0^2 + x(\lambda + 1).$$

Это значит, что  $(x, y) = 2(x_0, y_0)$ .  $\square$

**Следствие 14.1.** Точка  $(x, y) \in \mathcal{E}_1(n)$ ,  $n$  - нечетное, имеет порядок  $p$  тогда и только тогда, когда  $Tr(x) = 0$ .

**Утверждение 14.9.** Для точки  $(x, y) \in \mathcal{E}_a(n)$  такой, что  $y^2 + yx = x^3 + ax^2 + 1$ , где  $Tr(a) = 0$ , существует  $(x_1, y_1) \in \mathcal{E}_a(n)$  такая, что  $(x, y) = 4(x_1, y_1)$  тогда и только тогда, когда  $Tr(x) = 0$ ,  $Tr(y) = Tr(\lambda x)$ , где  $\lambda^2 + \lambda = x + a$ .

*Доказательство.* Необходимость: пусть

$$(x, y) = 2(x_2, y_2), \quad (x_2, y_2) = 2(x_1, y_1).$$

Тогда из предыдущего утверждения следует, что

$$Tr(x_2) = Tr(a) = 0 = Tr(x).$$

Пусть  $x_2 \neq 0$  и  $\lambda = x_2 + \frac{y_2}{x_2}$ . Тогда согласно правилам удвоения  $x = \lambda^2 + \lambda + a$ ,  $y = x_2^2 + (\lambda + 1)x$ . Отсюда следует, что  $Tr(y) = Tr(x_2^2) + Tr(\lambda x) + Tr(x) = Tr(\lambda x)$ . Необходимость доказана.

Достаточность: поскольку  $Tr(x) = 0 = Tr(a)$ , то из утверждения 14.8 следует, что  $(x, y) = 2(x_2, y_2)$ ,  $(x_2, y_2) \in \mathcal{E}_a(n)$ . Из правила удвоения точки следует, что

$$y = x_2^2 + (\lambda + 1)x, \quad x = \lambda^2 + \lambda + a, \quad \lambda = x_2 + \frac{y_2}{x_2}.$$

Отсюда имеем  $y + \lambda x = x + x_2^2$ . Поэтому, учитывая условие  $Tr(y) = Tr(\lambda x)$ , будем иметь

$$\begin{aligned} Tr(y + \lambda x) &= Tr(y) + Tr(\lambda x) = 0 = \\ &= Tr(x) + Tr(x_2) = Tr(x_2) = Tr(a). \end{aligned}$$

Из утверждения 14.8 следует, что  $(x_2, y_2) = 2(x_1, y_1)$ .  $\square$

**Следствие 14.2.** Точка  $(x, y) \in \mathcal{E}_0(n)$  имеет порядок  $p$  тогда и только тогда, когда  $\text{Tr}(x) = \text{Tr}(y) = \text{Tr}(\lambda x)$ , где  $\lambda^2 + \lambda = x$ .

**Упражнение 14.14.** Доказать, что если  $(x, y) \in \mathcal{E}_a(n)$ , то  $(x^2, y^2) \in \mathcal{E}_a(n)$ .

**Упражнение 14.15.** Доказать, что если отображение вида

$$\tau : \mathcal{E}_a(n) \rightarrow \mathcal{E}_a(n),$$

определенное правилом  $\tau(x, y) = (x^2, y^2)$  является изоморфизмом, т.е.  $\tau(P_1 + P_2) = \tau(P_1) + \tau(P_2)$ .

# Литература

- [1] Алферов Н. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии, М.: Гелиос АРВ, 2001 г.
- [2] Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994 г.
- [3] Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971 г.
- [4] Васilenко О. Н. Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2003 г.
- [5] Виноградов И. М. Основы теории чисел. М.: Наука, 1972 г.
- [6] Кострикин А. И. Введение в алгебру, М.: Наука, 1972 г.
- [7] Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2001 г.
- [8] Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. Изд. 2. М.: КомКнига/URSS, 2012.
- [9] Холл М. Теория групп, М.: Ил, 1968 г.
- [10] Применко Э. А. Конечные группы подстановок, М.: МИЭМ, 1982 г.

- [11] Применко Э. А., Скворцов Э. Ф. Об условиях регулярности конечных автономных автоматов // Дискретная математика. 1990. Т2(1) С. 23–30.
- [12] Грушо А. А., Применко Э. А., Тимонина Е. Е. Анализ и синтез криптоалгоритмов. Курс лекций. Йошкар-Ола, МОСУ, 2000 г.
- [13] Грушо А. А., Применко Э. А., Тимонина Е. Е. Криптографические протоколы. Йошкар-Ола, МОСУ, 2001 г.
- [14] Гашков С. Б., Применко Э. А., Черепнёв М. А. Криптографические методы защиты информации. М.: Академия, 2010 г., 304 с.
- [15] Цирлер Н. Линейные возвратные последовательности, Кибернетический сборник 6, М.: ИЛ, 1963. С. 55–79.
- [16] Handbook of Applied Cryptography by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.
- [17] Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth) by Bruce Schneier, 1996.
- [18] Pollard J. M. Monte Carlo Methods for Index Computation (mod p). Math.Comp. vol.32, no.143, July 1978, pp.918-924.

## Представляем Вам следующие книги:



### Алгебра

- ✓ **Буфееев С. В.** Коллекция задач по арифметике целых чисел: Задания С6 ЕГЭ.
- ✓ **Чеботарев Н. Г.** Основы теории Галуа. В 2 кн.
- ✓ **Вейль Г.** Классические группы. Их инварианты и представления.
- ✓ **Фробениус Ф. Г.** Теория характеров и представлений групп.
- ✓ **Эйзенхарт Л. П.** Непрерывные группы преобразований.
- ✓ **Бэр Р.** Линейная алгебра и проективная геометрия.
- ✓ **Никифоров В. А., Шкода Б. В.** Линейная алгебра и аналитическая геометрия.
- ✓ **Шевалле К.** Введение в теорию алгебраических функций.
- ✓ **Уокер Р.** Алгебраические кривые.
- ✓ **Супруненко Д. А., Тышкевич Р. И.** Перестановочные матрицы.
- ✓ **Киселев А. П.** Задачи и упражнения к «Элементам алгебры».
- ✓ **Золотаревская Д. И.** Сборник задач по линейной алгебре.

### Серия «Физико-математическое наследие: алгебра»

- ✓ **Чеботарев Н. Г.** Введение в теорию алгебр.
- ✓ **Чеботарев Н. Г.** Теория групп Ли.
- ✓ **Чеботарев Н. Г.** Теория Галуа.
- ✓ **Чеботарев Н. Г.** Теория алгебраических функций.
- ✓ **Александров П. С.** Введение в теорию групп.
- ✓ **Маркус М., Минк Х.** Обзор по теории матриц и матричных неравенств.
- ✓ **Бохер М.** Введение в высшую алгебру.
- ✓ **Младзеевский Б. К.** Основы высшей алгебры.
- ✓ **Шмидт О. Ю.** Абстрактная теория групп.

### Серия «Физико-математическое наследие: топология»

- ✓ **Александров П. С.** Введение в теорию множеств и общую топологию.
- ✓ **Милнор Дж.** Теория Морса.
- ✓ **Стинрод Н.** Топология косых произведений.
- ✓ **Листинг И. Б.** Предварительные исследования по топологии.

### Теория вероятностей и математическая статистика

- ✓ **Колмогоров А. Н.** Основные понятия теории вероятностей.
- ✓ **Гнеденко Б. В.** Курс теории вероятностей.
- ✓ **Гнеденко Б. В.** Очерк по истории теории вероятностей.
- ✓ **Гнеденко Б. В.** Математика и контроль качества продукции.
- ✓ **Гнеденко Б. В., Коваленко И. Н.** Введение в теорию массового обслуживания.
- ✓ **Ивченко Г. И., Каштанов В. А., Коваленко И. Н.** Теория массового обслуживания.
- ✓ **Хинчин А. Я.** Работы по математической теории массового обслуживания.
- ✓ **Хинчин А. Я.** Асимптотические законы теории вероятностей.
- ✓ **Хинчин А. Я.** Математические основания квантовой статистики.
- ✓ **Саати Т. Л.** Элементы теории массового обслуживания и ее приложения.
- ✓ **Боровков А. А.** Эргодичность и устойчивость случайных процессов.
- ✓ **Тактаров Н. Г.** Теория вероятностей и математическая статистика.

## Представляем Вам следующие книги:



### Теория чисел

- ✓ Оре О. Приглашение в теорию чисел.
- ✓ Вейль А. Основы теории чисел.
- ✓ Вейль Г. Алгебраическая теория чисел.
- ✓ Понtryагин Л. С. Обобщения чисел.
- ✓ Жуков А. В. Бездесущее число «пи».
- ✓ Хинчин А. Я. Три жемчужины теории чисел.
- ✓ Хинчин А. Я. Цепные дроби.
- ✓ Парфенов И. И. Цепные дроби — ожерелье мехатроники.
- ✓ Ожигова Е. П. Что такое теория чисел.
- ✓ Виноградов И. М. Особые варианты метода тригонометрических сумм.
- ✓ Карацуба А. А. Основы аналитической теории чисел.
- ✓ Гельфонд А. О. Трансцендентные и алгебраические числа.
- ✓ Яглом И. М. Комплексные числа и их применение в геометрии.
- ✓ Деза Е. И. Специальные числа натурального ряда.
- ✓ Деза Е. И., Котова Л. В. Сборник задач по теории чисел.

### Серия «Физико-математическое наследие: теория чисел»

- ✓ Диофант Александрийский. Арифметика и книга о многоугольных числах.
- ✓ Ферма П. Исследования по теории чисел и диофантову анализу.
- ✓ Дирихле П. Г. Л. Лекции по теории чисел.
- ✓ Дедекинд Р. Непрерывность и иррациональные числа.
- ✓ Ингам А. Э. Распределение простых чисел.
- ✓ Берман Г. Н. Число и наука о нем: Общедоступные очерки.
- ✓ Ландау Э. Основы анализа: Действия над числами.
- ✓ Титчмарш Э. Ч. Дзета-функция Римана.
- ✓ Дэвенпорт Г. Высшая арифметика: Введение в теорию чисел.
- ✓ Гельфонд А. О. Решение уравнений в целых числах.

### Дифференциальные и интегральные уравнения

- ✓ Филиппов А. Ф. Введение в теорию дифференциальных уравнений.
- ✓ Филиппов А. Ф. Сборник задач по дифференциальным уравнениям.
- ✓ Эльсгольц Л. Э. Дифференциальные уравнения.
- ✓ Степанов В. В. Курс дифференциальных уравнений.
- ✓ Немыцкий В. В., Степанов В. В. Качественная теория дифференциальных уравнений.
- ✓ Краснов М. Л. и др. Обыкновенные дифференциальные уравнения. Сборник задач «Вся высшая математика» с подробными решениями.
- ✓ Краснов М. Л. Интегральные уравнения. Введение в теорию.
- ✓ Шалдырован В. А., Медведев К. В. Руководство по решению обыкновенных дифференциальных уравнений. Кн. 1, 2.
- ✓ Петровский И. Г. Лекции по теории обыкновенных дифференциальных уравнений.
- ✓ Петровский И. Г. Лекции по теории интегральных уравнений.
- ✓ Федорюк М. В. Обыкновенные дифференциальные уравнения.
- ✓ Федорюк М. В. Асимптотика: Интегралы и ряды.

## Представляем Вам следующие книги:



### Серия «НАУКУ — ВСЕМ! Шедевры научно-популярной литературы»

- ✓ Колмогоров А. Н. Математика — наука и профессия.
- ✓ Гашков С. Б. Занимательная компьютерная арифметика: Математика и искусство счета на компьютерах и без них.
- ✓ Гашков С. Б. Занимательная компьютерная арифметика: Быстрые алгоритмы операций с числами и многочленами.
- ✓ Гнеденко Б. В. Беседы о теории массового обслуживания.
- ✓ Гнеденко Б. В. Беседы о математической статистике.
- ✓ Гнеденко Б. В., Хинчин А. Я. Элементарное введение в теорию вероятностей.
- ✓ Мизес Р. Вероятность и статистика.
- ✓ Менкхен Ф. Некоторые тайны артистов-вычислителей.
- ✓ Вильямс Дж. Д. Совершенный стратег, или Букварь по теории стратегических игр.
- ✓ Юдин Д. Б., Юдин А. Д. Математики измеряют сложность.

### Математическая логика

- ✓ Колмогоров А. Н., Драгалин А. Г. Математическая логика: Введение в математическую логику.
- ✓ Колмогоров А. Н., Драгалин А. Г. Математическая логика: Дополнительные главы.
- ✓ Драгалин А. Г. Конструктивная теория доказательств и нестандартный анализ.
- ✓ Фреге Г. Логика и логическая семантика.
- ✓ Гладкий А. В. Введение в современную логику.
- ✓ Гамов Г., Стерн М. Занимательные задачи.
- ✓ Карпенко А. С. Развитие многозначной логики.
- ✓ Карпенко А. С. Логики Лукасевича и простые числа.

### Серия «Физико-математическое наследие: основания математики и логика»

- ✓ Чёр A. Введение в математическую логику.
- ✓ Гудстейн Р. Л. Математическая логика.
- ✓ Бурбаки Н. Теория множеств.
- ✓ Хаусдорф Ф. Теория множеств.
- ✓ Френкель А. А., Бар-Хиллел И. Основания теории множеств.

### Серия «Физико-математическое наследие: теория функций»

- ✓ Курант Р. Геометрическая теория функций комплексной переменной.
- ✓ Привалов И. И. Субгармонические функции.
- ✓ Бор Г. Почти периодические функции.
- ✓ Артин Э. Введение в теорию гамма-функций.

### Дискретная математика

- ✓ Харари Ф. Теория графов.
- ✓ Оре О. Графы и их применение.
- ✓ Оре О. Теория графов.
- ✓ Емеличев В. А., Мельников О. И. и др. Лекции по теории графов.
- ✓ Мельников О. И. Теория графов в занимательных задачах: Более 250 задач с подробными решениями.

## Представляем Вам следующие книги:



### Серия «Основы защиты информации»

- ✓ Борисов М. А. Особенности защиты персональных данных в трудовых отношениях.
- ✓ Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации.
- ✓ Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации.
- ✓ Жданов О. Н., Чалкин В. А. Эллиптические кривые: Основы теории и криптографические приложения.

- ✓ Крэндалл Р., Померанс К. Простые числа: Вычислительные и криптографические аспекты.
- ✓ Александрова Н. В. Из истории векторного исчисления.
- ✓ Горобец Б. С. Теория вероятностей, математическая статистика и элементы случайных процессов: Упрощенный курс.
- ✓ Пухначев Ю. В., Попов Ю. П. Математика без формул. В 2 кн.
- ✓ Супрун В. П. Математика для старшеклассников: Задачи повышенной сложности.
- ✓ Супрун В. П. Математика для старшеклассников: Нестандартные методы решения задач.
- ✓ Супрун В. П. Математика для старшеклассников: Методы решения и доказательства неравенств. 367 задач с подробными решениями.
- ✓ Мордухай-Болтовской Д. Д. Геометрия радиолярий.
- ✓ Золотаревская Д. И. Теория вероятностей. Задачи с решениями.
- ✓ Федин С. Н. Математики тоже шутят.
- ✓ Петров Н. Н. Математические игры.
- ✓ Пойа Д. Как решать задачу.
- ✓ Гнеденко Б. В., Беляев Ю. К., Соловьев А. Д. Математические методы в теории надежности: Основные характеристики надежности и их статистический анализ.
- ✓ Литвинов В. Н. Правильный пятиугольник: Геометрия, декоративное искусство, архитектура.
- ✓ Амелькин В. В. Дифференциальные уравнения в приложениях.
- ✓ Медведев Г. Н. Участникам олимпиад и вступительных испытаний по математике.

### Наши книги можно приобрести в магазинах:

«НАУКУ – ВСЕМ!» (м. Профсоюзная, Нахимовский пр-т, 56. Тел. (499) 724-2545)  
 «Библио-Глобус» (м. Лубянка, ул. Мясницкая, 6. Тел. (495) 625-2457)  
 «Московский дом книги» (м. Арбатская, ул. Новый Арбат, 8. Тел. (495) 203-8242)  
 «Молодая гвардия» (м. Полянка, ул. Б. Полянка, 28. Тел. (495) 238-5001, (495) 780-3370)  
 «Дом научно-технической книги» (Ленинский пр-т, 40. Тел. (495) 137-6019)  
 «Дом книги на Ладожской» (м. Бауманская, ул. Ладожская, 8, стр. 1. Тел. (495) 267-0302)  
 «Санкт-Петербургский Дом книги» (Невский пр., 28. Тел. (812) 448-2355)  
 «Нижний бум» (г. Киев, книжный рынок «Петровка», ряд 62, место 8 (павильон «АкадемКнига»). Тел. +38 (067) 273-5010)  
 Сеть магазинов «Дом книги» (г. Екатеринбург, ул. Антона Валеева, 12. Тел. (343) 253-5010)

Тел./факс:  
+7 (499) 724-25-45  
(многоканальный)

E-mail:  
URSS@URSS.ru  
<http://URSS.ru>

## Уважаемые читатели! Уважаемые авторы!

Наше издательство специализируется на выпуске научной и учебной литературы, в том числе монографий, журналов, трудов ученых Российской академии наук, научно-исследовательских институтов и учебных заведений. Мы предлагаем авторам свои услуги на выгодных экономических условиях. При этом мы берем на себя всю работу по подготовке издания — от набора, редактирования и верстки до тиражирования и распространения.



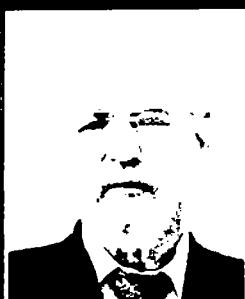
Среди вышедших и готовящихся к изданию книг мы предлагаем Вам следующие:

- ✓ Краснов М. Л. и др. Вся высшая математика. Т. 1–7.
- ✓ Краснов М. Л., Киселев А. И., Макаренко Г. И. Сборники задач «Вся высшая математика» с подробными решениями.
- ✓ Тактаров Н. Г. Справочник по высшей математике для студентов вузов.
- ✓ Боярчук А. К., Ляшко И. И., Гай Я. Г., Головач Г. П. Справочное пособие по высшей математике (Антидемидович). Т. 1–5.
- Т. 1. Введение в анализ, производная, интеграл.
- Т. 2. Ряды, функции векторного аргумента.
- Т. 3. Интегралы, зависящие от параметра; кратные и криволинейные интегралы.
- Т. 4. Функции комплексного переменного: теория и практика.
- Т. 5. Дифференциальные уравнения в примерах и задачах.
- ✓ Босс В. Лекции по теории управления. Т. 1: Автоматическое регулирование.
- ✓ Босс В. Интуиция и математика.
- ✓ Босс В. Лекции по математике. Т. 1–16. Т. 1: Анализ; Т. 2: Дифференциальные уравнения; Т. 3: Линейная алгебра; Т. 4: Вероятность, информация, статистика; Т. 5: Функциональный анализ; Т. 6: От Диофанта до Тьюринга; Т. 7: Оптимизация; Т. 8: Теория групп; Т. 9: ТФКП; Т. 10. Перебор и эффективные алгоритмы; Т. 11. Уравнения математической физики; Т. 12. Конtrapримеры и парадоксы; Т. 13. Топология; Т. 14. Теория чисел; Т. 15. Нелинейные операторы и неподвижные точки; Т. 16. Теория множеств: От Кантора до Коэна.
- ✓ Ивченко Г. И., Медведев Ю. И. Введение в математическую статистику. Статистика знает все.
- ✓ Пантаев М. Ю. Матанализ с человеческим лицом, или Как выжить после предельного перехода: Полный курс математического анализа. В 2 т.
- ✓ Зуев Ю. А. По океану дискретной математики: От перечислительной комбинаторики до современной криптографии. В 2 т.
- ✓ Moscow Journal of Combinatorics and Number Theory. (One volume of four issues is published annually.)
- ✓ Боровков А. А. Теория вероятностей.
- ✓ Жуков А. В. Элегантная математика: Задачи и решения.
- ✓ Жуков А. В. Прометеева искра: Античные истоки искусства математики.

По всем вопросам Вы можете обратиться к нам:  
тел. +7 (499) 724–25–45 (многоканальный)  
или электронной почтой [URSS@URSS.ru](mailto:URSS@URSS.ru)  
Полный каталог изданий представлен  
в интернет-магазине: <http://URSS.ru>

Научная и учебная  
литература

## Об авторе

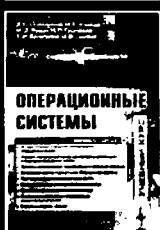
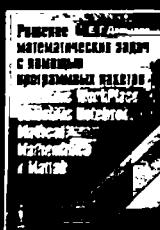


## Эдуард Андреевич ПРИМЕНКО

Кандидат физико-математических наук, доцент кафедры математической кибернетики Московского государственного университета. Научный библиограф МГУ, ответственный секретарь журнала «Математика» Российской академии наук. Автор более 60 научных работ и нескольких учебников по дискретной математике и информатике. Руководитель и разработчик магистерской программы МГУ по направлению «математическое и программное обеспечение защиты информации».

67073880

Наше издательство предлагает следующие книги:



13588 ID 169492



9 785397 038201 >

Издательская группа  
**URSS**

Каталог изданий  
в Интернете:  
<http://URSS.ru>  
E-mail: [URSS@URSS.ru](mailto:URSS@URSS.ru)

117335, Москва,  
Нахимовский  
проспект, 56      Телефон / факс  
(многоканальный)  
+7 (499) 724 25 45

Отзывы о настоящем издании, а также обнаруженные  
ошибки присыпайте по адресу [URSS@URSS.ru](mailto:URSS@URSS.ru).  
Ваше замечание и предложения будут учтены  
и отражены на web-странице этой книги на сайте  
<http://URSS.ru>