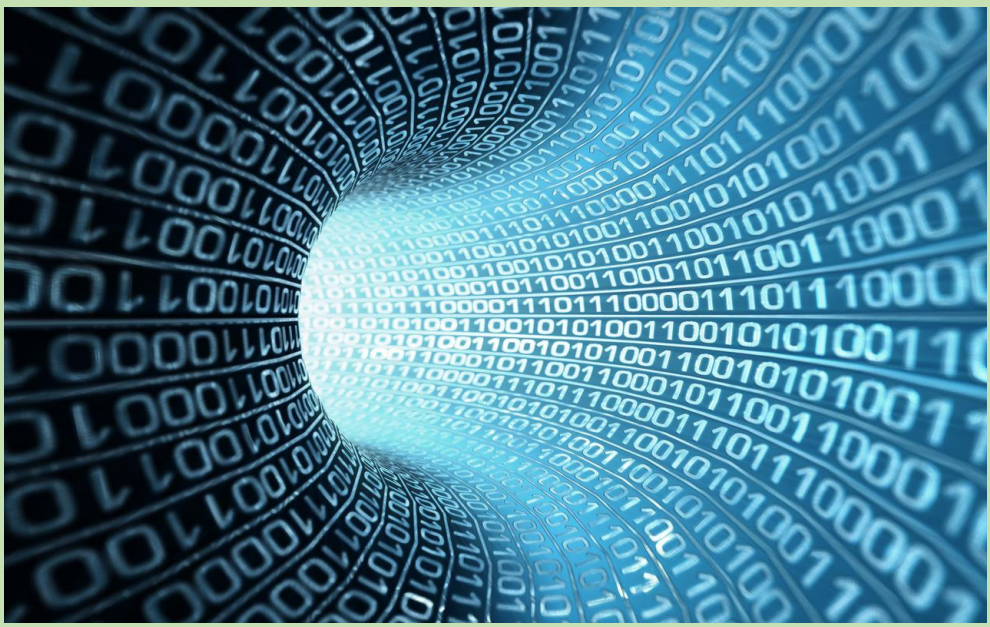
Ю. В. КУЛАКОВ

ВВЕДЕНИЕ В КРИПТОЛОГИЮ

В четырех частях

Часть 3



Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2025

Министерство науки и высшего образования Российской Федерации

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Тамбовский государственный технический университет»**

Ю. В. КУЛАКОВ

ВВЕДЕНИЕ В КРИПТОЛОГИЮ

В четырех частях

Часть 3

Утверждено Ученым советом университета в качестве
учебного пособия для студентов направлений подготовки
09.03.02, 09.04.02 «Информационные системы и технологии»,
27.04.03 «Системный анализ и управление», 38.03.05 «Бизнес-информатика»
и специальностей 10.05.03 «Информационная безопасность автоматизированных систем»,
38.05.01 «Экономическая безопасность» очной и заочной форм обучения

Учебное электронное издание

Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2025

УДК 51(075.8)
ББК з811я73
В24

Рецензенты:

Доктор физико-математических наук, профессор
ФГБОУ ВО «ТГУ им. Г. Р. Державина»
Е. С. Жуковский

Кандидат технических наук, доцент,
заведующий кафедрой «Системы автоматизированной поддержки
принятия решений» ФГБОУ ВО «ТГТУ»
И. Л. Коробова

В24 **Введение** в криптологию [Электронный ресурс] : учебное пособие : в 4-х ч. / Ю. В. Кулаков, О. Г. Иванова, Н. Г. Шахов, А. И. Елисеев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ».
ISBN 978-5-8265-2366-7

Ч. 3. – Ю. В. Кулаков. – 2025. – 1 электрон. опт. диск (CD-ROM). – ПК не ниже класса Pentium IV ; RAM 512 Mb ; необходимое место на HDD 2,0 Mb ; Windows 7/8/10/11 ; дисковод CD-ROM ; мышь. – Загл. с экрана.
ISBN 978-5-8265-2923-2

Содержит теоретический материал по основным понятиям, определениям и алгоритмам арифметики остатков, конечных групп и полей и список рекомендуемой литературы.

Предназначено для студентов направлений подготовки 09.03.02, 09.04.02 «Информационные системы и технологии», 27.04.03 «Системный анализ и управление», 38.03.05 «Бизнес-информатика» и специальностей 10.05.03 «Информационная безопасность автоматизированных систем», 38.05.01 «Экономическая безопасность» очной и заочной форм обучения.

УДК 51(075.8)
ББК з811я73

ISBN 978-5-8265-2366-7 (общ.)
ISBN 978-5-8265-2923-2 (ч. 3)

ВВЕДЕНИЕ

В третьей части учебного пособия представлен материал, который ориентирован на изучение вопросов, связанных с так называемыми эллиптическими кривыми, а именно введением в эллиптические кривые и групповому закону, которому эллиптические кривые удовлетворяют.

Среди вопросов, связанных с введением в эллиптические кривые, рассматриваются такие понятия, как: проективная плоскость, проективная точка проективной плоскости, эллиптическая кривая в проективных и криволинейных (аффинных) координатах.

Проективная плоскость над заданным полем определяется как множество последовательностей из трех, не равных одновременно нулю элементов, в котором задано отношение эквивалентности, а проективная точка проективной плоскости – как некоторый класс эквивалентности, определяемый этим отношением.

Эллиптическая кривая в проективных координатах характеризуется как множество точек проективной плоскости, удовлетворяющих длинной форме однородного уравнения Вейерштрасса, а эллиптическая кривая в криволинейных координатах – аффинной версии этого уравнения.

В материале по групповому закону рассматриваются понятия изоморфной эллиптической кривой; собственно групповому закону, вводимому по методу хорд и касательных; сложения точек эллиптической кривой и дискретного логарифмирования на эллиптической кривой.

При этом одна эллиптическая кривая считается изоморфной другой эллиптической кривой, если при определенной замене переменных в первой эллиптической кривой она переходит во вторую кривую.

Вводимый методом хорд и касательных групповой закон наделяет эллиптическую кривую структурой абелевой группы с бесконечно удаленной точкой в качестве нейтрального элемента по сложению.

Реализация многократного сложения (умножения) точек эллиптической кривой позволяет ввести понятие дискретного логарифмирования на эллиптической кривой по сложению.

Новизна данного учебного пособия, в сравнении с ранее изданной литературой по вопросам введения в криптологию [1 – 18], заключается в рассмотрении примеров практически к каждому даваемому понятию, определению и алгоритму.

Применение данного пособия будет способствовать формированию у выпускников следующих компетенций по направлениям подготовки и специальностям.

По направлению подготовки 09.03.02 «Информационные системы и технологии»: способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3).

По направлению подготовки 09.04.02 «Информационные системы и технологии»: способен разрабатывать требования к информационным системам (ИС) и осуществлять организационное и технологическое обеспечение возможности их реализации в ИС (ПК-1).

По направлению 27.04.03 «Системный анализ и управление»: способен решать задачи системного анализа и управления в технических системах на базе последних достижений науки и техники (ОПК-3).

По направлению 38.03.05 «Бизнес-информатика»: способен организовывать взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия (ПК-1).

По специальности 10.05.03 «Информационная безопасность автоматизированных систем»: способен использовать математические методы, необходимые для решения задач профессиональной деятельности (ОПК-3); способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10); способен разрабатывать компоненты систем защиты информации автоматизированных систем (ОПК-11).

По специальности 38.05.01 «Экономическая безопасность»: способен работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12); способен соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20).

2. ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

2.1. ВВЕДЕНИЕ В ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

2.1.1. ПРОЕКТИВНАЯ ПЛОСКОСТЬ

Некоторые из наиболее современных криптографических систем с открытым ключом основаны на использовании эллиптической кривой, в результате чего они обеспечивают высокую эффективность и большую пропускную способность. Заметим, что эллиптическая кривая над конечным полем является конечной абелевой группой, в которой можно ставить задачу о вычислении дискретных логарифмов.

Проективной плоскостью $\mathbf{P}^2(K)$ над полем K называется множество последовательностей (X,Y,Z) из трех не равных одновременно нулю элементов $X,Y,Z \in K$, в котором задано отношение эквивалентности:

$$(X,Y,Z) \equiv (\lambda X, \lambda Y, \lambda Z) \text{ для любых } \lambda \in K^* = K \setminus \{0\}. \qquad (2.1)$$

При этом, в качестве поля K может выступать и поле вычетов по простому модулю p, обозначаемое символом $\mathbf{F}_p$. Тогда проективная плоскость $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p)$ будет иметь мощность, равную $(p^3 - 1)$.

Например, при p = 3 проективной плоскостью $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$ над полем $K = \mathbf{F}_p = \mathbf{F}_3 = \{0, 1, 2\}$ является множество $\mathbf{P}^2(\mathbf{F}_3)$ = {(0, 0, 1), (0, 0, 2), (0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 0, 0), (1, 0, 1), (1, 0, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2), (2, 0, 0), (2, 0, 1), (2, 0, 2), (2, 1, 0), (2, 1, 1), (2, 1, 2), (2, 2, 0), (2, 2, 1), (2, 2, 2)} мощности $p^3 - 1 = 3^3 - 1 = 27 - 1 = 26$.

Во втором примере (при p = 5) проективной плоскостью $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_5)$ над полем $K = \mathbf{F}_p = \mathbf{F}_5 = \{0, 1, 2, 3, 4\}$ является множество $\mathbf{P}^2(\mathbf{F}_5)$ = {(0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4), (0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 1, 3), (0, 1, 4), (0, 2, 0), (0, 2, 1), (0, 2, 2), (0, 2, 3), (0, 2, 4), (0, 3, 0), (0, 3, 1), (0, 3, 2), (0, 3, 3), (0, 3, 4), (0, 4, 0), (0, 4, 1), (0, 4, 2), (0, 4, 3), (0, 4, 4), (1, 0, 0), (1, 0, 1), (1, 0, 2), (1, 0, 3), (1, 0, 4), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 1, 4), (1, 2, 0), (1, 2, 1), (1, 2, 2), (1, 2, 3), (1, 2, 4), (1, 3, 0), (1, 3, 1), (1, 3, 2), (1, 3, 3), (1, 3, 4), (1, 4, 0), (1, 4, 1), (1, 4, 2), (1, 4, 3), (1, 4, 4), (2, 0, 0), (2, 0, 1), (2, 0, 2), (2, 0, 3), (2, 0, 4), (2, 1, 0), (2, 1, 1), (2, 1, 2), (2, 1, 3), (2, 1, 4), (2, 2, 0), (2, 2, 1), (2, 2, 2), (2, 2, 3), (2, 2, 4), (2, 3, 0), (2, 3, 1), (2, 3, 2), (2, 3, 3), (2, 3, 4), (2, 4, 0), (2, 4, 1), (2, 4, 2), (2, 4, 3), (2, 4, 4), (3, 0, 0), (3, 0, 1), (3, 0, 2), (3, 0, 3), (3, 0, 4), (3, 1, 0), (3, 1, 1), (3, 1, 2),

(3, 1, 3), (3, 1, 4), (3, 2, 0), (3, 2, 1), (3, 2, 2), (3, 2, 3), (3, 2, 4), (3, 3, 0), (3, 3, 1), (3, 3, 2), (3, 3, 3), (3, 3, 4), (3, 4, 0), (3, 4, 1), (3, 4, 2), (3, 4, 3), (3, 4, 4), (4, 0, 0), (4, 0, 1), (4, 0, 2), (4, 0, 3), (4, 0, 4), (4, 1, 0), (4, 1, 1), (4, 1, 2), (4, 1, 3), (4, 1, 4), (4, 2, 0), (4, 2, 1), (4, 2, 2), (4, 2, 3), (4, 2, 4), (4, 3, 0), (4, 3, 1), (4, 3, 2), (4, 3, 3), (4, 3, 4), (4, 4, 0), (4, 4, 1), (4, 4, 2), (4, 4, 3), (4, 4, 4)} мощности $p^3 - 1 = 5^3 - 1 = 125 - 1 = 124$.

В третьем примере (при $p = 7$) проективной плоскостью $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$ над полем $K = \mathbf{F}_p = \mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ является множество $\mathbf{P}^2(\mathbf{F}_7) = \{$(0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4), (0, 0, 5), (0, 0, 6), (0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 1, 3), (0, 1, 4), (0, 1, 5), (0, 1, 6), (0, 2, 0), (0, 2, 1), (0, 2, 2), (0, 2, 3), (0, 2, 4), (0, 2, 5), (0, 2, 6), (0, 3, 0), (0, 3, 1), (0, 3, 2), (0, 3, 3), (0, 3, 4), (0, 3, 5), (0, 3, 6), (0, 4, 0), (0, 4, 1), (0, 4, 2), (0, 4, 3), (0, 4, 4), (0, 4, 5), (0, 4, 6), (0, 5, 0), (0, 5, 1), (0, 5, 2), (0, 5, 3), (0, 5, 4), (0, 5, 5), (0, 5, 6), (0, 6, 0), (0, 6, 1), (0, 6, 2), (0, 6, 3), (0, 6, 4), (0, 6, 5), (0, 6, 6), (1, 0, 0), (1, 0, 1), (1, 0, 2), (1, 0, 3), (1, 0, 4), (1, 0, 5), (1, 0, 6), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 1, 4), (1, 1, 5), (1, 1, 6), (1, 2, 0), (1, 2, 1), (1, 2, 2), (1, 2, 3), (1, 2, 4), (1, 2, 5), (1, 2, 6), (1, 3, 0), (1, 3, 1), (1, 3, 2), (1, 3, 3), (1, 3, 4), (1, 3, 5), (1, 3, 6), (1, 4, 0), (1, 4, 1), (1, 4, 2), (1, 4, 3), (1, 4, 4), (1, 4, 5), (1, 4, 6), (1, 5, 0), (1, 5, 1), (1, 5, 2), (1, 5, 3), (1, 5, 4), (1, 5, 5), (1, 5, 6), (1, 6, 0), (1, 6, 1), (1, 6, 2), (1, 6, 3), (1, 6, 4), (1, 6, 5), (1, 6, 6), (2, 0, 0), (2, 0, 1), (2, 0, 2), (2, 0, 3), (2, 0, 4), (2, 0, 5), (2, 0, 6), (2, 1, 0), (2, 1, 1), (2, 1, 2), (2, 1, 3), (2, 1, 4), (2, 1, 5), (2, 1, 6), (2, 2, 0), (2, 2, 1), (2, 2, 2), (2, 2, 3), (2, 2, 4), (2, 2, 5), (2, 2, 6), (2, 3, 0), (2, 3, 1), (2, 3, 2), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 3, 6), (2, 4, 0), (2, 4, 1), (2, 4, 2), (2, 4, 3), (2, 4, 4), (2, 4, 5), (2, 4, 6), (2, 5, 0), (2, 5, 1), (2, 5, 2), (2, 5, 3), (2, 5, 4), (2, 5, 5), (2, 5, 6), (2, 6, 0), (2, 6, 1), (2, 6, 2), (2, 6, 3), (2, 6, 4), (2, 6, 5), (2, 6, 6), (3, 0, 0), (3, 0, 1), (3, 0, 2), (3, 0, 3), (3, 0, 4), (3, 0, 5), (3, 0, 6), (3, 1, 0), (3, 1, 1), (3, 1, 2), (3, 1, 3), (3, 1, 4), (3, 1, 5), (3, 1, 6), (3, 2, 0), (3, 2, 1), (3, 2, 2), (3, 2, 3), (3, 2, 4), (3, 2, 5), (3, 2, 6), (3, 3, 0), (3, 3, 1), (3, 3, 2), (3, 3, 3), (3, 3, 4), (3, 3, 5), (3, 3, 6), (3, 4, 0), (3, 4, 1), (3, 4, 2), (3, 4, 3), (3, 4, 4), (3, 4, 5), (3, 4, 6), (3, 5, 0), (3, 5, 1), (3, 5, 2), (3, 5, 3), (3, 5, 4), (3, 5, 5), (3, 5, 6), (3, 6, 0), (3, 6, 1), (3, 6, 2), (3, 6, 3), (3, 6, 4), (3, 6, 5), (3, 6, 6), (4, 0, 0), (4, 0, 1), (4, 0, 2), (4, 0, 3), (4, 0, 4), (4, 0, 5), (4, 0, 6), (4, 1, 0), (4, 1, 1), (4, 1, 2), (4, 1, 3), (4, 1, 4), (4, 1, 5), (4, 1, 6), (4, 2, 0), (4, 2, 1), (4, 2, 2), (4, 2, 3), (4, 2, 4), (4, 2, 5), (4, 2, 6), (4, 3, 0), (4, 3, 1), (4, 3, 2), (4, 3, 3), (4, 3, 4), (4, 3, 5), (4, 3, 6), (4, 4, 0), (4, 4, 1), (4, 4, 2), (4, 4, 3), (4, 4, 4), (4, 4, 5), (4, 4, 6), (4, 5, 0), (4, 5, 1), (4, 5, 2), (4, 5, 3), (4, 5, 4), (4, 5, 5), (4, 5, 6), (4, 6, 0), (4, 6, 1), (4, 6, 2), (4, 6, 3), (4, 6, 4), (4, 6, 5), (4, 6, 6), (5, 0, 0), (5, 0, 1), (5, 0, 2), (5, 0, 3), (5, 0, 4), (5, 0, 5), (5, 0, 6), (5, 1, 0), (5, 1, 1), (5, 1, 2), (5, 1, 3), (5, 1, 4), (5, 1, 5), (5, 1, 6), (5, 2, 0), (5, 2, 1), (5, 2, 2), (5, 2, 3), (5, 2, 4), (5, 2, 5), (5, 2, 6), (5, 3, 0), (5, 3, 1), (5, 3, 2), (5, 3, 3), (5, 3, 4), (5, 3, 5), (5, 3, 6), (5, 4, 0), (5, 4, 1), (5, 4, 2), (5, 4, 3), (5, 4, 4), (5, 4, 5), (5, 4, 6), (5, 5, 0), (5, 5, 1), (5, 5, 2), (5, 5, 3), (5, 5, 4), (5, 5, 5), (5, 5, 6), (5, 6, 0), (5, 6, 1), (5, 6, 2), (5, 6, 3), (5, 6, 4),

(5, 6, 5), (5, 6, 6), (6, 0, 0), (6, 0, 1), (6, 0, 2), (6, 0, 3), (6, 0, 4), (6, 0, 5), (6, 0, 6), (6, 1, 0), (6, 1, 1), (6, 1, 2), (6, 1, 3), (6, 1, 4), (6, 1, 5), (6, 1, 6), (6, 2, 0), (6, 2, 1), (6, 2, 2), (6, 2, 3), (6, 2, 4), (6, 2, 5), (6, 2, 6), (6, 3, 0), (6, 3, 1), (6, 3, 2), (6, 3, 3), (6, 3, 4), (6, 3, 5), (6, 3, 6), (6, 4, 0), (6, 4, 1), (6, 4, 2), (6, 4, 3), (6, 4, 4), (6, 4, 5), (6, 4, 6), (6, 5, 0), (6, 5, 1), (6, 5, 2), (6, 5, 3), (6, 5, 4), (6, 5, 5), (6, 5, 6), (6, 6, 0), (6, 6, 1), (6, 6, 2), (6, 6, 3), (6, 6, 4), (6, 6, 5), (6, 6, 6)} мощности $p^3 - 1 = 7^3 - 1 = 343 - 1 = 342$.

В четвертом примере (при $p = 11$) проективной плоскостью $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_{11})$ над полем $K = \mathbf{F}_p = \mathbf{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ является множество $\mathbf{P}^2(\mathbf{F}_{11})$ = {(0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4), (0, 0, 5), (0, 0, 6), (0, 0, 7), (0, 0, 8), (0, 0, 9), (0, 0, 10), (0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 1, 3), (0, 1, 4), (0, 1, 5), (0, 1, 6), (0, 1, 7), (0, 1, 8), (0, 1, 9), (0, 1, 10), (0, 2, 0), (0, 2, 1), (0, 2, 2), (0, 2, 3), (0, 2, 4), (0, 2, 5), (0, 2, 6), (0, 2, 7), (0, 2, 8), (0, 2, 9), (0, 2, 10), (0, 3, 0), (0, 3, 1), (0, 3, 2), (0, 3, 3), (0, 3, 4), (0, 3, 5), (0, 3, 6), (0, 3, 7), (0, 3, 8), (0, 3, 9), (0, 3, 10), (0, 4, 0), (0, 4, 1), (0, 4, 2), (0, 4, 3), (0, 4, 4), (0, 4, 5), (0, 4, 6), (0, 4, 7), (0, 4, 8), (0, 4, 9), (0, 4, 10), (0, 5, 0), (0, 5, 1), (0, 5, 2), (0, 5, 3), (0, 5, 4), (0, 5, 5), (0, 5, 6), (0, 5, 7), (0, 5, 8), (0, 5, 9), (0, 5, 10), (0, 6, 0), (0, 6, 1), (0, 6, 2), (0, 6, 3), (0, 6, 4), (0, 6, 5), (0, 6, 6), (0, 6, 7), (0, 6, 8), (0, 6, 9), (0, 6, 10), (0, 7, 0), (0, 7, 1), (0, 7, 2), (0, 7, 3), (0, 7, 4), (0, 7, 5), (0, 7, 6), (0, 7, 7), (0, 7, 8), (0, 7, 9), (0, 7, 10), (0, 8, 0), (0, 8, 1), (0, 8, 2), (0, 8, 3), (0, 8, 4), (0, 8, 5), (0, 8, 6), (0, 8, 7), (0, 8, 8), (0, 8, 9), (0, 8, 10), (0, 9, 0), (0, 9, 1), (0, 9, 2), (0, 9, 3), (0, 9, 4), (0, 9, 5), (0, 9, 6), (0, 9, 7), (0, 9, 8), (0, 9, 9), (0, 9, 10), (0, 10, 0), (0, 10, 1), (0, 10, 2), (0, 10, 3), (0, 10, 4), (0, 10, 5), (0, 10, 6), (0, 10, 7), (0, 10, 8), (0, 10, 9), (0, 10, 10), (1, 0, 0), (1, 0, 1), (1, 0, 2), (1, 0, 3), (1, 0, 4), (1, 0, 5), (1, 0, 6), (1, 0, 7), (1, 0, 8), (1, 0, 9), (1, 0, 10), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 1, 4), (1, 1, 5), (1, 1, 6), (1, 1, 7), (1, 1, 8), (1, 1, 9), (1, 1, 10), (1, 2, 0), (1, 2, 1), (1, 2, 2), (1, 2, 3), (1, 2, 4), (1, 2, 5), (1, 2, 6), (1, 2, 7), (1, 2, 8), (1, 2, 9), (1, 2, 10), (1, 3, 0), (1, 3, 1), (1, 3, 2), (1, 3, 3), (1, 3, 4), (1, 3, 5), (1, 3, 6), (1, 3, 7), (1, 3, 8), (1, 3, 9), (1, 3, 10), (1, 4, 0), (1, 4, 1), (1, 4, 2), (1, 4, 3), (1, 4, 4), (1, 4, 5), (1, 4, 6), (1, 4, 7), (1, 4, 8), (1, 4, 9), (1, 4, 10), (1, 5, 0), (1, 5, 1), (1, 5, 2), (1, 5, 3), (1, 5, 4), (1, 5, 5), (1, 5, 6), (1, 5, 7), (1, 5, 8), (1, 5, 9), (1, 5, 10), (1, 6, 0), (1, 6, 1), (1, 6, 2), (1, 6, 3), (1, 6, 4), (1, 6, 5), (1, 6, 6), (1, 6, 7), (1, 6, 8), (1, 6, 9), (1, 6, 10), (1, 7, 0), (1, 7, 1), (1, 7, 2), (1, 7, 3), (1, 7, 4), (1, 7, 5), (1, 7, 6), (1, 7, 7), (1, 7, 8), (1, 7, 9), (1, 7, 10), (1, 8, 0), (1, 8, 1), (1, 8, 2), (1, 8, 3), (1, 8, 4), (1, 8, 5), (1, 8, 6), (1, 8, 7), (1, 8, 8), (1, 8, 9), (1, 8, 10), (1, 9, 0), (1, 9, 1), (1, 9, 2), (1, 9, 3), (1, 9, 4), (1, 9, 5), (1, 9, 6), (1, 9, 7), (1, 9, 8), (1, 9, 9), (1, 9, 10), (1, 10, 0), (1, 10, 1), (1, 10, 2), (1, 10, 3), (1, 10, 4), (1, 10, 5), (1, 10, 6), (1, 10, 7), (1, 10, 8), (1, 10, 9), (1, 10, 10), (2, 0, 0), (2, 0, 1), (2, 0, 2), (2, 0, 3), (2, 0, 4), (2, 0, 5), (2, 0, 6), (2, 0, 7), (2, 0, 8), (2, 0, 9), (2, 0, 10), (2, 1, 0), (2, 1, 1), (2, 1, 2), (2, 1, 3), (2, 1, 4), (2, 1, 5), (2, 1, 6), (2, 1, 7), (2, 1, 8), (2, 1, 9), (2, 1, 10), (2, 2, 0), (2, 2, 1), (2, 2, 2), (2, 2, 3), (2, 2, 4), (2, 2, 5), (2, 2, 6), (2, 2, 7), (2, 2, 8), (2, 2, 9), (2, 2, 10), (2, 3, 0), (2, 3, 1), (2, 3, 2), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 3, 6), (2, 3, 7), (2, 3, 8), (2, 3, 9),

(2, 3, 10), (2, 4, 0), (2, 4, 1), (2, 4, 2), (2, 4, 3), (2, 4, 4), (2, 4, 5), (2, 4, 6), (2, 4, 7), (2, 4, 8), (2, 4, 9), (2, 4, 10), (2, 5, 0), (2, 5, 1), (2, 5, 2), (2, 5, 3), (2, 5, 4), (2, 5, 5), (2, 5, 6), (2, 5, 7), (2, 5, 8), (2, 5, 9), (2, 5, 10), (2, 6, 0), (2, 6, 1), (2, 6, 2), (2, 6, 3), (2, 6, 4), (2, 6, 5), (2, 6, 6), (2, 6, 7), (2, 6, 8), (2, 6, 9), (2, 6, 10), (2, 7, 0), (2, 7, 1), (2, 7, 2), (2, 7, 3), (2, 7, 4), (2, 7, 5), (2, 7, 6), (2, 7, 7), (2, 7, 8), (2, 7, 9), (2, 7, 10), (2, 8, 0), (2, 8, 1), (2, 8, 2), (2, 8, 3), (2, 8, 4), (2, 8, 5), (2, 8, 6), (2, 8, 7), (2, 8, 8), (2, 8, 9), (2, 8, 10), (2, 9, 0), (2, 9, 1), (2, 9, 2), (2, 9, 3), (2, 9, 4), (2, 9, 5), (2, 9, 6), (2, 9, 7), (2, 9, 8), (2, 9, 9), (2, 9, 10), (2, 10, 0), (2, 10, 1), (2, 10, 2), (2, 10, 3), (2, 10, 4), (2, 10, 5), (2, 10, 6), (2, 10, 7), (2, 10, 8), (2, 10, 9), (2, 10, 10), (3, 0, 0), (3, 0, 1), (3, 0, 2), (3, 0, 3), (3, 0, 4), (3, 0, 5), (3, 0, 6), (3, 0, 7), (3, 0, 8), (3, 0, 9), (3, 0, 10), (3, 1, 0), (3, 1, 1), (3, 1, 2), (3, 1, 3), (3, 1, 4), (3, 1, 5), (3, 1, 6), (3, 1, 7), (3, 1, 8), (3, 1, 9), (3, 1, 10), (3, 2, 0), (3, 2, 1), (3, 2, 2), (3, 2, 3), (3, 2, 4), (3, 2, 5), (3, 2, 6), (3, 2, 7), (3, 2, 8), (3, 2, 9), (3, 2, 10), (3, 3, 0), (3, 3, 1), (3, 3, 2), (3, 3, 3), (3, 3, 4), (3, 3, 5), (3, 3, 6), (3, 3, 7), (3, 3, 8), (3, 3, 9), (3, 3, 10), (3, 4, 0), (3, 4, 1), (3, 4, 2), (3, 4, 3), (3, 4, 4), (3, 4, 5), (3, 4, 6), (3, 4, 7), (3, 4, 8), (3, 4, 9), (3, 4, 10), (3, 5, 0), (3, 5, 1), (3, 5, 2), (3, 5, 3), (3, 5, 4), (3, 5, 5), (3, 5, 6), (3, 5, 7), (3, 5, 8), (3, 5, 9), (3, 5, 10), (3, 6, 0), (3, 6, 1), (3, 6, 2), (3, 6, 3), (3, 6, 4), (3, 6, 5), (3, 6, 6), (3, 6, 7), (3, 6, 8), (3, 6, 9), (3, 6, 10), (3, 7, 0), (3, 7, 1), (3, 7, 2), (3, 7, 3), (3, 7, 4), (3, 7, 5), (3, 7, 6), (3, 7, 7), (3, 7, 8), (3, 7, 9), (3, 7, 10), (3, 8, 0), (3, 8, 1), (3, 8, 2), (3, 8, 3), (3, 8, 4), (3, 8, 5), (3, 8, 6), (3, 8, 7), (3, 8, 8), (3, 8, 9), (3, 8, 10), (3, 9, 0), (3, 9, 1), (3, 9, 2), (3, 9, 3), (3, 9, 4), (3, 9, 5), (3, 9, 6), (3, 9, 7), (3, 9, 8), (3, 9, 9), (3, 9, 10), (3, 10, 0), (3, 10, 1), (3, 10, 2), (3, 10, 3), (3, 10, 4), (3, 10, 5), (3, 10, 6), (3, 10, 7), (3, 10, 8), (3, 10, 9), (3, 10, 10), (4, 0, 0), (4, 0, 1), (4, 0, 2), (4, 0, 3), (4, 0, 4), (4, 0, 5), (4, 0, 6), (4, 0, 7), (4, 0, 8), (4, 0, 9), (4, 0, 10), (4, 1, 0), (4, 1, 1), (4, 1, 2), (4, 1, 3), (4, 1, 4), (4, 1, 5), (4, 1, 6), (4, 1, 7), (4, 1, 8), (4, 1, 9), (4, 1, 10), (4, 2, 0), (4, 2, 1), (4, 2, 2), (4, 2, 3), (4, 2, 4), (4, 2, 5), (4, 2, 6), (4, 2, 7), (4, 2, 8), (4, 2, 9), (4, 2, 10), (4, 3, 0), (4, 3, 1), (4, 3, 2), (4, 3, 3), (4, 3, 4), (4, 3, 5), (4, 3, 6), (4, 3, 7), (4, 3, 8), (4, 3, 9), (4, 3, 10), (4, 4, 0), (4, 4, 1), (4, 4, 2), (4, 4, 3), (4, 4, 4), (4, 4, 5), (4, 4, 6), (4, 4, 7), (4, 4, 8), (4, 4, 9), (4, 4, 10), (4, 5, 0), (4, 5, 1), (4, 5, 2), (4, 5, 3), (4, 5, 4), (4, 5, 5), (4, 5, 6), (4, 5, 7), (4, 5, 8), (4, 5, 9), (4, 5, 10), (4, 6, 0), (4, 6, 1), (4, 6, 2), (4, 6, 3), (4, 6, 4), (4, 6, 5), (4, 6, 6), (4, 6, 7), (4, 6, 8), (4, 6, 9), (4, 6, 10), (4, 7, 0), (4, 7, 1), (4, 7, 2), (4, 7, 3), (4, 7, 4), (4, 7, 5), (4, 7, 6), (4, 7, 7), (4, 7, 8), (4, 7, 9), (4, 7, 10), (4, 8, 0), (4, 8, 1), (4, 8, 2), (4, 8, 3), (4, 8, 4), (4, 8, 5), (4, 8, 6), (4, 8, 7), (4, 8, 8), (4, 8, 9), (4, 8, 10), (4, 9, 0), (4, 9, 1), (4, 9, 2), (4, 9, 3), (4, 9, 4), (4, 9, 5), (4, 9, 6), (4, 9, 7), (4, 9, 8), (4, 9, 9), (4, 9, 10), (4, 10, 0), (4, 10, 1), (4, 10, 2), (4, 10, 3), (4, 10, 4), (4, 10, 5), (4, 10, 6), (4, 10, 7), (4, 10, 8), (4, 10, 9), (4, 10, 10), (5, 0, 0), (5, 0, 1), (5, 0, 2), (5, 0, 3), (5, 0, 4), (5, 0, 5), (5, 0, 6), (5, 0, 7), (5, 0, 8), (5, 0, 9), (5, 0, 10), (5, 1, 0), (5, 1, 1), (5, 1, 2), (5, 1, 3), (5, 1, 4), (5, 1, 5), (5, 1, 6), (5, 1, 7), (5, 1, 8), (5, 1, 9), (5, 1, 10), (5, 2, 0), (5, 2, 1), (5, 2, 2), (5, 2, 3), (5, 2, 4), (5, 2, 5), (5, 2, 6), (5, 2, 7), (5, 2, 8), (5, 2, 9), (5, 2, 10), (5, 3, 0), (5, 3, 1), (5, 3, 2), (5, 3, 3), (5, 3, 4), (5, 3, 5), (5, 3, 6), (5, 3, 7), (5, 3, 8), (5, 3, 9), (5, 3, 10), (5, 4, 0), (5, 4, 1), (5, 4, 2),

(5, 4, 3), (5, 4, 4), (5, 4, 5), (5, 4, 6), (5, 4, 7), (5, 4, 8), (5, 4, 9), (5, 4, 10), (5, 5, 0), (5, 5, 1), (5, 5, 2), (5, 5, 3), (5, 5, 4), (5, 5, 5), (5, 5, 6), (5, 5, 7), (5, 5, 8), (5, 5, 9), (5, 5, 10), (5, 6, 0), (5, 6, 1), (5, 6, 2), (5, 6, 3), (5, 6, 4), (5, 6, 5), (5, 6, 6), (5, 6, 7), (5, 6, 8), (5, 6, 9), (5, 6, 10), (5, 7, 0), (5, 7, 1), (5, 7, 2), (5, 7, 3), (5, 7, 4), (5, 7, 5), (5, 7, 6), (5, 7, 7), (5, 7, 8), (5, 7, 9), (5, 7, 10), (5, 8, 0), (5, 8, 1), (5, 8, 2), (5, 8, 3), (5, 8, 4), (5, 8, 5), (5, 8, 6), (5, 8, 7), (5, 8, 8), (5, 8, 9), (5, 8, 10), (5, 9, 0), (5, 9, 1), (5, 9, 2), (5, 9, 3), (5, 9, 4), (5, 9, 5), (5, 9, 6), (5, 9, 7), (5, 9, 8), (5, 9, 9), (5, 9, 10), (5, 10, 0), (5, 10, 1), (5, 10, 2), (5, 10, 3), (5, 10, 4), (5, 10, 5), (5, 10, 6), (5, 10, 7), (5, 10, 8), (5, 10, 9), (5, 10, 10), (6, 0, 0), (6, 0, 1), (6, 0, 2), (6, 0, 3), (6, 0, 4), (6, 0, 5), (6, 0, 6), (6, 0, 7), (6, 0, 8), (6, 0, 9), (6, 0, 10), (6, 1, 0), (6, 1, 1), (6, 1, 2), (6, 1, 3), (6, 1, 4), (6, 1, 5), (6, 1, 6), (6, 1, 7), (6, 1, 8), (6, 1, 9), (6, 1, 10), (6, 2, 0), (6, 2, 1), (6, 2, 2), (6, 2, 3), (6, 2, 4), (6, 2, 5), (6, 2, 6), (6, 2, 7), (6, 2, 8), (6, 2, 9), (6, 2, 10), (6, 3, 0), (6, 3, 1), (6, 3, 2), (6, 3, 3), (6, 3, 4), (6, 3, 5), (6, 3, 6), (6, 3, 7), (6, 3, 8), (6, 3, 9), (6, 3, 10), (6, 4, 0), (6, 4, 1), (6, 4, 2), (6, 4, 3), (6, 4, 4), (6, 4, 5), (6, 4, 6), (6, 4, 7), (6, 4, 8), (6, 4, 9), (6, 4, 10), (6, 5, 0), (6, 5, 1), (6, 5, 2), (6, 5, 3), (6, 5, 4), (6, 5, 5), (6, 5, 6), (6, 5, 7), (6, 5, 8), (6, 5, 9), (6, 5, 10), (6, 6, 0), (6, 6, 1), (6, 6, 2), (6, 6, 3), (6, 6, 4), (6, 6, 5), (6, 6, 6), (6, 6, 7), (6, 6, 8), (6, 6, 9), (6, 6, 10), (6, 7, 0), (6, 7, 1), (6, 7, 2), (6, 7, 3), (6, 7, 4), (6, 7, 5), (6, 7, 6), (6, 7, 7), (6, 7, 8), (6, 7, 9), (6, 7, 10), (6, 8, 0), (6, 8, 1), (6, 8, 2), (6, 8, 3), (6, 8, 4), (6, 8, 5), (6, 8, 6), (6, 8, 7), (6, 8, 8), (6, 8, 9), (6, 8, 10), (6, 9, 0), (6, 9, 1), (6, 9, 2), (6, 9, 3), (6, 9, 4), (6, 9, 5), (6, 9, 6), (6, 9, 7), (6, 9, 8), (6, 9, 9), (6, 9, 10), (6, 10, 0), (6, 10, 1), (6, 10, 2), (6, 10, 3), (6, 10, 4), (6, 10, 5), (6, 10, 6), (6, 10, 7), (6, 10, 8), (6, 10, 9), (6, 10, 10), (7, 0, 0), (7, 0, 1), (7, 0, 2), (7, 0, 3), (7, 0, 4), (7, 0, 5), (7, 0, 6), (7, 0, 7), (7, 0, 8), (7, 0, 9), (7, 0, 10), (7, 1, 0), (7, 1, 1), (7, 1, 2), (7, 1, 3), (7, 1, 4), (7, 1, 5), (7, 1, 6), (7, 1, 7), (7, 1, 8), (7, 1, 9), (7, 1, 10), (7, 2, 0), (7, 2, 1), (7, 2, 2), (7, 2, 3), (7, 2, 4), (7, 2, 5), (7, 2, 6), (7, 2, 7), (7, 2, 8), (7, 2, 9), (7, 2, 10), (7, 3, 0), (7, 3, 1), (7, 3, 2), (7, 3, 3), (7, 3, 4), (7, 3, 5), (7, 3, 6), (7, 3, 7), (7, 3, 8), (7, 3, 9), (7, 3, 10), (7, 4, 0), (7, 4, 1), (7, 4, 2), (7, 4, 3), (7, 4, 4), (7, 4, 5), (7, 4, 6), (7, 4, 7), (7, 4, 8), (7, 4, 9), (7, 4, 10), (7, 5, 0), (7, 5, 1), (7, 5, 2), (7, 5, 3), (7, 5, 4), (7, 5, 5), (7, 5, 6), (7, 5, 7), (7, 5, 8), (7, 5, 9), (7, 5, 10), (7, 6, 0), (7, 6, 1), (7, 6, 2), (7, 6, 3), (7, 6, 4), (7, 6, 5), (7, 6, 6), (7, 6, 7), (7, 6, 8), (7, 6, 9), (7, 6, 10), (7, 7, 0), (7, 7, 1), (7, 7, 2), (7, 7, 3), (7, 7, 4), (7, 7, 5), (7, 7, 6), (7, 7, 7), (7, 7, 8), (7, 7, 9), (7, 7, 10), (7, 8, 0), (7, 8, 1), (7, 8, 2), (7, 8, 3), (7, 8, 4), (7, 8, 5), (7, 8, 6), (7, 8, 7), (7, 8, 8), (7, 8, 9), (7, 8, 10), (7, 9, 0), (7, 9, 1), (7, 9, 2), (7, 9, 3), (7, 9, 4), (7, 9, 5), (7, 9, 6), (7, 9, 7), (7, 9, 8), (7, 9, 9), (7, 9, 10), (7, 10, 0), (7, 10, 1), (7, 10, 2), (7, 10, 3), (7, 10, 4), (7, 10, 5), (7, 10, 6), (7, 10, 7), (7, 10, 8), (7, 10, 9), (7, 10, 10), (8, 0, 0), (8, 0, 1), (8, 0, 2), (8, 0, 3), (8, 0, 4), (8, 0, 5), (8, 0, 6), (8, 0, 7), (8, 0, 8), (8, 0, 9), (8, 0, 10), (8, 1, 0), (8, 1, 1), (8, 1, 2), (8, 1, 3), (8, 1, 4), (8, 1, 5), (8, 1, 6), (8, 1, 7), (8, 1, 8), (8, 1, 9), (8, 1, 10), (8, 2, 0), (8, 2, 1), (8, 2, 2), (8, 2, 3), (8, 2, 4), (8, 2, 5), (8, 2, 6), (8, 2, 7), (8, 2, 8), (8, 2, 9), (8, 2, 10), (8, 3, 0), (8, 3, 1), (8, 3, 2), (8, 3, 3), (8, 3, 4), (8, 3, 5), (8, 3, 6),

(8, 3, 7), (8, 3, 8), (8, 3, 9), (8, 3, 10), (8, 4, 0), (8, 4, 1), (8, 4, 2), (8, 4, 3), (8, 4, 4), (8, 4, 5), (8, 4, 6), (8, 4, 7), (8, 4, 8), (8, 4, 9), (8, 4, 10), (8, 5, 0), (8, 5, 1), (8, 5, 2), (8, 5, 3), (8, 5, 4), (8, 5, 5), (8, 5, 6), (8, 5, 7), (8, 5, 8), (8, 5, 9), (8, 5, 10), (8, 6, 0), (8, 6, 1), (8, 6, 2), (8, 6, 3), (8, 6, 4), (8, 6, 5), (8, 6, 6), (8, 6, 7), (8, 6, 8), (8, 6, 9), (8, 6, 10), (8, 7, 0), (8, 7, 1), (8, 7, 2), (8, 7, 3), (8, 7, 4), (8, 7, 5), (8, 7, 6), (8, 7, 7), (8, 7, 8), (8, 7, 9), (8, 7, 10), (8, 8, 0), (8, 8, 1), (8, 8, 2), (8, 8, 3), (8, 8, 4), (8, 8, 5), (8, 8, 6), (8, 8, 7), (8, 8, 8), (8, 8, 9), (8, 8, 10), (8, 9, 0), (8, 9, 1), (8, 9, 2), (8, 9, 3), (8, 9, 4), (8, 9, 5), (8, 9, 6), (8, 9, 7), (8, 9, 8), (8, 9, 9), (8, 9, 10), (8, 10, 0), (8, 10, 1), (8, 10, 2), (8, 10, 3), (8, 10, 4), (8, 10, 5), (8, 10, 6), (8, 10, 7), (8, 10, 8), (8, 10, 9), (8, 10, 10), (9, 0, 0), (9, 0, 1), (9, 0, 2), (9, 0, 3), (9, 0, 4), (9, 0, 5), (9, 0, 6), (9, 0, 7), (9, 0, 8), (9, 0, 9), (9, 0, 10), (9, 1, 0), (9, 1, 1), (9, 1, 2), (9, 1, 3), (9, 1, 4), (9, 1, 5), (9, 1, 6), (9, 1, 7), (9, 1, 8), (9, 1, 9), (9, 1, 10), (9, 2, 0), (9, 2, 1), (9, 2, 2), (9, 2, 3), (9, 2, 4), (9, 2, 5), (9, 2, 6), (9, 2, 7), (9, 2, 8), (9, 2, 9), (9, 2, 10), (9, 3, 0), (9, 3, 1), (9, 3, 2), (9, 3, 3), (9, 3, 4), (9, 3, 5), (9, 3, 6), (9, 3, 7), (9, 3, 8), (9, 3, 9), (9, 3, 10), (9, 4, 0), (9, 4, 1), (9, 4, 2), (9, 4, 3), (9, 4, 4), (9, 4, 5), (9, 4, 6), (9, 4, 7), (9, 4, 8), (9, 4, 9), (9, 4, 10), (9, 5, 0), (9, 5, 1), (9, 5, 2), (9, 5, 3), (9, 5, 4), (9, 5, 5), (9, 5, 6), (9, 5, 7), (9, 5, 8), (9, 5, 9), (9, 5, 10), (9, 6, 0), (9, 6, 1), (9, 6, 2), (9, 6, 3), (9, 6, 4), (9, 6, 5), (9, 6, 6), (9, 6, 7), (9, 6, 8), (9, 6, 9), (9, 6, 10), (9, 7, 0), (9, 7, 1), (9, 7, 2), (9, 7, 3), (9, 7, 4), (9, 7, 5), (9, 7, 6), (9, 7, 7), (9, 7, 8), (9, 7, 9), (9, 7, 10), (9, 8, 0), (9, 8, 1), (9, 8, 2), (9, 8, 3), (9, 8, 4), (9, 8, 5), (9, 8, 6), (9, 8, 7), (9, 8, 8), (9, 8, 9), (9, 8, 10), (9, 9, 0), (9, 9, 1), (9, 9, 2), (9, 9, 3), (9, 9, 4), (9, 9, 5), (9, 9, 6), (9, 9, 7), (9, 9, 8), (9, 9, 9), (9, 9, 10), (9, 10, 0), (9, 10, 1), (9, 10, 2), (9, 10, 3), (9, 10, 4), (9, 10, 5), (9, 10, 6), (9, 10, 7), (9, 10, 8), (9, 10, 9), (9, 10, 10), (10, 0, 0), (10, 0, 1), (10, 0, 2), (10, 0, 3), (10, 0, 4), (10, 0, 5), (10, 0, 6), (10, 0, 7), (10, 0, 8), (10, 0, 9), (10, 0, 10), (10, 1, 0), (10, 1, 1), (10, 1, 2), (10, 1, 3), (10, 1, 4), (10, 1, 5), (10, 1, 6), (10, 1, 7), (10, 1, 8), (10, 1, 9), (10, 1, 10), (10, 2, 0), (10, 2, 1), (10, 2, 2), (10, 2, 3), (10, 2, 4), (10, 2, 5), (10, 2, 6), (10, 2, 7), (10, 2, 8), (10, 2, 9), (10, 2, 10), (10, 3, 0), (10, 3, 1), (10, 3, 2), (10, 3, 3), (10, 3, 4), (10, 3, 5), (10, 3, 6), (10, 3, 7), (10, 3, 8), (10, 3, 9), (10, 3, 10), (10, 4, 0), (10, 4, 1), (10, 4, 2), (10, 4, 3), (10, 4, 4), (10, 4, 5), (10, 4, 6), (10, 4, 7), (10, 4, 8), (10, 4, 9), (10, 4, 10), (10, 5, 0), (10, 5, 1), (10, 5, 2), (10, 5, 3), (10, 5, 4), (10, 5, 5), (10, 5, 6), (10, 5, 7), (10, 5, 8), (10, 5, 9), (10, 5, 10), (10, 6, 0), (10, 6, 1), (10, 6, 2), (10, 6, 3), (10, 6, 4), (10, 6, 5), (10, 6, 6), (10, 6, 7), (10, 6, 8), (10, 6, 9), (10, 6, 10), (10, 7, 0), (10, 7, 1), (10, 7, 2), (10, 7, 3), (10, 7, 4), (10, 7, 5), (10, 7, 6), (10, 7, 7), (10, 7, 8), (10, 7, 9), (10, 7, 10), (10, 8, 0), (10, 8, 1), (10, 8, 2), (10, 8, 3), (10, 8, 4), (10, 8, 5), (10, 8, 6), (10, 8, 7), (10, 8, 8), (10, 8, 9), (10, 8, 10), (10, 9, 0), (10, 9, 1), (10, 9, 2), (10, 9, 3), (10, 9, 4), (10, 9, 5), (10, 9, 6), (10, 9, 7), (10, 9, 8), (10, 9, 9), (10, 9, 10), (10, 10, 0), (10, 10, 1), (10, 10, 2), (10, 10, 3), (10, 10, 4), (10, 10, 5), (10, 10, 6), (10, 10, 7), (10, 10, 8), (10, 10, 9), (10, 10, 10)} мощности $p^3 - 1 = 11^3 - 1 = 1331 - 1 = 1330$.

2.1.2. ПРОЕКТИВНАЯ ТОЧКА ПРОЕКТИВНОЙ ПЛОСКОСТИ

Проективной точкой проективной плоскости $\mathbf{P}^2(K)$ над полем K называется класс эквивалентности какой-либо последовательности вида (X, Y, Z), состоящей из не равных одновременно нулю элементов $X, Y, Z \in K$.

При этом, если в качестве поля K выступает $\mathbf{F}_p$ (поле вычетов по модулю p), проективная точка будет иметь мощность, равную $p - 1$.

Рассмотрим, например, классы эквивалентности проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$ над полем $K = \mathbf{F}_p = \mathbf{F}_3 =$ {0, 1, 2}. Заметим, что при этом $\lambda \in K^* = K \setminus \{0\} = \mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\} = \mathbf{F}_3 \setminus \{0\} = \{0, 1, 2\} \setminus \{0\} = \{1, 2\}$.

Так, элемент (0, 0, 1) проективной плоскости $\mathbf{P}^2(\mathbf{F}_3)$ при $\lambda = 1$ в соответствии с (2.1) эквивалентен сам себе:

$$(0, 0, 1) \equiv (1 \cdot 0 \pmod 3, 1 \cdot 0 \pmod 3, 1 \cdot 1 \pmod 3) \equiv (0, 0, 1),$$

а при $\lambda = 2$ эквивалентен элементу (0, 0, 2):

$$(0, 0, 1) \equiv (2 \cdot 0 \pmod 3, 2 \cdot 0 \pmod 3, 2 \cdot 1 \pmod 3) \equiv (0, 0, 2).$$

Элемент (0, 0, 2) проективной плоскости $\mathbf{P}^2(\mathbf{F}_3)$ при $\lambda = 1$ эквивалентен сам себе:

$$(0, 0, 2) \equiv (1 \cdot 0 \pmod 3, 1 \cdot 0 \pmod 3, 1 \cdot 2 \pmod 3) \equiv (0, 0, 2),$$

а при $\lambda = 2$ эквивалентен элементу (0, 0, 1):

$$(0, 0, 2) \equiv (2 \cdot 0 \pmod 3, 2 \cdot 0 \pmod 3, 2 \cdot 2 \pmod 3) \equiv (0, 0, 1).$$

Следовательно, классом эквивалентности элемента (0, 0, 1) является множество эквивалентных элементов C_1 = {(0, 0, 1), (0, 0, 2)}.

Аналогично, классом эквивалентности элемента (0, 1, 0) является множество эквивалентных элементов C_2 = {(0, 1, 0), (0, 2, 0)}.

Далее, классом эквивалентности элемента (0, 1, 1) является множество эквивалентных элементов C_3 = {(0, 1, 1), (0, 2, 2)}.

Остальными классами эквивалентности (проективными точками) проективной плоскости $\mathbf{P}^2(\mathbf{F}_3)$ являются множества:

C_4 = {(0, 1, 2), (0, 2, 1)},
C_5 = {(1, 0, 0), (2, 0, 0)},
C_6 = {(1, 0, 1), (2, 0, 2)},
C_7 = {(1, 0, 2), (2, 0, 1)},
C_8 = {(1, 1, 0), (2, 2, 0)},
C_9 = {(1, 1, 1), (2, 2, 2)},
C_{10} = {(1, 1, 2), (2, 2, 1)},
C_{11} = {(1, 2, 0), (2, 1, 0)},
C_{12} = {(1, 2, 1), (2, 1, 2)},
C_{13} = {(1, 2, 2), (2, 1, 1)}.

Заметим, что каждая из этих тринадцати проективных точек проективной плоскости $\mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$, имеет мощность, равную $p - 1 = 3 - 1 = 2$.

Во втором примере классами эквивалентности (проективными точками) проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_5)$ над полем $K = \mathbf{F}_p = \mathbf{F}_5 = \{0, 1, 2, 3, 4\}$ при $\lambda \in K^* = \mathbf{F}_p^* = \mathbf{F}_5^* = \{1, 2, 3, 4\}$ являются множества:

$C_1 = \{(0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4)\}$,
$C_2 = \{(0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 4, 0)\}$,
$C_3 = \{(0, 1, 1), (0, 2, 2), (0, 3, 3), (0, 4, 4)\}$,
$C_4 = \{(0, 1, 2), (0, 2, 4), (0, 3, 1), (0, 4, 3)\}$,
$C_5 = \{(0, 1, 3), (0, 2, 1), (0, 3, 4), (0, 4, 2)\}$,
$C_6 = \{(0, 1, 4), (0, 2, 3), (0, 3, 2), (0, 4, 1)\}$,
$C_7 = \{(1, 0, 0), (2, 0, 0), (3, 0, 0), (4, 0, 0)\}$,
$C_8 = \{(1, 0, 1), (2, 0, 2), (3, 0, 3), (4, 0, 4)\}$,
$C_9 = \{(1, 0, 2), (2, 0, 4), (3, 0, 1), (4, 0, 3)\}$,
$C_{10} = \{(1, 0, 3), (2, 0, 1), (3, 0, 4), (4, 0, 2)\}$,
$C_{11} = \{(1, 0, 4), (2, 0, 3), (3, 0, 2), (4, 0, 1)\}$,
$C_{12} = \{(1, 1, 0), (2, 2, 0), (3, 3, 0), (4, 4, 0)\}$,
$C_{13} = \{(1, 1, 1), (2, 2, 2), (3, 3, 3), (4, 4, 4)\}$,
$C_{14} = \{(1, 1, 2), (2, 2, 4), (3, 3, 1), (4, 4, 3)\}$,
$C_{15} = \{(1, 1, 3), (2, 2, 1), (3, 3, 4), (4, 4, 2)\}$,
$C_{16} = \{(1, 1, 4), (2, 2, 3), (3, 3, 2), (4, 4, 1)\}$,
$C_{17} = \{(1, 2, 0), (2, 4, 0), (3, 1, 0), (4, 3, 0)\}$,
$C_{18} = \{(1, 2, 1), (2, 4, 2), (3, 1, 3), (4, 3, 4)\}$,
$C_{19} = \{(1, 2, 2), (2, 4, 4), (3, 1, 1), (4, 3, 3)\}$,
$C_{20} = \{(1, 2, 3), (2, 4, 1), (3, 1, 4), (4, 3, 2)\}$,
$C_{21} = \{(1, 2, 4), (2, 4, 3), (3, 1, 2), (4, 3, 1)\}$,
$C_{22} = \{(1, 3, 0), (2, 1, 0), (3, 4, 0), (4, 2, 0)\}$,
$C_{23} = \{(1, 3, 1), (2, 1, 2), (3, 4, 3), (4, 2, 4)\}$,
$C_{24} = \{(1, 3, 2), (2, 1, 4), (3, 4, 1), (4, 2, 3)\}$,
$C_{25} = \{(1, 3, 3), (2, 1, 1), (3, 4, 4), (4, 2, 2)\}$,
$C_{26} = \{(1, 3, 4), (2, 1, 3), (3, 4, 2), (4, 2, 1)\}$,
$C_{27} = \{(1, 4, 0), (2, 3, 0), (3, 2, 0), (4, 1, 0)\}$,
$C_{28} = \{(1, 4, 1), (2, 3, 2), (3, 2, 3), (4, 1, 4)\}$,
$C_{29} = \{(1, 4, 2), (2, 3, 4), (3, 2, 1), (4, 1, 3)\}$,
$C_{30} = \{(1, 4, 3), (2, 3, 1), (3, 2, 4), (4, 1, 2)\}$,
$C_{31} = \{(1, 4, 4), (2, 3, 3), (3, 2, 2), (4, 1, 1)\}$.

Заметим, что каждая из этих тридцати одной проективной точки проективной плоскости $\mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_5)$, имеет мощность, равную $p - 1 = 5 - 1 = 4$.

В этой проективной плоскости, например, точки (2, 1, 3) и (3, 4, 2) эквивалентны, поскольку существует значение $(\lambda = 4) \in K^* = \mathbf{F}_p^* = \mathbf{F}_5^* = \{1, 2, 3, 4\}$, при котором:

$$(2, 1, 3) \equiv (4 \cdot 2 \pmod 5, 4 \cdot 1 \pmod 5, 4 \cdot 3 \pmod 5)) \equiv (3, 4, 2),$$

а точки, например, (2, 1, 3) и (4, 2, 3) эквивалентными не являются, поскольку не существует значения $\lambda \in K^* = \mathbf{F}_p^* = \mathbf{F}_5^* = \{1, 2, 3, 4\}$, обеспечивающего эквивалентность данных элементов проективной плоскости:

$$(2, 1, 3) \equiv (1 \cdot 2 \pmod 5, 1 \cdot 1 \pmod 5, 1 \cdot 3 \pmod 5)) \equiv (2, 1, 3) \neq (4, 2, 3),$$
$$(2, 1, 3) \equiv (2 \cdot 2 \pmod 5, 2 \cdot 1 \pmod 5, 2 \cdot 3 \pmod 5)) \equiv (4, 2, 1) \neq (4, 2, 3),$$
$$(2, 1, 3) \equiv (3 \cdot 2 \pmod 5, 3 \cdot 1 \pmod 5, 3 \cdot 3 \pmod 5)) \equiv (1, 3, 4) \neq (4, 2, 3),$$
$$(2, 1, 3) \equiv (4 \cdot 2 \pmod 5, 4 \cdot 1 \pmod 5, 4 \cdot 3 \pmod 5)) \equiv (3, 4, 2) \neq (4, 2, 3).$$

В третьем примере классами эквивалентности (проективными точками) проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$ над полем $K = \mathbf{F}_p = \mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ при $\lambda \in K^* = \mathbf{F}_p^* = \mathbf{F}_7^* = \{1, 2, 3, 4, 5, 6\}$ являются множества:

$$C_1 = \{(0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4), (0, 0, 5), (0, 0, 6)\},$$
$$C_2 = \{(0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 4, 0), (0, 5, 0), (0, 6, 0)\},$$
$$C_3 = \{(0, 1, 1), (0, 2, 2), (0, 3, 3), (0, 4, 4), (0, 5, 5), (0, 6, 6)\},$$
$$C_4 = \{(0, 1, 2), (0, 2, 4), (0, 3, 6), (0, 4, 1), (0, 5, 3), (0, 6, 5)\},$$
$$C_5 = \{(0, 1, 3), (0, 2, 6), (0, 3, 2), (0, 4, 5), (0, 5, 1), (0, 6, 4)\},$$
$$C_6 = \{(0, 1, 4), (0, 2, 1), (0, 3, 5), (0, 4, 2), (0, 5, 6), (0, 6, 3)\},$$
$$C_7 = \{(0, 1, 5), (0, 2, 3), (0, 3, 1), (0, 4, 6), (0, 5, 4), (0, 6, 2)\},$$
$$C_8 = \{(0, 1, 6), (0, 2, 5), (0, 3, 4), (0, 4, 3), (0, 5, 2), (0, 6, 1)\},$$
$$C_9 = \{(1, 0, 0), (2, 0, 0), (3, 0, 0), (4, 0, 0), (5, 0, 0), (6, 0, 0)\},$$
$$C_{10} = \{(1, 0, 1), (2, 0, 2), (3, 0, 3), (4, 0, 4), (5, 0, 5), (6, 0, 6)\},$$
$$C_{11} = \{(1, 0, 2), (2, 0, 4), (3, 0, 6), (4, 0, 1), (5, 0, 3), (6, 0, 5)\},$$
$$C_{12} = \{(1, 0, 3), (2, 0, 6), (3, 0, 2), (4, 0, 5), (5, 0, 1), (6, 0, 4)\},$$
$$C13 = \{(1, 0, 4), (2, 0, 1), (3, 0, 5), (4, 0, 2), (5, 0, 6), (6, 0, 3)\},$$
$$C_{14} = \{(1, 0, 5), (2, 0, 3), (3, 0, 1), (4, 0, 6), (5, 0, 4), (6, 0, 2)\},$$
$$C_{15} = \{(1, 0, 6), (2, 0, 5), (3, 0, 4), (4, 0, 3), (5, 0, 2), (6, 0, 1)\},$$
$$C_{16} = \{(1, 1, 0), (2, 2, 0), (3, 3, 0), (4, 4, 0), (5, 5, 0), (6, 6, 0)\},$$
$$C_{17} = \{(1, 1, 1), (2, 2, 2), (3, 3, 3), (4, 4, 4), (5, 5, 5), (6, 6, 6)\},$$
$$C_{18} = \{(1, 1, 2), (2, 2, 4), (3, 3, 6), (4, 4, 1), (5, 5, 3), (6, 6, 5)\},$$
$$C_{19} = \{(1, 1, 3), (2, 2, 6), (3, 3, 2), (4, 4, 5), (5, 5, 1), (6, 6, 4)\},$$
$$C_{20} = \{(1, 1, 4), (2, 2, 1), (3, 3, 5), (4, 4, 2), (5, 5, 6), (6, 6, 3)\},$$

C_{21} = {(1, 1, 5), (2, 2, 3), (3, 3, 1), (4, 4, 6), (5, 5, 4), (6, 6, 2)},

C_{22} = {(1, 1, 6), (2, 2, 5), (3, 3, 4), (4, 4, 3), (5, 5, 2), (6, 6, 1)},

C_{23} = {(1, 2, 0), (2, 4, 0), (3, 6, 0), (4, 1, 0), (5, 3, 0), (6, 5, 0)},

C_{24} = {(1, 2, 1), (2, 4, 2), (3, 6, 3), (4, 1, 4), (5, 3, 5), (6, 5, 6)},

C_{25} = {(1, 2, 2), (2, 4, 4), (3, 6, 6), (4, 1, 1), (5, 3, 3), (6, 5, 5)},

C_{26} = {(1, 2, 3), (2, 4, 6), (3, 6, 2), (4, 1, 5), (5, 3, 1), (6, 5, 4)},

C_{27} = {(1, 2, 4), (2, 4, 1), (3, 6, 5), (4, 1, 2), (5, 3, 6), (6, 5, 3)},

C_{28} = {(1, 2, 5), (2, 4, 3), (3, 6, 1), (4, 1, 6), (5, 3, 4), (6, 5, 2)},

C_{29} = {(1, 2, 6), (2, 4, 5), (3, 6, 4), (4, 1, 3), (5, 3, 2), (6, 5, 1)},

C_{30} = {(1, 3, 0), (2, 6, 0), (3, 2, 0), (4, 5, 0), (5, 1, 0), (6, 4, 0)},

C_{31} = {(1, 3, 1), (2, 6, 2), (3, 2, 3), (4, 5, 4), (5, 1, 5), (6, 4, 6)},

C_{32} = {(1, 3, 2), (2, 6, 4), (3, 2, 6), (4, 5, 1), (5, 1, 3), (6, 4, 5)},

C_{33} = {(1, 3, 3), (2, 6, 6), (3, 2, 2), (4, 5, 5), (5, 1, 1), (6, 4, 4)},

C_{34} = {(1, 3, 4), (2, 6, 1), (3, 2, 5), (4, 5, 2), (5, 1, 6), (6, 4, 3)},

C_{35} = {(1, 3, 5), (2, 6, 3), (3, 2, 1), (4, 5, 6), (5, 1, 4), (6, 4, 2)},

C_{36} = {(1, 3, 6), (2, 6, 5), (3, 2, 4), (4, 5, 3), (5, 1, 2), (6, 4, 1)},

C_{37} = {(1, 4, 0), (2, 1, 0), (3, 5, 0), (4, 2, 0), (5, 6, 0), (6, 3, 0)},

C_{38} = {(1, 4, 1), (2, 1, 2), (3, 5, 3), (4, 2, 4), (5, 6, 5), (6, 3, 6)},

C_{39} = {(1, 4, 2), (2, 1, 4), (3, 5, 6), (4, 2, 1), (5, 6, 3), (6, 3, 5)},

C_{40} = {(1, 4, 3), (2, 1, 6), (3, 5, 2), (4, 2, 5), (5, 6, 1), (6, 3, 4)},

C_{41} = {(1, 4, 4), (2, 1, 1), (3, 5, 5), (4, 2, 2), (5, 6, 6), (6, 3, 3)},

C_{42} = {(1, 4, 5), (2, 1, 3), (3, 5, 1), (4, 2, 6), (5, 6, 4), (6, 3, 2)},

C_{43} = {(1, 4, 6), (2, 1, 5), (3, 5, 4), (4, 2, 3), (5, 6, 2), (6, 3, 1)},

C_{44} = {(1, 5, 0), (2, 3, 0), (3, 1, 0), (4, 6, 0), (5, 4, 0), (6, 2, 0)},

C_{45} = {(1, 5, 1), (2, 3, 2), (3, 1, 3), (4, 6, 4), (5, 4, 5), (6, 2, 6)},

C_{46} = {(1, 5, 2), (2, 3, 4), (3, 1, 6), (4, 6, 1), (5, 4, 3), (6, 2, 5)},

C_{47} = {(1, 5, 3), (2, 3, 6), (3, 1, 2), (4, 6, 5), (5, 4, 1), (6, 2, 4)},

C_{48} = {(1, 5, 4), (2, 3, 1), (3, 1, 5), (4, 6, 2), (5, 4, 6), (6, 2, 3)},

C_{49} = {(1, 5, 5), (2, 3, 3), (3, 1, 1), (4, 6, 6), (5, 4, 4), (6, 2, 2)},

C_{50} = {(1, 5, 6), (2, 3, 5), (3, 1, 4), (4, 6, 3), (5, 4, 2), (6, 2, 1)},

C_{51} = {(1, 6, 0), (2, 5, 0), (3, 4, 0), (4, 3, 0), (5, 2, 0), (6, 1, 0)},

C_{52} = {(1, 6, 1), (2, 5, 2), (3, 4, 3), (4, 3, 4), (5, 2, 5), (6, 1, 6)},

C_{53} = {(1, 6, 2), (2, 5, 4), (3, 4, 6), (4, 3, 1), (5, 2, 3), (6, 1, 5)},

C_{54} = {(1, 6, 3), (2, 5, 6), (3, 4, 2), (4, 3, 5), (5, 2, 1), (6, 1, 4)},

C_{55} = {(1, 6, 4), (2, 5, 1), (3, 4, 5), (4, 3, 2), (5, 2, 6), (6, 1, 3)},

C_{56} = {(1, 6, 5), (2, 5, 3), (3, 4, 1), (4, 3, 6), (5, 2, 4), (6, 1, 2)},

C_{57} = {(1, 6, 6), (2, 5, 5), (3, 4, 4), (4, 3, 3), (5, 2, 2), (6, 1, 1)}.

Заметим, что каждая из этих пятидесяти семи проективных точек проективной плоскости $\mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$ имеет мощность, равную $p - 1 = 7 - 1 = 6$.

В четвертом примере классами эквивалентности (проективными точками) проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_{11})$ над полем $K = \mathbf{F}_p = \mathbf{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ при $\lambda \in K^* = \mathbf{F}_p^* = \mathbf{F}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ являются множества:

C_1 = {(0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4), (0, 0, 5), (0, 0, 6), (0, 0, 7), (0, 0, 8), (0, 0, 9), (0, 0, 10)},

C_2 = {(0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 4, 0), (0, 5, 0), (0, 6, 0), (0, 7, 0), (0, 8, 0), (0, 9, 0), (0, 10, 0)},

C_3 = {(0, 1, 1), (0, 2, 2), (0, 3, 3), (0, 4, 4), (0, 5, 5), (0, 6, 6), (0, 7, 7), (0, 8, 8), (0, 9, 9), (0, 10, 10)},

C_4 = {(0, 1, 2), (0, 2, 4), (0, 3, 6), (0, 4, 8), (0, 5, 10), (0, 6, 1), (0, 7, 3), (0, 8, 5), (0, 9, 7), (0, 10, 9)},

C_5 = {(0, 1, 3), (0, 2, 6), (0, 3, 9), (0, 4, 1), (0, 5, 4), (0, 6, 7), (0, 7, 10), (0, 8, 2), (0, 9, 5), (0, 10, 8)},

C_6 = {(0, 1, 4), (0, 2, 8), (0, 3, 1), (0, 4, 5), (0, 5, 9), (0, 6, 2), (0, 7, 6), (0, 8, 10), (0, 9, 3), (0, 10, 7)},

C_7 = {(0, 1, 5), (0, 2, 10), (0, 3, 4), (0, 4, 9), (0, 5, 3), (0, 6, 8), (0, 7, 2), (0, 8, 7), (0, 9, 1), (0, 10, 6)},

C_8 = {(0, 1, 6), (0, 2, 1), (0, 3, 7), (0, 4, 2), (0, 5, 8), (0, 6, 3), (0, 7, 9), (0, 8, 4), (0, 9, 10), (0, 10, 5)},

C_9 = {(0, 1, 7), (0, 2, 3), (0, 3, 10), (0, 4, 6), (0, 5, 2), (0, 6, 9), (0, 7, 5), (0, 8, 1), (0, 9, 8), (0, 10, 4)},

C_{10} = {(0, 1, 8), (0, 2, 5), (0, 3, 2), (0, 4, 10), (0, 5, 7), (0, 6, 4), (0, 7, 1), (0, 8, 9), (0, 9, 6), (0, 10, 3)},

C_{11} = {(0, 1, 9), (0, 2, 7), (0, 3, 5), (0, 4, 3), (0, 5, 1), (0, 6, 10), (0, 7, 8), (0, 8, 6), (0, 9, 4), (0, 10, 2)},

C_{12} = {(0, 1, 10), (0, 2, 9), (0, 3, 8), (0, 4, 7), (0, 5, 6), (0, 6, 5), (0, 7, 4), (0, 8, 3), (0, 9, 2), (0, 10, 1)},

C_{13} = {(1, 0, 0), (2, 0, 0), (3, 0, 0), (4, 0, 0), (5, 0, 0), (6, 0, 0), (7, 0, 0), (8, 0, 0), (9, 0, 0), (10, 0, 0)},

C_{14} = {(1, 0, 1), (2, 0, 2), (3, 0, 3), (4, 0, 4), (5, 0, 5), (6, 0, 6), (7, 0, 7), (8, 0, 8), (9, 0, 9), (10, 0, 10)},

C_{15} = {(1, 0, 2), (2, 0, 4), (3, 0, 6), (4, 0, 8), (5, 0, 10), (6, 0, 1), (7, 0, 3), (8, 0, 5), (9, 0, 7), (10, 0, 9)},

C_{16} = {(1, 0, 3), (2, 0, 6), (3, 0, 9), (4, 0, 1), (5, 0, 4), (6, 0, 7), (7, 0, 10), (8, 0, 2), (9, 0, 5), (10, 0, 8)},

C_{17} = {(1, 0, 4), (2, 0, 8), (3, 0, 1), (4, 0, 5), (5, 0, 9), (6, 0, 2), (7, 0, 6), (8, 0, 10), (9, 0, 3), (10, 0, 7)},

C_{18} = {(1, 0, 5), (2, 0, 10), (3, 0, 4), (4, 0, 9), (5, 0, 3), (6, 0, 8), (7, 0, 2), (8, 0, 7), (9, 0, 1), (10, 0, 6)},

C_{19} = {(1, 0, 6), (2, 0, 1), (3, 0, 7), (4, 0, 2), (5, 0, 8), (6, 0, 3), (7, 0, 9), (8, 0, 4), (9, 0, 10), (10, 0, 5)},

C_{20} = {(1, 0, 7), (2, 0, 3), (3, 0, 10), (4, 0, 6), (5, 0, 2), (6, 0, 9), (7, 0, 5), (8, 0, 1), (9, 0, 8), (10, 0, 4)},

C_{21} = {(1, 0, 8), (2, 0, 5), (3, 0, 2), (4, 0, 10), (5, 0, 7), (6, 0, 4), (7, 0, 1), (8, 0, 9), (9, 0, 6), (10, 0, 3)},

C_{22} = {(1, 0, 9), (2, 0, 7), (3, 0, 5), (4, 0, 3), (5, 0, 1), (6, 0, 10), (7, 0, 8), (8, 0, 6), (9, 0, 4), (10, 0, 2)},

C_{23} = {(1, 0, 10), (2, 0, 9), (3, 0, 8), (4, 0, 7), (5, 0, 6), (6, 0, 5), (7, 0, 4), (8, 0, 3), (9, 0, 2), (10, 0, 1)},

C_{24} = {(1, 1, 0), (2, 2, 0), (3, 3, 0), (4, 4, 0), (5, 5, 0), (6, 6, 0), (7, 7, 0), (8, 8, 0), (9, 9, 0), (10, 10, 0)},

C_{25} = {(1, 1, 1), (2, 2, 2), (3, 3, 3), (4, 4, 4), (5, 5, 5), (6, 6, 6), (7, 7, 7), (8, 8, 8), (9, 9, 9), (10, 10, 10)},

C_{26} = {(1, 1, 2), (2, 2, 4), (3, 3, 6), (4, 4, 8), (5, 5, 10), (6, 6, 1), (7, 7, 3), (8, 8, 5), (9, 9, 7), (10, 10, 9)},

C_{27} = {(1, 1, 3), (2, 2, 6), (3, 3, 9), (4, 4, 1), (5, 5, 4), (6, 6, 7), (7, 7, 10), (8, 8, 2), (9, 9, 5), (10, 10, 8)},

C_{28} = {(1, 1, 4), (2, 2, 8), (3, 3, 1), (4, 4, 5), (5, 5, 9), (6, 6, 2), (7, 7, 6), (8, 8, 10), (9, 9, 3), (10, 10, 7)},

C_{29} = {(1, 1, 5), (2, 2, 10), (3, 3, 4), (4, 4, 9), (5, 5, 3), (6, 6, 8), (7, 7, 2), (8, 8, 7), (9, 9, 1), (10, 10, 6)},

C_{30} = {(1, 1, 6), (2, 2, 1), (3, 3, 7), (4, 4, 2), (5, 5, 8), (6, 6, 3), (7, 7, 9), (8, 8, 4), (9, 9, 10), (10, 10, 5)},

C_{31} = {(1, 1, 7), (2, 2, 3), (3, 3, 10), (4, 4, 6), (5, 5, 2), (6, 6, 9), (7, 7, 5), (8, 8, 1), (9, 9, 8), (10, 10, 4)},

C_{32} = {(1, 1, 8), (2, 2, 5), (3, 3, 2), (4, 4, 10), (5, 5, 7), (6, 6, 4), (7, 7, 1), (8, 8, 9), (9, 9, 6), (10, 10, 3)},

C_{33} = {(1, 1, 9), (2, 2, 7), (3, 3, 5), (4, 4, 3), (5, 5, 1), (6, 6, 10), (7, 7, 8), (8, 8, 6), (9, 9, 4), (10, 10, 2)},

C_{34} = {(1, 1, 10), (2, 2, 9), (3, 3, 8), (4, 4, 7), (5, 5, 6), (6, 6, 5), (7, 7, 4), (8, 8, 3), (9, 9, 2), (10, 10, 1)},

C_{35} = {(1, 2, 0), (2, 4, 0), (3, 6, 0), (4, 8, 0), (5, 10, 0), (6, 1, 0), (7, 3, 0), (8, 5, 0), (9, 7, 0), (10, 9, 0)},

C_{36} = {(1, 2, 1), (2, 4, 2), (3, 6, 3), (4, 8, 4), (5, 10, 5), (6, 1, 6), (7, 3, 7), (8, 5, 8), (9, 7, 9), (10, 9, 10)},

C_{37} = {(1, 2, 2), (2, 4, 4), (3, 6, 6), (4, 8, 8), (5, 10, 10), (6, 1, 1), (7, 3, 3), (8, 5, 5), (9, 7, 7), (10, 9, 9)},

C_{38} = {(1, 2, 3), (2, 4, 6), (3, 6, 9), (4, 8, 1), (5, 10, 4), (6, 1, 7), (7, 3, 10), (8, 5, 2), (9, 7, 5), (10, 9, 8)},

C_{39} = {(1, 2, 4), (2, 4, 8), (3, 6, 1), (4, 8, 5), (5, 10, 9), (6, 1, 2), (7, 3, 6), (8, 5, 10), (9, 7, 3), (10, 9, 7)},

C_{40} = {(1, 2, 5), (2, 4, 10), (3, 6, 4), (4, 8, 9), (5, 10, 3), (6, 1, 8), (7, 3, 2), (8, 5, 7), (9, 7, 1), (10, 9, 6)},

C_{41} = {(1, 2, 6), (2, 4, 1), (3, 6, 7), (4, 8, 2), (5, 10, 8), (6, 1, 3), (7, 3, 9), (8, 5, 4), (9, 7, 10), (10, 9, 5)},

C_{42} = {(1, 2, 7), (2, 4, 3), (3, 6, 10), (4, 8, 6), (5, 10, 2), (6, 1, 9), (7, 3, 5), (8, 5, 1), (9, 7, 8), (10, 9, 4)},

C_{43} = {(1, 2, 8), (2, 4, 5), (3, 6, 2), (4, 8, 10), (5, 10, 7), (6, 1, 4), (7, 3, 1), (8, 5, 9), (9, 7, 6), (10, 9, 3)},

C_{44} = {(1, 2, 9), (2, 4, 7), (3, 6, 5), (4, 8, 3), (5, 10, 1), (6, 1, 10), (7, 3, 8), (8, 5, 6), (9, 7, 4), (10, 9, 2)},

C_{45} = {(1, 2, 10), (2, 4, 9), (3, 6, 8), (4, 8, 7), (5, 10, 6), (6, 1, 5), (7, 3, 4), (8, 5, 3), (9, 7, 2), (10, 9, 1)},

C_{46} = {(1, 3, 0), (2, 6, 0), (3, 9, 0), (4, 1, 0), (5, 4, 0), (6, 7, 0), (7, 10, 0), (8, 2, 0), (9, 5, 0), (10, 8, 0)},

C_{47} = {(1, 3, 1), (2, 6, 2), (3, 9, 3), (4, 1, 4), (5, 4, 5), (6, 7, 6), (7, 10, 7), (8, 2, 8), (9, 5, 9), (10, 8, 10)},

C_{48} = {(1, 3, 2), (2, 6, 4), (3, 9, 6), (4, 1, 8), (5, 4, 10), (6, 7, 1), (7, 10, 3), (8, 2, 5), (9, 5, 7), (10, 8, 9)},

C_{49} = {(1, 3, 3), (2, 6, 6), (3, 9, 9), (4, 1, 1), (5, 4, 4), (6, 7, 7), (7, 10, 10), (8, 2, 2), (9, 5, 5), (10, 8, 8)},

C_{50} = {(1, 3, 4), (2, 6, 8), (3, 9, 1), (4, 1, 5), (5, 4, 9), (6, 7, 2), (7, 10, 6), (8, 2, 10), (9, 5, 3), (10, 8, 7)},

C_{51} = {(1, 3, 5), (2, 6, 10), (3, 9, 4), (4, 1, 9), (5, 4, 3), (6, 7, 8), (7, 10, 2), (8, 2, 7), (9, 5, 1), (10, 8, 6)},

C_{52} = {(1, 3, 6), (2, 6, 1), (3, 9, 7), (4, 1, 2), (5, 4, 8), (6, 7, 3), (7, 10, 9), (8, 2, 4), (9, 5, 10), (10, 8, 5)},

C_{53} = {(1, 3, 7), (2, 6, 3), (3, 9, 10), (4, 1, 6), (5, 4, 2), (6, 7, 9), (7, 10, 5), (8, 2, 1), (9, 5, 8), (10, 8, 4)},

C_{54} = {(1, 3, 8), (2, 6, 5), (3, 9, 2), (4, 1, 10), (5, 4, 7), (6, 7, 4), (7, 10, 1), (8, 2, 9), (9, 5, 6), (10, 8, 3)},

C_{55} = {(1, 3, 9), (2, 6, 7), (3, 9, 5), (4, 1, 3), (5, 4, 1), (6, 7, 10), (7, 10, 8), (8, 2, 6), (9, 5, 4), (10, 8, 2)},

C_{56} = {(1, 3, 10), (2, 6, 9), (3, 9, 8), (4, 1, 7), (5, 4, 6), (6, 7, 5), (7, 10, 4), (8, 2, 3), (9, 5, 2), (10, 8, 1)},

C_{57} = {(1, 4, 0), (2, 8, 0), (3, 1, 0), (4, 5, 0), (5, 9, 0), (6, 2, 0), (7, 6, 0), (8, 10, 0), (9, 3, 0), (10, 7, 0)},

C_{58} = {(1, 4, 1), (2, 8, 2), (3, 1, 3), (4, 5, 4), (5, 9, 5), (6, 2, 6), (7, 6, 7), (8, 10, 8), (9, 3, 9), (10, 7, 10)},

C_{59} = {(1, 4, 2), (2, 8, 4), (3, 1, 6), (4, 5, 8), (5, 9, 10), (6, 2, 1), (7, 6, 3), (8, 10, 5), (9, 3, 7), (10, 7, 9)},

C_{60} = {(1, 4, 3), (2, 8, 6), (3, 1, 9), (4, 5, 1), (5, 9, 4), (6, 2, 7), (7, 6, 10), (8, 10, 2), (9, 3, 5), (10, 7, 8)},

C_{61} = {(1, 4, 4), (2, 8, 8), (3, 1, 1), (4, 5, 5), (5, 9, 9), (6, 2, 2), (7, 6, 6), (8, 10, 10), (9, 3, 3), (10, 7, 7)},

C_{62} = {(1, 4, 5), (2, 8, 10), (3, 1, 4), (4, 5, 9), (5, 9, 3), (6, 2, 8), (7, 6, 2), (8, 10, 7), (9, 3, 1), (10, 7, 6)},

C_{63} = {(1, 4, 6), (2, 8, 1), (3, 1, 7), (4, 5, 2), (5, 9, 8), (6, 2, 3), (7, 6, 9), (8, 10, 4), (9, 3, 10), (10, 7, 5)},

C_{64} = {(1, 4, 7), (2, 8, 3), (3, 1, 10), (4, 5, 6), (5, 9, 2), (6, 2, 9), (7, 6, 5), (8, 10, 1), (9, 3, 8), (10, 7, 4)},

C_{65} = {(1, 4, 8), (2, 8, 5), (3, 1, 2), (4, 5, 10), (5, 9, 7), (6, 2, 4), (7, 6, 1), (8, 10, 9), (9, 3, 6), (10, 7, 3)},

C_{66} = {(1, 4, 9), (2, 8, 7), (3, 1, 5), (4, 5, 3), (5, 9, 1), (6, 2, 10), (7, 6, 8), (8, 10, 6), (9, 3, 4), (10, 7, 2)},

C_{67} = {(1, 4, 10), (2, 8, 9), (3, 1, 8), (4, 5, 7), (5, 9, 6), (6, 2, 5), (7, 6, 4), (8, 10, 3), (9, 3, 2), (10, 7, 1)},

C_{68} = {(1, 5, 0), (2, 10, 0), (3, 4, 0), (4, 9, 0), (5, 3, 0), (6, 8, 0), (7, 2, 0), (8, 7, 0), (9, 1, 0), (10, 6, 0)},

C_{69} = {(1, 5, 1), (2, 10, 2), (3, 4, 3), (4, 9, 4), (5, 3, 5), (6, 8, 6), (7, 2, 7), (8, 7, 8), (9, 1, 9), (10, 6, 10)},

C_{70} = {(1, 5, 2), (2, 10, 4), (3, 4, 6), (4, 9, 8), (5, 3, 10), (6, 8, 1), (7, 2, 3), (8, 7, 5), (9, 1, 7), (10, 6, 9)},

C_{71} = {(1, 5, 3), (2, 10, 6), (3, 4, 9), (4, 9, 1), (5, 3, 4), (6, 8, 7), (7, 2, 10), (8, 7, 2), (9, 1, 5), (10, 6, 8)},

C_{72} = {(1, 5, 4), (2, 10, 8), (3, 4, 1), (4, 9, 5), (5, 3, 9), (6, 8, 2), (7, 2, 6), (8, 7, 10), (9, 1, 3), (10, 6, 7)},

C_{73} = {(1, 5, 5), (2, 10, 10), (3, 4, 4), (4, 9, 9), (5, 3, 3), (6, 8, 8), (7, 2, 2), (8, 7, 7), (9, 1, 1), (10, 6, 6)},

C_{74} = {(1, 5, 6), (2, 10, 1), (3, 4, 7), (4, 9, 2), (5, 3, 8), (6, 8, 3), (7, 2, 9), (8, 7, 4), (9, 1, 10), (10, 6, 5)},

C_{75} = {(1, 5, 7), (2, 10, 3), (3, 4, 10), (4, 9, 6), (5, 3, 2), (6, 8, 9), (7, 2, 5), (8, 7, 1), (9, 1, 8), (10, 6, 4)},

C_{76} = {(1, 5, 8), (2, 10, 5), (3, 4, 2), (4, 9, 10), (5, 3, 7), (6, 8, 4), (7, 2, 1), (8, 7, 9), (9, 1, 6), (10, 6, 3)},

C_{77} = {(1, 5, 9), (2, 10, 7), (3, 4, 5), (4, 9, 3), (5, 3, 1), (6, 8, 10), (7, 2, 8), (8, 7, 6), (9, 1, 4), (10, 6, 2)},

C_{78} = {(1, 5, 10), (2, 10, 9), (3, 4, 8), (4, 9, 7), (5, 3, 6), (6, 8, 5), (7, 2, 4), (8, 7, 3), (9, 1, 2), (10, 6, 1)},

C_{79} = {(1, 6, 0), (2, 1, 0), (3, 7, 0), (4, 2, 0), (5, 8, 0), (6, 3, 0), (7, 9, 0), (8, 4, 0), (9, 10, 0), (10, 5, 0)},

C_{80} = {(1, 6, 1), (2, 1, 2), (3, 7, 3), (4, 2, 4), (5, 8, 5), (6, 3, 6), (7, 9, 7), (8, 4, 8), (9, 10, 9), (10, 5, 10)},

C_{81} = {(1, 6, 2), (2, 1, 4), (3, 7, 6), (4, 2, 8), (5, 8, 10), (6, 3, 1), (7, 9, 3), (8, 4, 5), (9, 10, 7), (10, 5, 9)},

C_{82} = {(1, 6, 3), (2, 1, 6), (3, 7, 9), (4, 2, 1), (5, 8, 4), (6, 3, 7), (7, 9, 10), (8, 4, 2), (9, 10, 5), (10, 5, 8)},

C_{83} = {(1, 6, 4), (2, 1, 8), (3, 7, 1), (4, 2, 5), (5, 8, 9), (6, 3, 2), (7, 9, 6), (8, 4, 10), (9, 10, 3), (10, 5, 7)},

C_{84} = {(1, 6, 5), (2, 1, 10), (3, 7, 4), (4, 2, 9), (5, 8, 3), (6, 3, 8), (7, 9, 2), (8, 4, 7), (9, 10, 1), (10, 5, 6)},

C_{85} = {(1, 6, 6), (2, 1, 1), (3, 7, 7), (4, 2, 2), (5, 8, 8), (6, 3, 3), (7, 9, 9), (8, 4, 4), (9, 10, 10), (10, 5, 5)},

C_{86} = {(1, 6, 7), (2, 1, 3), (3, 7, 10), (4, 2, 6), (5, 8, 2), (6, 3, 9), (7, 9, 5), (8, 4, 1), (9, 10, 8), (10, 5, 4)},

C_{87} = {(1, 6, 8), (2, 1, 5), (3, 7, 2), (4, 2, 10), (5, 8, 7), (6, 3, 4), (7, 9, 1), (8, 4, 9), (9, 10, 6), (10, 5, 3)},

C_{88} = {(1, 6, 9), (2, 1, 7), (3, 7, 5), (4, 2, 3), (5, 8, 1), (6, 3, 10), (7, 9, 8), (8, 4, 6), (9, 10, 4), (10, 5, 2)},

C_{89} = {(1, 6, 10), (2, 1, 9), (3, 7, 8), (4, 2, 7), (5, 8, 6), (6, 3, 5), (7, 9, 4), (8, 4, 3), (9, 10, 2), (10, 5, 1)},

C_{90} = {(1, 7, 0), (2, 3, 0), (3, 10, 0), (4, 6, 0), (5, 2, 0), (6, 9, 0), (7, 5, 0), (8, 1, 0), (9, 8, 0), (10, 4, 0)},

C_{91} = {(1, 7, 1), (2, 3, 2), (3, 10, 3), (4, 6, 4), (5, 2, 5), (6, 9, 6), (7, 5, 7), (8, 1, 8), (9, 8, 9), (10, 4, 10)},

C_{92} = {(1, 7, 2), (2, 3, 4), (3, 10, 6), (4, 6, 8), (5, 2, 10), (6, 9, 1), (7, 5, 3), (8, 1, 5), (9, 8, 7), (10, 4, 9)},

C_{93} = {(1, 7, 3), (2, 3, 6), (3, 10, 9), (4, 6, 1), (5, 2, 4), (6, 9, 7), (7, 5, 10), (8, 1, 2), (9, 8, 5), (10, 4, 8)},

C_{94} = {(1, 7, 4), (2, 3, 8), (3, 10, 1), (4, 6, 5), (5, 2, 9), (6, 9, 2), (7, 5, 6), (8, 1, 10), (9, 8, 3), (10, 4, 7)},

C_{95} = {(1, 7, 5), (2, 3, 10), (3, 10, 4), (4, 6, 9), (5, 2, 3), (6, 9, 8), (7, 5, 2), (8, 1, 7), (9, 8, 1), (10, 4, 6)},

C_{96} = {(1, 7, 6), (2, 3, 1), (3, 10, 7), (4, 6, 2), (5, 2, 8), (6, 9, 3), (7, 5, 9), (8, 1, 4), (9, 8, 10), (10, 4, 5)},

C_{97} = {(1, 7, 7), (2, 3, 3), (3, 10, 10), (4, 6, 6), (5, 2, 2), (6, 9, 9), (7, 5, 5), (8, 1, 1), (9, 8, 8), (10, 4, 4)},

C_{98} = {(1, 7, 8), (2, 3, 5), (3, 10, 2), (4, 6, 10), (5, 2, 7), (6, 9, 4), (7, 5, 1), (8, 1, 9), (9, 8, 6), (10, 4, 3)},

C_{99} = {(1, 7, 9), (2, 3, 7), (3, 10, 5), (4, 6, 3), (5, 2, 1), (6, 9, 10), (7, 5, 8), (8, 1, 6), (9, 8, 4), (10, 4, 2)},

C_{100} = {(1, 7, 10), (2, 3, 9), (3, 10, 8), (4, 6, 7), (5, 2, 6), (6, 9, 5), (7, 5, 4), (8, 1, 3), (9, 8, 2), (10, 4, 1)},

C_{101} = {(1, 8, 0), (2, 5, 0), (3, 2, 0), (4, 10, 0), (5, 7, 0), (6, 4, 0), (7, 1, 0), (8, 9, 0), (9, 6, 0), (10, 3, 0)},

C_{102} = {(1, 8, 1), (2, 5, 2), (3, 2, 3), (4, 10, 4), (5, 7, 5), (6, 4, 6), (7, 1, 7), (8, 9, 8), (9, 6, 9), (10, 3, 10)},

C_{103} = {(1, 8, 2), (2, 5, 4), (3, 2, 6), (4, 10, 8), (5, 7, 10), (6, 4, 1), (7, 1, 3), (8, 9, 5), (9, 6, 7), (10, 3, 9)},

C_{104} = {(1, 8, 3), (2, 5, 6), (3, 2, 9), (4, 10, 1), (5, 7, 4), (6, 4, 7), (7, 1, 10), (8, 9, 2), (9, 6, 5), (10, 3, 8)},

C_{105} = {(1, 8, 4), (2, 5, 8), (3, 2, 1), (4, 10, 5), (5, 7, 9), (6, 4, 2), (7, 1, 6), (8, 9, 10), (9, 6, 3), (10, 3, 7)},

C_{106} = {(1, 8, 5), (2, 5, 10), (3, 2, 4), (4, 10, 9), (5, 7, 3), (6, 4, 8), (7, 1, 2), (8, 9, 7), (9, 6, 1), (10, 3, 6)},

C_{107} = {(1, 8, 6), (2, 5, 1), (3, 2, 7), (4, 10, 2), (5, 7, 8), (6, 4, 3), (7, 1, 9), (8, 9, 4), (9, 6, 10), (10, 3, 5)},

C_{108} = {(1, 8, 7), (2, 5, 3), (3, 2, 10), (4, 10, 6), (5, 7, 2), (6, 4, 9), (7, 1, 5), (8, 9, 1), (9, 6, 8), (10, 3, 4)},

C_{109} = {(1, 8, 8), (2, 5, 5), (3, 2, 2), (4, 10, 10), (5, 7, 7), (6, 4, 4), (7, 1, 1), (8, 9, 9), (9, 6, 6), (10, 3, 3)},

C_{110} = {(1, 8, 9), (2, 5, 7), (3, 2, 5), (4, 10, 3), (5, 7, 1), (6, 4, 10), (7, 1, 8), (8, 9, 6), (9, 6, 4), (10, 3, 2)},

C_{111} = {(1, 8, 10), (2, 5, 9), (3, 2, 8), (4, 10, 7), (5, 7, 6), (6, 4, 5), (7, 1, 4), (8, 9, 3), (9, 6, 2), (10, 3, 1)},

C_{112} = {(1, 9, 0), (2, 7, 0), (3, 5, 0), (4, 3, 0), (5, 1, 0), (6, 10, 0), (7, 8, 0), (8, 6, 0), (9, 4, 0), (10, 2, 0)},

C_{113} = {(1, 9, 1), (2, 7, 2), (3, 5, 3), (4, 3, 4), (5, 1, 5), (6, 10, 6), (7, 8, 7), (8, 6, 8), (9, 4, 9), (10, 2, 10)},

C_{114} = {(1, 9, 2), (2, 7, 4), (3, 5, 6), (4, 3, 8), (5, 1, 10), (6, 10, 1), (7, 8, 3), (8, 6, 5), (9, 4, 7), (10, 2, 9)},

C_{115} = {(1, 9, 3), (2, 7, 6), (3, 5, 9), (4, 3, 1), (5, 1, 4), (6, 10, 7), (7, 8, 10), (8, 6, 2), (9, 4, 5), (10, 2, 8)},

C_{116} = {(1, 9, 4), (2, 7, 8), (3, 5, 1), (4, 3, 5), (5, 1, 9), (6, 10, 2), (7, 8, 6), (8, 6, 10), (9, 4, 3), (10, 2, 7)},

C_{117} = {(1, 9, 5), (2, 7, 10), (3, 5, 4), (4, 3, 9), (5, 1, 3), (6, 10, 8), (7, 8, 2), (8, 6, 7), (9, 4, 1), (10, 2, 6)},

C_{118} = {(1, 9, 6), (2, 7, 1), (3, 5, 7), (4, 3, 2), (5, 1, 8), (6, 10, 3), (7, 8, 9), (8, 6, 4), (9, 4, 10), (10, 2, 5)},

C_{119} = {(1, 9, 7), (2, 7, 3), (3, 5, 10), (4, 3, 6), (5, 1, 2), (6, 10, 9), (7, 8, 5), (8, 6, 1), (9, 4, 8), (10, 2, 4)},

C_{120} = {(1, 9, 8), (2, 7, 5), (3, 5, 2), (4, 3, 10), (5, 1, 7), (6, 10, 4), (7, 8, 1), (8, 6, 9), (9, 4, 6), (10, 2, 3)},

C_{121} = {(1, 9, 9), (2, 7, 7), (3, 5, 5), (4, 3, 3), (5, 1, 1), (6, 10, 10), (7, 8, 8), (8, 6, 6), (9, 4, 4), (10, 2, 2)},

C_{122} = {(1, 9, 10), (2, 7, 9), (3, 5, 8), (4, 3, 7), (5, 1, 6), (6, 10, 5), (7, 8, 4), (8, 6, 3), (9, 4, 2), (10, 2, 1)},

C_{123} = {(1, 10, 0), (2, 9, 0), (3, 8, 0), (4, 7, 0), (5, 6, 0), (6, 5, 0), (7, 4, 0), (8, 3, 0), (9, 2, 0), (10, 1, 0)},

C_{124} = {(1, 10, 1), (2, 9, 2), (3, 8, 3), (4, 7, 4), (5, 6, 5), (6, 5, 6), (7, 4, 7), (8, 3, 8), (9, 2, 9), (10, 1, 10)},

C_{125} = {(1, 10, 2), (2, 9, 4), (3, 8, 6), (4, 7, 8), (5, 6, 10), (6, 5, 1), (7, 4, 3), (8, 3, 5), (9, 2, 7), (10, 1, 9)},

C_{126} = {(1, 10, 3), (2, 9, 6), (3, 8, 9), (4, 7, 1), (5, 6, 4), (6, 5, 7), (7, 4, 10), (8, 3, 2), (9, 2, 5), (10, 1, 8)},

C_{127} = {(1, 10, 4), (2, 9, 8), (3, 8, 1), (4, 7, 5), (5, 6, 9), (6, 5, 2), (7, 4, 6), (8, 3, 10), (9, 2, 3), (10, 1, 7)},

C_{128} = {(1, 10, 5), (2, 9, 10), (3, 8, 4), (4, 7, 9), (5, 6, 3), (6, 5, 8), (7, 4, 2), (8, 3, 7), (9, 2, 1), (10, 1, 6)},

C_{129} = {(1, 10, 6), (2, 9, 1), (3, 8, 7), (4, 7, 2), (5, 6, 8), (6, 5, 3), (7, 4, 9), (8, 3, 4), (9, 2, 10), (10, 1, 5)},

C_{130} = {(1, 10, 7), (2, 9, 3), (3, 8, 10), (4, 7, 6), (5, 6, 2), (6, 5, 9), (7, 4, 5), (8, 3, 1), (9, 2, 8), (10, 1, 4)},

C_{131} = {(1, 10, 8), (2, 9, 5), (3, 8, 2), (4, 7, 10), (5, 6, 7), (6, 5, 4), (7, 4, 1), (8, 3, 9), (9, 2, 6), (10, 1, 3)},

C_{132} = {(1, 10, 9), (2, 9, 7), (3, 8, 5), (4, 7, 3), (5, 6, 1), (6, 5, 10), (7, 4, 8), (8, 3, 6), (9, 2, 4), (10, 1, 2)},

C_{133} = {(1, 10, 10), (2, 9, 9), (3, 8, 8), (4, 7, 7), (5, 6, 6), (6, 5, 5), (7, 4, 4), (8, 3, 3), (9, 2, 2), (10, 1, 1)}.

Заметим, что каждая из этих ста тридцати трех проективных точек проективной плоскости $\mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_{11})$ имеет мощность, равную $p - 1 = 11 - 1 = 10$.

2.1.3. ЭЛЛИПТИЧЕСКАЯ КРИВАЯ (В ПРОЕКТИВНЫХ КООРДИНАТАХ)

Эллиптической кривой E называется множество точек проективной плоскости $\mathbf{P}^2(K)$, удовлетворяющих однородному уравнению Вейерштрасса (*длинной форме Вейерштрасса*):

$$F(X,Y,Z) = -X^3 + Y^2Z + a_1XYZ - a_2X^2Z + a_3YZ^2 - a_4XZ^2 - a_6Z^3 = 0, \qquad (2.2)$$

где коэффициенты (с исторически сложившимися обозначениями) a_1, a_2, a_3, a_4, $a_6 \in K$.

Пусть в качестве поля K выступает поле вычетов по простому модулю p, обозначаемое символом $\mathbf{F}_p$, и пусть при этом, например, $p = 3$. Вычислим значения функции Вейерштрасса $F(X,Y,Z) = -X^3 + Y^2Z + a_1XYZ - a_2X^2Z + a_3YZ^2 - a_4XZ^2 - a_6Z^3$ для точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$:

(0, 0, 1): $F(X,Y,Z) = -X^3 + Y^2Z + a_1XYZ - a_2X^2Z + a_3YZ^2 - a_4XZ^2 - a_6Z^3 =$

$= -X^3 + Y^2Z + 0 \cdot XYZ - 0 \cdot X^2Z + 0 \cdot YZ^2 - 2 \cdot XZ^2 - 1 \cdot Z^3 =$

$= -X^3 + Y^2Z - 2XZ^2 - Z^3 =$

$= -0^3 + 0^2 \cdot 1 - 2 \cdot 0 \cdot 1^2 - 1^3 = -1 \pmod 3 = 2,$

(0, 0, 2): $F(X,Y,Z) = -X^3 + Y^2Z - 2XZ^2 - Z^3 =$

$= -0^3 + 0^2 \cdot 2 - 2 \cdot 0 \cdot 2^2 - 2^3 = -8 \pmod 3 = 1,$

(0, 1, 0): $F(X,Y,Z) = -X^3 + Y^2Z - 2XZ^2 - Z^3 =$

$= -0^3 + 1^2 \cdot 0 - 2 \cdot 0 \cdot 0^2 - 0^3 = 0,$

(0, 1, 1): $F(X,Y,Z) = -X^3 + Y^2Z - 2XZ^2 - Z^3 =$

$= -0^3 + 1^2 \cdot 1 - 2 \cdot 0 \cdot 1^2 - 1^3 = 1 - 1 = 0,$

(0, 1, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -0^3+1^2\cdot 2-2\cdot 0\cdot 2^2-2^3 = 2-8 = -6 \pmod 3 = 0,$

(0, 2, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -0^3+2^2\cdot 0-2\cdot 0\cdot 0^2-0^3 = 0,$

(0, 2, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -0^3+2^2\cdot 1-2\cdot 0\cdot 1^2-1^3 = 4-1 = 3 \pmod 3 = 0,$

(0, 2, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -0^3+2^2\cdot 2-2\cdot 0\cdot 2^2-2^3 = 8-8 = 0,$

(1, 0, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+0^2\cdot 0-2\cdot 1\cdot 0^2-0^3 = -1 \pmod 3 = 2,$

(1, 0, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+0^2\cdot 1-2\cdot 1\cdot 1^2-1^3 = -1-2-1 = -4 \pmod 3 = 2,$

(1, 0, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+0^2\cdot 2-2\cdot 1\cdot 2^2-2^3 = -1-8-8 = -17 \pmod 3 = 1,$

(1, 1, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+1^2\cdot 0-2\cdot 1\cdot 0^2-0^3 = -1 \pmod 3 = 2,$

(1, 1, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+1^2\cdot 1-2\cdot 1\cdot 1^2-1^3 = -1+1-2-1 = -3 \pmod 3 = 0,$

(1, 1, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+1^2\cdot 2-2\cdot 1\cdot 2^2-2^3 = -1+2-8-8 = -15 \pmod 3 = 0,$

(1, 2, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+2^2\cdot 0-2\cdot 1\cdot 0^2-0^3 = -1 \pmod 3 = 2,$

(1, 2, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+2^2\cdot 1-2\cdot 1\cdot 1^2-1^3 = -1+4-2-1 = 0,$

(1, 2, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -1^3+2^2\cdot 2-2\cdot 1\cdot 2^2-2^3 = -1+8-8-8 = -9 \pmod 3 = 0,$

(2, 0, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+0^2\cdot 0-2\cdot 2\cdot 0^2-0^3 = -8 \pmod 3 = 1,$

(2, 0, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+0^2\cdot 1-2\cdot 2\cdot 1^2-1^3 = -8-4-1 = -13 \pmod 3 = 2,$

(2, 0, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+0^2\cdot 2-2\cdot 2\cdot 2^2-2^3 = -8-16-8 = -32 \pmod 3 = 1,$

(2, 1, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+1^2\cdot 0-2\cdot 2\cdot 0^2-0^3 = -8 \pmod 3 = 1,$

(2, 1, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+1^2\cdot 1-2\cdot 2\cdot 1^2-1^3 = -8+1-4-1 = -12 \pmod 3 = 0,$

(2, 1, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+1^2\cdot 2-2\cdot 2\cdot 2^2-2^3 = -8+2-16-8 = -30 \pmod 3 = 0,$

(2, 2, 0): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+2^2\cdot 0-2\cdot 2\cdot 0^2-0^3 = -8 \pmod 3 = 1,$

(2, 2, 1): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+2^2\cdot 1-2\cdot 2\cdot 1^2-1^3 = -8+4-4-1 = -9 \pmod 3 = 0,$

(2, 2, 2): $F(X,Y,Z) = -X^3+Y^2Z-2XZ^2-Z^3 =$

$= -2^3+2^2\cdot 2-2\cdot 2\cdot 2^2-2^3 = -8+8-16-8 = -24 \pmod 3 = 0.$

Следовательно, множеством точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$, удовлетворяющих длинной форме Вейерштрасса (2.2) при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$, является множество

{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 1, 1), (1, 1, 2), (1, 2, 1),
(1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)} (2.3)

мощности 14.

Пусть во втором примере в качестве поля K выступает поле вычетов $\mathbf{F}_p$ по простому модулю $p = 5$. Тогда множеством точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_5)$, удовлетворяющих длинной форме Вейерштрасса (2.2) при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, является множество

{(0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 4, 0), (1, 0, 4), (1, 2, 1), (1, 3, 2), (1, 4, 1),
(1, 4, 2), (1, 4, 4), (2, 0, 3), (2, 1, 4), (2, 3, 2), (2, 3, 3), (2, 3, 4), (2, 4, 2),
(3, 0, 2), (3, 1, 3), (3, 2, 1), (3, 2, 2), (3, 2, 3), (3, 4, 1), (4, 0, 1), (4, 1, 1),
(4, 1, 3), (4, 1, 4), (4, 2, 3), (4, 3, 4)} (2.4)

мощности 28.

В третьем примере, когда в качестве поля K выступает поле вычетов $\mathbf{F}_p$ по простому модулю p = 7, множеством точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$, удовлетворяющих длинной форме Вейерштрасса (2.2) при a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_6 = 3, является множество

{(0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 4, 0), (0, 5, 0), (0, 6, 0), (1, 0, 3),
(1, 1, 6), (1, 2, 2), (1, 5, 2), (1, 6, 6), (2, 0, 6), (2, 2, 5), (2, 3, 4), (2, 4, 4),
(2, 5, 5), (3, 0, 2), (3, 1, 6), (3, 3, 4), (3, 4, 4), (3, 6, 6), (4, 0, 5), (4, 1, 1),
(4, 3, 3), (4, 4, 3), (4, 6, 1), (5, 0, 1), (5, 2, 2), (5, 3, 3), (5, 4, 3), (5, 5, 2),
(6, 0, 4), (6, 1, 1), (6, 2, 5), (6, 5, 5), (6, 6, 1)} (2.5)

мощности 36.

В четвертом примере, когда в качестве поля K выступает поле вычетов $\mathbf{F}_p$ по простому модулю p = 11, множеством точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_{11})$, удовлетворяющих длинной форме Вейерштрасса (2.2) при a_1 = 10, a_2 = 4, a_3 = 2, a_4 = 0, a_6 = 4, является множество

{(0, 1, 0), (0, 1, 2), (0, 1, 4), (0, 2, 0), (0, 2, 4), (0, 2, 8), (0, 3, 0), (0, 3, 1),
(0, 3, 6), (0, 4, 0), (0, 4, 5), (0, 4, 8), (0, 5, 0), (0, 5, 9), (0, 5, 10), (0, 6, 0),
(0, 6, 1), (0, 6, 2), (0, 7, 0), (0, 7, 3), (0, 7, 6), (0, 8, 0), (0, 8, 5), (0, 8, 10),
(0, 9, 0), (0, 9, 3), (0, 9, 7), (0, 10, 0), (0, 10, 7), (0, 10, 9), (1, 0, 3), (1, 1, 2),
(1, 3, 5), (1, 4, 1), (1, 5, 4), (1, 6, 1), (1, 6, 3), (1, 6, 10), (1, 7, 2), (1, 7, 9),
(1, 8, 10), (1, 9, 9), (1, 10, 4), (1, 10, 5), (1, 10, 7), (2, 0, 6), (2, 1, 2), (2, 1, 6),
(2, 1, 9), (2, 2, 4), (2, 3, 4), (2, 3, 7), (2, 5, 9), (2, 6, 10), (2, 7, 7), (2, 8, 2),
(2, 9, 3), (2, 9, 8), (2, 9, 10), (2, 10, 8), (3, 0, 9), (3, 1, 3), (3, 2, 8), (3, 3, 6),
(3, 4, 1), (3, 5, 5), (3, 7, 3), (3, 7, 8), (3, 7, 9), (3, 8, 1), (3, 8, 4), (3, 8, 10),
(3, 9, 4), (3, 10, 5), (3, 10, 6), (4, 0, 1), (4, 1, 9), (4, 2, 1), (4, 2, 4), (4, 2, 7),
(4, 3, 3), (4, 4, 8), (4, 5, 4), (4, 6, 3), (4, 6, 8), (4, 7, 5), (4, 7, 6), (4, 7, 9),
(4, 9, 5), (4, 10, 7), (5, 0, 4), (5, 1, 1), (5, 2, 1), (5, 2, 10), (5, 3, 9), (5, 4, 3),
(5, 5, 10), (5, 6, 2), (5, 6, 3), (5, 6, 9), (5, 7, 6), (5, 8, 4), (5, 8, 5), (5, 8, 6),
(5, 9, 5), (6, 0, 7), (6, 2, 6), (6, 3, 5), (6, 3, 6), (6, 3, 7), (6, 4, 5), (6, 5, 2),
(6, 5, 8), (6, 5, 9), (6, 6, 1), (6, 7, 8), (6, 8, 2), (6, 9, 1), (6, 9, 10), (6, 10, 10),
(7, 0, 10), (7, 1, 4), (7, 2, 6), (7, 4, 2), (7, 4, 5), (7, 4, 6), (7, 5, 3), (7, 5, 8),
(7, 6, 7), (7, 7, 3), (7, 8, 8), (7, 9, 4), (7, 9, 7), (7, 9, 10), (7, 10, 2), (8, 0, 2),
(8, 1, 5), (8, 1, 6), (8, 2, 7), (8, 3, 1), (8, 3, 7), (8, 3, 10), (8, 4, 2), (8, 4, 3),
(8, 4, 8), (8, 6, 6), (8, 7, 10), (8, 8, 5), (8, 9, 3), (8, 10, 8), (9, 0, 5), (9, 1, 3),
(9, 2, 1), (9, 2, 3), (9, 2, 8), (9, 3, 9), (9, 4, 4), (9, 5, 1), (9, 6, 2), (9, 8, 4),
(9, 8, 7), (9, 9, 7), (9, 10, 2), (9, 10, 5), (9, 10, 9), (10, 0, 8), (10, 1, 4),
(10, 1, 6), (10, 1, 7), (10, 2, 2), (10, 3, 1), (10, 4, 2), (10, 4, 9), (10, 5, 1),
(10, 5, 8), (10, 5, 10), (10, 6, 7), (10, 7, 10), (10, 8, 6), (10, 10, 9)} (2.6)

мощности 180.

Эллиптическая кривая должна быть неособой в том смысле, что частные производные функции Вейерштрасса $F(X,Y,Z)$

$$\frac{\partial F}{\partial X} = -3X^2 + a_1 YZ - 2a_2 XZ - a_4 Z^2, \quad (2.7)$$

$$\frac{\partial F}{\partial Y} = 2YZ + a_1 XZ + a_3 Z^2, \quad (2.8)$$

$$\frac{\partial F}{\partial Z} = Y^2 + a_1 XY - a_2 X^2 + 2a_3 YZ - 2a_4 XZ - 3a_6 Z^2 \quad (2.9)$$

не должны обращаться в нуль одновременно ни в одной ее точке.

В первом примере, когда в качестве поля K выступает поле вычетов $\mathbf{F}_p = \mathbf{F}_3$, в множестве точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.3), ни в одной из точек не обращаются в нуль одновременно частные производные (2.7) – (2.9).

Поэтому множество точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_3)$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$, в которых не обращаются в нуль одновременно ни в одной его точке частные производные $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ и $\frac{\partial F}{\partial Z}$, равно множеству (2.3).

Во втором примере в качестве поля K выступает поле вычетов $\mathbf{F}_p = \mathbf{F}_5$ и в множестве точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_5)$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.4), также ни в одной из точек не обращаются в нуль одновременно частные производные (2.7) – (2.9).

Следовательно, множество точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_5)$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, в которых не обращаются в нуль одновременно ни в одной его точке частные производные $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ и $\frac{\partial F}{\partial Z}$, равно множеству (2.4).

В третьем примере, когда в качестве поля K выступает поле вычетов $\mathbf{F}_p = \mathbf{F}_7$, в множестве точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.5), так же, как и в первых двух примерах, ни в одной из точек не обращаются в нуль одновременно частные производные (2.7) – (2.9).

Поэтому множество точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, в которых не обращаются в нуль одновременно ни в одной его точке частные производные $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ и $\frac{\partial F}{\partial Z}$, равно множеству (2.5).

В четвертом примере, когда в качестве поля K выступает поле вычетов $\mathbf{F}_p = \mathbf{F}_{11}$, в множестве точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_{11})$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.6), так же, как и в первых трех примерах, ни в одной из точек не обращаются в нуль одновременно частные производные (2.7) – (2.9).

Поэтому множество точек проективной плоскости $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_{11})$, удовлетворяющих длинной форме Вейерштрасса при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, в которых не обращаются в нуль одновременно ни в одной его точке частные производные $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ и $\frac{\partial F}{\partial Z}$, равно множеству (2.6).

Множество K-рациональных точек эллиптической кривой E, т.е. точек проективной плоскости $\mathbf{P}^2(K)$, удовлетворяющих уравнению кривой, обозначается через $E(K)$. Заметим, что эллиптическая кривая E имеет ровно одну точку, чья координата Z равна нулю, а именно точку (0, 1, 0). Ее принято называть *бесконечно удаленной точкой* (или просто *точкой на бесконечности*) и обозначать символом O.

В первом примере, исключив из множества (2.3) точку (0, 2, 0), чья координата Z равна нулю, и отличную от бесконечно удаленной точки (0, 1, 0), получим эллиптическую кривую над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$:

$$E = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 1), (0, 2, 2), (1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\} \quad (2.10)$$

мощности 13.

Во втором примере исключим из множества (2.4) точки (0, 2, 0), (0, 3, 0) и (0, 4, 0), чьи координаты Z равны нулю, отличные от бесконечно удаленной точки (0, 1, 0), и в результате получим эллиптическую кривую над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$:

$$E = \{(0, 1, 0), (1, 0, 4), (1, 2, 1), (1, 3, 2), (1, 4, 1), (1, 4, 2), (1, 4, 4), (2, 0, 3), (2, 1, 4), (2, 3, 2), (2, 3, 3), (2, 3, 4), (2, 4, 2), (3, 0, 2), (3, 1, 3), (3, 2, 1), (3, 2, 2), (3, 2, 3), (3, 4, 1), (4, 0, 1), (4, 1, 1), (4, 1, 3), (4, 1, 4), (4, 2, 3), (4, 3, 4)\} \quad (2.11)$$

мощности 25.

В третьем примере, исключив из множества (2.5) точки (0, 2, 0), (0, 3, 0), (0, 4, 0), (0, 5, 0), (0, 6, 0), чьи координаты Z равны нулю, и отличные от бесконечно удаленной точки (0, 1, 0), получим эллиптическую кривую над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$:

$$E = \{(0, 1, 0), (1, 0, 3), (1, 1, 6), (1, 2, 2), (1, 5, 2), (1, 6, 6), (2, 0, 6),$$
$$(2, 2, 5), (2, 3, 4), (2, 4, 4), (2, 5, 5), (3, 0, 2), (3, 1, 6), (3, 3, 4), (3, 4, 4), (3, 6, 6),$$
$$(4, 0, 5), (4, 1, 1), (4, 3, 3), (4, 4, 3), (4, 6, 1), (5, 0, 1), (5, 2, 2), (5, 3, 3), (5, 4, 3),$$
$$(5, 5, 2), (6, 0, 4), (6, 1, 1), (6, 2, 5), (6, 5, 5), (6, 6, 1)\} \quad (2.12)$$

мощности 31.

В четвертом примере, исключив из множества (2.6) точки (0, 2, 0), (0, 3, 0), (0, 4, 0), (0, 5, 0), (0, 6, 0), (0, 7, 0), (0, 8, 0), (0, 9, 0), (0, 10, 0), чьи координаты Z равны нулю, и отличные от бесконечно удаленной точки (0, 1, 0), получим эллиптическую кривую над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$:

$$E = \{(0, 1, 0), (0, 1, 2), (0, 1, 4), (0, 2, 4), (0, 2, 8), (0, 3, 1), (0, 3, 6),$$
$$(0, 4, 5), (0, 4, 8), (0, 5, 9), (0, 5, 10), (0, 6, 1), (0, 6, 2), (0, 7, 3),$$
$$(0, 7, 6), (0, 8, 5), (0, 8, 10), (0, 9, 3), (0, 9, 7), (0, 10, 7), (0, 10, 9),$$
$$(1, 0, 3), (1, 1, 2), (1, 3, 5), (1, 4, 1), (1, 5, 4), (1, 6, 1), (1, 6, 3),$$
$$(1, 6, 10), (1, 7, 2), (1, 7, 9), (1, 8, 10), (1, 9, 9), (1, 10, 4), (1, 10, 5),$$
$$(1, 10, 7), (2, 0, 6), (2, 1, 2), (2, 1, 6), (2, 1, 9), (2, 2, 4), (2, 3, 4),$$
$$(2, 3, 7), (2, 5, 9), (2, 6, 10), (2, 7, 7), (2, 8, 2), (2, 9, 3), (2, 9, 8),$$
$$(2, 9, 10), (2, 10, 8), (3, 0, 9), (3, 1, 3), (3, 2, 8), (3, 3, 6), (3, 4, 1),$$
$$(3, 5, 5), (3, 7, 3), (3, 7, 8), (3, 7, 9), (3, 8, 1), (3, 8, 4), (3, 8, 10),$$
$$(3, 9, 4), (3, 10, 5), (3, 10, 6), (4, 0, 1), (4, 1, 9), (4, 2, 1), (4, 2, 4),$$
$$(4, 2, 7), (4, 3, 3), (4, 4, 8), (4, 5, 4), (4, 6, 3), (4, 6, 8), (4, 7, 5),$$
$$(4, 7, 6), (4, 7, 9), (4, 9, 5), (4, 10, 7), (5, 0, 4), (5, 1, 1), (5, 2, 1),$$
$$(5, 2, 10), (5, 3, 9), (5, 4, 3), (5, 5, 10), (5, 6, 2), (5, 6, 3), (5, 6, 9),$$
$$(5, 7, 6), (5, 8, 4), (5, 8, 5), (5, 8, 6), (5, 9, 5), (6, 0, 7), (6, 2, 6),$$
$$(6, 3, 5), (6, 3, 6), (6, 3, 7), (6, 4, 5), (6, 5, 2), (6, 5, 8), (6, 5, 9),$$
$$(6, 6, 1), (6, 7, 8), (6, 8, 2), (6, 9, 1), (6, 9, 10), (6, 10, 10), (7, 0, 10),$$
$$(7, 1, 4), (7, 2, 6), (7, 4, 2), (7, 4, 5), (7, 4, 6), (7, 5, 3), (7, 5, 8),$$
$$(7, 6, 7), (7, 7, 3), (7, 8, 8), (7, 9, 4), (7, 9, 7), (7, 9, 10), (7, 10, 2),$$
$$(8, 0, 2), (8, 1, 5), (8, 1, 6), (8, 2, 7), (8, 3, 1), (8, 3, 7), (8, 3, 10),$$
$$(8, 4, 2), (8, 4, 3), (8, 4, 8), (8, 6, 6), (8, 7, 10), (8, 8, 5), (8, 9, 3),$$
$$(8, 10, 8), (9, 0, 5), (9, 1, 3), (9, 2, 1), (9, 2, 3), (9, 2, 8), (9, 3, 9),$$
$$(9, 4, 4), (9, 5, 1), (9, 6, 2), (9, 8, 4), (9, 8, 7), (9, 9, 7), (9, 10, 2),$$
$$(9, 10, 5), (9, 10, 9), (10, 0, 8), (10, 1, 4), (10, 1, 6), (10, 1, 7),$$
$$(10, 2, 2), (10, 3, 1), (10, 4, 2), (10, 4, 9), (10, 5, 1), (10, 5, 8),$$
$$(10, 5, 10), (10, 6, 7), (10, 7, 10), (10, 8, 6), (10, 10, 9\} \quad (2.13)$$

мощности 171.

2.1.4. ЭЛЛИПТИЧЕСКАЯ КРИВАЯ (В АФФИННЫХ КООРДИНАТАХ)

Для удобства, вместо длинной формы Вейерштрасса (2.2) часто пользуются аффинной (в криволинейных координатах) версией уравнения Вейерштрасса, которому удовлетворяет эллиптическая кривая:

$$E: \qquad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{2.14}$$

где $a_1, a_2, a_3, a_4, a_6 \in K$.

В данном (аффинном) случае *K*-рациональными точками (эллиптической кривой) являются решения уравнения в K^2 и бесконечно удаленная точка *O*.

Пусть в первом примере в качестве поля K выступает поле вычетов по простому модулю *p*, обозначаемое символом $\mathbf{F}_p$ и пусть при этом $p = 3$. Установим, какие из элементов $K^2 = \mathbf{F}_p^2 = \mathbf{F}_p \times \mathbf{F}_p = \mathbf{F}_3 \times \mathbf{F}_3 = \{0, 1, 2\} \times \{0, 1, 2\} = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\}$ удовлетворяют аффинной версии уравнения Вейерштрасса (2.14), например, при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$:

$$(0, 0): \; Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

$$Y^2 + 0 \cdot XY + 0 \cdot Y = X^3 + 0 \cdot X^2 + 2X + 1,$$

$$Y^2 = X^3 + 2X + 1,$$

$$0^2 = 0^3 + 2 \cdot 0 + 1,$$

$$0 = 1 \text{ (ЛОЖЬ)},$$

$$(0, 1): \; Y^2 = X^3 + 2X + 1,$$

$$1^2 = 0^3 + 2 \cdot 0 + 1,$$

$$1 = 1 \text{ (ИСТИНА)},$$

$$(0, 2): \; Y^2 = X^3 + 2X + 1,$$

$$2^2 = 0^3 + 2 \cdot 0 + 1,$$

$$4 \pmod 3 = 1,$$

$$1 = 1 \text{ (ИСТИНА)},$$

$$(1, 0): \; Y^2 = X^3 + 2X + 1,$$

$$0^2 = 1^3 + 2 \cdot 1 + 1,$$

$$0 = 1 + 2 + 1,$$

$$0 = 4 \pmod 3,$$

$$0 = 1 \text{ (ЛОЖЬ)},$$

$$(1, 1): \; Y^2 = X^3 + 2X + 1,$$

$$1^2 = 1^3 + 2 \cdot 1 + 1,$$

$$1 = 1 + 2 + 1,$$

$$1 = 4 \pmod 3,$$

$$1 = 1 \text{ (ИСТИНА)},$$

$$(1, 2): \; Y^2 = X^3 + 2X + 1,$$

$$2^2 = 1^3 + 2 \cdot 1 + 1,$$

$$4 = 1 + 2 + 1,$$

$$4 \pmod 3 = 4 \pmod 3,$$

$$1 = 1 \text{ (ИСТИНА)},$$

$$(2, 0): \; Y^2 = X^3 + 2X + 1,$$

$$0^2 = 2^3 + 2 \cdot 2 + 1,$$

$$0 = 8 + 4 + 1,$$

$$0 = 13 \pmod 3,$$

$$0 = 1 \text{ (ЛОЖЬ)},$$

$$(2, 1): \; Y^2 = X^3 + 2X + 1,$$

$$1^2 = 2^3 + 2 \cdot 2 + 1,$$

$$1 = 8 + 4 + 1,$$

$$1 = 13 \pmod 3,$$

$$1 = 1 \text{ (ИСТИНА)},$$

$$(2, 2): \; Y^2 = X^3 + 2X + 1,$$

$$2^2 = 2^3 + 2 \cdot 2 + 1,$$

$$4 = 8 + 4 + 1,$$

$$4 \pmod 3 = 13 \pmod 3,$$

$$1 = 1 \text{ (ИСТИНА)}.$$

Следовательно, в первом примере данного (аффинного) случая $\mathbf{F}_3$-рациональными точками (эллиптической кривой) являются решения уравнения (2.14) в $\mathbf{F}_3^2$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$:

$$\{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\} \qquad (2.15)$$

и бесконечно удаленная точка O.

Если во втором примере в качестве поля K выступает поле вычетов по простому модулю $p = 5$, то в этом (аффинном) случае $\mathbf{F}_5$-рациональными точками (эллиптической кривой) являются решения уравнения (2.14) в $\mathbf{F}_5^2 = \mathbf{F}_5 \times \mathbf{F}_5 = \{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3, 4\}$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$:

$$\{(1, 2), (1, 4), (3, 2), (3, 4), (4, 0), (4, 1)\} \qquad (2.16)$$

и бесконечно удаленная точка O.

Пусть в третьем примере в качестве поля K выступает поле вычетов по простому модулю $p = 7$. Тогда в данном (аффинном) случае $\mathbf{F}_7$-рациональными точками (эллиптической кривой) являются решения уравнения (2.14) в $\mathbf{F}_7^2 = \mathbf{F}_7 \times \mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\} \times \{0, 1, 2, 3, 4, 5, 6\}$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$:

$$\{(4, 1), (4, 6), (5, 0), (6, 1), (6, 6)\} \qquad (2.17)$$

и бесконечно удаленная точка O.

Если в четвертом примере в качестве поля K выступает поле вычетов по простому модулю $p = 11$, то в этом (аффинном) случае $\mathbf{F}_{11}$-рациональными точками (эллиптической кривой) являются решения уравнения (2.14) в $\mathbf{F}_{11}^2 = \mathbf{F}_{11} \times \mathbf{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \times \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$:

$$\{(0, 3), (0, 6), (1, 4), (1, 6), (3, 4), (3, 8), (4, 0), (4, 2), (5, 1), (5, 2),$$
$$(6, 6), (6, 9), (8, 3), (9, 2), (9, 5), (10, 3), (10, 5)\} \qquad (2.18)$$

и бесконечно удаленная точка O.

Хотя большинство протоколов в криптографии используют эллиптическую кривую в аффинном виде, с точки зрения вычислений бывает удобно перейти к проективным координатам. Заметим, что такой переход достаточно легко осуществить, поскольку:

– точка на бесконечности всегда переходит в бесконечно удаленную точку, как при переходе от аффинных координат к проективным, так и наоборот;

– проективная точка (X, Y, Z) эллиптической кривой, отличная от бесконечно удаленной ($Z \neq 0$), переходит в аффинную точку с координатами $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$;

– для того, чтобы найти проективные координаты аффинной точки (X, Y) эллиптической кривой, не лежащей на бесконечности, достаточно выбрать значения $Z \in K^*$ и вычислить координаты проективной точки $(X \cdot Z, Y \cdot Z, Z)$.

Рассмотрим переход проективных точек (X, Y, Z) эллиптической кривой (в первом примере) над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10), отличных от бесконечно удаленной точки ($Z \neq 0$), в аффинные точки вида $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$:

$$(X, Y, Z) = (0, 1, 1) \text{ переходит в } \left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{0}{1}, \frac{1}{1}\right) = (0, 1),$$

$$(X, Y, Z) = (0, 1, 2) \text{ переходит в } \left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{0}{2}, \frac{1}{2}\right) = (0, 1 \cdot 2^{-1} \pmod 3) = (0, 1 \cdot 2) = (0, 2),$$

$$(X, Y, Z) = (0, 2, 1) \text{ переходит в } \left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{0}{1}, \frac{2}{1}\right) = (0, 2),$$

$$(X, Y, Z) = (0, 2, 2) \text{ переходит в } \left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{0}{2}, \frac{2}{2}\right) = (0, 1),$$

$(X, Y, Z) = (1, 1, 1)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{1}{1}, \frac{1}{1}\right) = (1, 1)$,

$(X, Y, Z) = (1, 1, 2)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{1}{2}, \frac{1}{2}\right) = (1 \cdot 2^{-1} \pmod 3, 1 \cdot 2^{-1} \pmod 3) =$

$= (1 \cdot 2, 1 \cdot 2) = (2, 2)$,

$(X, Y, Z) = (1, 2, 1)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{1}{1}, \frac{2}{1}\right) = (1, 2)$,

$(X, Y, Z) = (1, 2, 2)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{1}{2}, \frac{2}{2}\right) = (1 \cdot 2^{-1} \pmod 3, 1) = (1 \cdot 2, 1) = (2, 1)$,

$(X, Y, Z) = (2, 1, 1)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{2}{1}, \frac{1}{1}\right) = (2, 1)$,

$(X, Y, Z) = (2, 1, 2)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{2}{2}, \frac{1}{2}\right) = (1, 1 \cdot 2^{-1} \pmod 3) = (1, 1 \cdot 2) = (1, 2)$,

$(X, Y, Z) = (2, 2, 1)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{2}{1}, \frac{2}{1}\right) = (2, 2)$,

$(X, Y, Z) = (2, 2, 2)$ переходит в $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{2}{2}, \frac{2}{2}\right) = (1, 1)$.

Обобщая рассмотренные переходы проективных точек вида (X, Y, Z) эллиптической кривой (в первом примере) над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10), отличных от бесконечно удаленной точки ($Z \neq 0$), в аффинные точки вида $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ имеем:

$(0, 1, 1)$ и $(0, 2, 2)$ переходят в $(0, 1)$,
$(0, 1, 2)$ и $(0, 2, 1)$ переходят в $(0, 2)$,
$(1, 1, 1)$ и $(2, 2, 2)$ переходят в $(1, 1)$,
$(1, 1, 2)$ и $(2, 2, 1)$ переходят в $(2, 2)$,
$(1, 2, 1)$ и $(2, 1, 2)$ переходят в $(1, 2)$,
$(1, 2, 2)$ и $(2, 1, 1)$ переходят в $(2, 1)$.

Представим переход проективных точек (X, Y, Z) эллиптической кривой (во втором примере) над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.11), отличных от бесконечно удаленной точки ($Z \neq 0$), в аффинные точки $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$:

$(1, 0, 4)$, $(2, 0, 3)$, $(3, 0, 2)$, $(4, 0, 1)$ переходят в $(4, 0)$,
$(1, 2, 1)$, $(2, 4, 2)$, $(3, 1, 3)$, $(4, 3, 4)$ переходят в $(1, 2)$,
$(1, 3, 2)$, $(2, 1, 4)$, $(3, 4, 1)$, $(4, 2, 3)$ переходят в $(3, 4)$,
$(1, 4, 1)$, $(2, 3, 2)$, $(3, 2, 3)$, $(4, 1, 4)$ переходят в $(1, 4)$,

(1, 4, 2), (2, 3, 4), (3, 2, 1), (4, 1, 3) переходят в (3, 2),

(1, 4, 4), (2, 3, 3), (3, 2, 2), (4, 1, 1) переходят в (4, 1).

Представим переход проективных точек (X, Y, Z) эллиптической кривой (в третьем примере) над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.12), отличных от бесконечно удаленной точки ($Z \neq 0$), в аффинные точки $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$:

(1, 0, 3), (2, 0, 6), (3, 0, 2), (4, 0, 5), (5, 0, 1), (6, 0, 4) переходят в (5, 0),

(1, 1, 6), (2, 2, 5), (3, 3, 4), (4, 4, 3), (5, 5, 2), (6, 6, 1) переходят в (6, 6),

(1, 2, 2), (2, 4, 4), (3, 6, 6), (4, 1, 1), (5, 3, 3), (6, 5, 5) переходят в (4, 1),

(1, 5, 2), (2, 3, 4), (3, 1, 6), (4, 6, 1), (5, 4, 3), (6, 2, 5) переходят в (4, 6),

(1, 6, 6), (2, 5, 5), (3, 4, 4), (4, 3, 3), (5, 2, 2), (6, 1, 1) переходят в (6, 1).

Представим переход проективных точек (X, Y, Z) эллиптической кривой (в четвертом примере) над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.13), отличных от бесконечно удаленной точки ($Z \neq 0$), в аффинные точки $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$:

(0, 1, 2) (0, 2, 4) (0, 3, 6) (0, 4, 8) (0, 5, 10) (0, 6, 1) (0, 7, 3) (0, 8, 5) (0, 9, 7) (0, 10, 9)
переходят в (0, 6),

(0, 1, 4) (0, 2, 8) (0, 3, 1) (0, 4, 5) (0, 5, 9) (0, 6, 2) (0, 7, 6) (0, 8, 10) (0, 9, 3) (0, 10, 7)
переходят в (0, 3),

(1, 0, 3) (2, 0, 6) (3, 0, 9) (4, 0, 1) (5, 0, 4) (6, 0, 7) (7, 0, 10) (8, 0, 2) (9, 0, 5) (10, 0, 8)
переходят в (4, 0),

(1, 1, 2) (2, 2, 4) (3, 3, 6) (4, 4, 8) (5, 5, 10) (6, 6, 1) (7, 7, 3) (8, 8, 5) (9, 9, 7) (10, 10, 9)
переходят в (6, 6),

(1, 3, 5) (2, 6, 10) (3, 9, 4) (4, 1, 9) (5, 4, 3) (6, 7, 8) (7, 10, 2) (8, 2, 7) (9, 5, 1) (10, 8, 6)
переходят в (9, 5),

(1, 4, 1) (2, 8, 2) (3, 1, 3) (4, 5, 4) (5, 9, 5) (6, 2, 6) (7, 6, 7) (8, 10, 8) (9, 3, 9) (10, 7, 10)
переходят в (1, 4),

(1, 5, 4) (2, 10, 8) (3, 4, 1) (4, 9, 5) (5, 3, 9) (6, 8, 2) (7, 2, 6) (8, 7, 10) (9, 1, 3) (10, 6, 7)
переходят в (3, 4),

(1, 6, 1) (2, 1, 2) (3, 7, 3) (4, 2, 4) (5, 8, 5) (6, 3, 6) (7, 9, 7) (8, 4, 8) (9, 10, 9) (10, 5, 10)
переходят в (1, 6),

(1, 6, 3) (2, 1, 6) (3, 7, 9) (4, 2, 1) (5, 8, 4) (6, 3, 7) (7, 9, 10) (8, 4, 2) (9, 10, 5) (10, 5, 8)
переходят в (4, 2),

(1, 6, 10) (2, 1, 9) (3, 7, 8) (4, 2, 7) (5, 8, 6) (6, 3, 5) (7, 9, 4) (8, 4, 3) (9, 10, 2) (10, 5, 1)
переходят в (10, 5),

(1, 7, 2) (2, 3, 4) (3, 10, 6) (4, 6, 8) (5, 2, 10) (6, 9, 1) (7, 5, 3) (8, 1, 5) (9, 8, 7) (10, 4, 9)
переходят в (6, 9),

(1, 7, 9) (2, 3, 7) (3, 10, 5) (4, 6, 3) (5, 2, 1) (6, 9, 10) (7, 5, 8) (8, 1, 6) (9, 8, 4) (10, 4, 2)

переходят в (5, 2),

(1, 8, 10) (2, 5, 9) (3, 2, 8) (4, 10, 7) (5, 7, 6) (6, 4, 5) (7, 1, 4) (8, 9, 3) (9, 6, 2) (10, 3, 1)

переходят в (10, 3),

(1, 9, 9) (2, 7, 7) (3, 5, 5) (4, 3, 3) (5, 1, 1) (6, 10, 10) (7, 8, 8) (8, 6, 6) (9, 4, 4) (10, 2, 2)

переходят в (5, 1),

(1, 10, 4) (2, 9, 8) (3, 8, 1) (4, 7, 5) (5, 6, 9) (6, 5, 2) (7, 4, 6) (8, 3, 10) (9, 2, 3) (10, 1, 7)

переходят в (3, 8),

(1, 10, 5) (2, 9, 10) (3, 8, 4) (4, 7, 9) (5, 6, 3) (6, 5, 8) (7, 4, 2) (8, 3, 7) (9, 2, 1) (10, 1, 6)

переходят в (9, 2),

(1, 10, 7) (2, 9, 3) (3, 8, 10) (4, 7, 6) (5, 6, 2) (6, 5, 9) (7, 4, 5) (8, 3, 1) (9, 2, 8) (10, 1, 4)

переходят в (8, 3).

Рассмотрим поиск проективных координат (X, Y, Z) эллиптической кривой (в первом примере) над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ по известным аффинным точкам (X, Y), не лежащим на бесконечности (2.15). Для этого выберем значения $Z \in K^* = \mathbf{F}_p^* = \mathbf{F}_3^* = \{0, 1, 2\}\backslash\{0\} = \{1, 2\}$ и вычислим координаты проективных точек ($X \cdot Z$, $Y \cdot Z$, Z):

(X, Y) = (0, 1), Z = 1: ($X \cdot Z$, $Y \cdot Z$, Z) = (0 · 1, 1 · 1, 1) = (0, 1, 1),

(X, Y) = (0, 1), Z = 2: ($X \cdot Z$, $Y \cdot Z$, Z) = (0 · 2, 1 · 2, 2) = (0, 2, 2),

(X, Y) = (0, 2), Z = 1: ($X \cdot Z$, $Y \cdot Z$, Z) = (0 · 1, 2 · 1, 1) = (0, 2, 1),

(X, Y) = (0, 2), Z = 2: ($X \cdot Z$, $Y \cdot Z$, Z) = (0 · 2, 2 · 2 (mod 3), 2) = (0, 4 (mod 3), 2) = (0, 1, 2),

(X, Y) = (1, 1), Z = 1: ($X \cdot Z$, $Y \cdot Z$, Z) = (1 · 1, 1 · 1, 1) = (1, 1, 1),

(X, Y) = (1, 1), Z = 2: ($X \cdot Z$, $Y \cdot Z$, Z) = (1 · 2, 1 · 2, 2) = (2, 2, 2),

(X, Y) = (1, 2), Z = 1: ($X \cdot Z$, $Y \cdot Z$, Z) = (1 · 1, 2 · 1, 1) = (1, 2, 1),

(X, Y) = (1, 2), Z = 2: ($X \cdot Z$, $Y \cdot Z$, Z) = (1 · 2, 2 · 2 (mod 3), 2) = (2, 4 (mod 3), 2) = (2, 1, 2),

(X, Y) = (2, 1), Z = 1: ($X \cdot Z$, $Y \cdot Z$, Z) = (2 · 1, 1 · 1, 1) = (2, 1, 1),

(X, Y) = (2, 1), Z = 2: ($X \cdot Z$, $Y \cdot Z$, Z) = (2 · 2 (mod 3), 1 · 2, 2) = (4 (mod 3), 2, 2) = (1, 2, 2),

(X, Y) = (2, 2), Z = 1: ($X \cdot Z$, $Y \cdot Z$, Z) = (2 · 1, 2 · 1, 1) = (2, 2, 1),

(X, Y) = (2, 2), Z = 2: ($X \cdot Z$, $Y \cdot Z$, Z) = (2 · 2 (mod 3), 2 · 2 (mod 3), 2) =

= (4 (mod 3), 4 (mod 3), 2) = (1, 1, 2).

Представим (во втором примере) переход аффинных точек (X, Y), не лежащих на бесконечности (2.16), эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ в проективные, осуществленный путем выбора значений $Z \in K^* = \mathbf{F}_p^* = \mathbf{F}_5^* = \{0, 1, 2, 3, 4\}\backslash\{0\} = \{1, 2, 3, 4\}$ и вычисления координат проективных точек ($X \cdot Z$, $Y \cdot Z$, Z):

(X, Y) = (1, 2), Z = 1: (1, 2) переходит в (1, 2, 1),

$(X, Y) = (1, 2)$, $Z = 2$: $(1, 2)$ переходит в $(2, 4, 2)$,
$(X, Y) = (1, 2)$, $Z = 3$: $(1, 2)$ переходит в $(3, 1, 3)$,
$(X, Y) = (1, 2)$, $Z = 4$: $(1, 2)$ переходит в $(4, 3, 4)$,
$(X, Y) = (1, 4)$, $Z = 1$: $(1, 4)$ переходит в $(1, 4, 1)$,
$(X, Y) = (1, 4)$, $Z = 2$: $(1, 4)$ переходит в $(2, 3, 2)$,
$(X, Y) = (1, 4)$, $Z = 3$: $(1, 4)$ переходит в $(3, 2, 3)$,
$(X, Y) = (1, 4)$, $Z = 4$: $(1, 4)$ переходит в $(4, 1, 4)$,
$(X, Y) = (3, 2)$, $Z = 1$: $(3, 2)$ переходит в $(3, 2, 1)$,
$(X, Y) = (3, 2)$, $Z = 2$: $(3, 2)$ переходит в $(1, 4, 2)$,
$(X, Y) = (3, 2)$, $Z = 3$: $(3, 2)$ переходит в $(4, 1, 3)$,
$(X, Y) = (3, 2)$, $Z = 4$: $(3, 2)$ переходит в $(2, 3, 4)$,
$(X, Y) = (3, 4)$, $Z = 1$: $(3, 4)$ переходит в $(3, 4, 1)$,
$(X, Y) = (3, 4)$, $Z = 2$: $(3, 4)$ переходит в $(1, 3, 2)$,
$(X, Y) = (3, 4)$, $Z = 3$: $(3, 4)$ переходит в $(4, 2, 3)$,
$(X, Y) = (3, 4)$, $Z = 4$: $(3, 4)$ переходит в $(2, 1, 4)$,
$(X, Y) = (4, 0)$, $Z = 1$: $(4, 0)$ переходит в $(4, 0, 1)$,
$(X, Y) = (4, 0)$, $Z = 2$: $(4, 0)$ переходит в $(3, 0, 2)$,
$(X, Y) = (4, 0)$, $Z = 3$: $(4, 0)$ переходит в $(2, 0, 3)$,
$(X, Y) = (4, 0)$, $Z = 4$: $(4, 0)$ переходит в $(1, 0, 4)$,
$(X, Y) = (4, 1)$, $Z = 1$: $(4, 1)$ переходит в $(4, 1, 1)$,
$(X, Y) = (4, 1)$, $Z = 2$: $(4, 1)$ переходит в $(3, 2, 2)$,
$(X, Y) = (4, 1)$, $Z = 3$: $(4, 1)$ переходит в $(2, 3, 3)$,
$(X, Y) = (4, 1)$, $Z = 4$: $(4, 1)$ переходит в $(1, 4, 4)$.

В третьем примере представим переход аффинных точек (X, Y), не лежащих на бесконечности (2.17), эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ в проективные, осуществленный путем выбора значений $Z \in K^* = \mathbf{F}_p^* =$ $= \mathbf{F}_7^* = \{0, 1, 2, 3, 4, 5, 6\} \setminus \{0\} = \{1, 2, 3, 4, 5, 6\}$ и вычисления координат проективных точек $(X \cdot Z,\ Y \cdot Z,\ Z)$:

$(X, Y) = (4, 1)$, $Z = 1$: $(4, 1)$ переходит в $(4, 1, 1)$,
$(X, Y) = (4, 1)$, $Z = 2$: $(4, 1)$ переходит в $(1, 2, 2)$,
$(X, Y) = (4, 1)$, $Z = 3$: $(4, 1)$ переходит в $(5, 3, 3)$,
$(X, Y) = (4, 1)$, $Z = 4$: $(4, 1)$ переходит в $(2, 4, 4)$,
$(X, Y) = (4, 1)$, $Z = 5$: $(4, 1)$ переходит в $(6, 5, 5)$,
$(X, Y) = (4, 1)$, $Z = 6$: $(4, 1)$ переходит в $(3, 6, 6)$,
$(X, Y) = (4, 6)$, $Z = 1$: $(4, 6)$ переходит в $(4, 6, 1)$,
$(X, Y) = (4, 6)$, $Z = 2$: $(4, 6)$ переходит в $(1, 5, 2)$,

$(X, Y) = (4, 6)$, $Z = 3$: $(4, 6)$ переходит в $(5, 4, 3)$,
$(X, Y) = (4, 6)$, $Z = 4$: $(4, 6)$ переходит в $(2, 3, 4)$,
$(X, Y) = (4, 6)$, $Z = 5$: $(4, 6)$ переходит в $(6, 2, 5)$,
$(X, Y) = (4, 6)$, $Z = 6$: $(4, 6)$ переходит в $(3, 1, 6)$,
$(X, Y) = (5, 0)$, $Z = 1$: $(5, 0)$ переходит в $(5, 0, 1)$,
$(X, Y) = (5, 0)$, $Z = 2$: $(5, 0)$ переходит в $(3, 0, 2)$,
$(X, Y) = (5, 0)$, $Z = 3$: $(5, 0)$ переходит в $(1, 0, 3)$,
$(X, Y) = (5, 0)$, $Z = 4$: $(5, 0)$ переходит в $(6, 0, 4)$,
$(X, Y) = (5, 0)$, $Z = 5$: $(5, 0)$ переходит в $(4, 0, 5)$,
$(X, Y) = (5, 0)$, $Z = 6$: $(5, 0)$ переходит в $(2, 0, 6)$,
$(X, Y) = (6, 1)$, $Z = 1$: $(6, 1)$ переходит в $(6, 1, 1)$,
$(X, Y) = (6, 1)$, $Z = 2$: $(6, 1)$ переходит в $(5, 2, 2)$,
$(X, Y) = (6, 1)$, $Z = 3$: $(6, 1)$ переходит в $(4, 3, 3)$,
$(X, Y) = (6, 1)$, $Z = 4$: $(6, 1)$ переходит в $(3, 4, 4)$,
$(X, Y) = (6, 1)$, $Z = 5$: $(6, 1)$ переходит в $(2, 5, 5)$,
$(X, Y) = (6, 1)$, $Z = 6$: $(6, 1)$ переходит в $(1, 6, 6)$,
$(X, Y) = (6, 6)$, $Z = 1$: $(6, 6)$ переходит в $(6, 6, 1)$,
$(X, Y) = (6, 6)$, $Z = 2$: $(6, 6)$ переходит в $(5, 5, 2)$,
$(X, Y) = (6, 6)$, $Z = 3$: $(6, 6)$ переходит в $(4, 4, 3)$,
$(X, Y) = (6, 6)$, $Z = 4$: $(6, 6)$ переходит в $(3, 3, 4)$,
$(X, Y) = (6, 6)$, $Z = 5$: $(6, 6)$ переходит в $(2, 2, 5)$,
$(X, Y) = (6, 6)$, $Z = 6$: $(6, 6)$ переходит в $(1, 1, 6)$.

В четвертом примере представим переход аффинных точек (X, Y), не лежащих на бесконечности (2.18), эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ в проективные, осуществленный путем выбора значений $Z \in K^* = \mathbf{F}_p^* = \mathbf{F}_{11}^* = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \setminus \{0\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ и вычисления координат проективных точек $(X \cdot Z, Y \cdot Z, Z)$:

$(X, Y) = (0, 3)$, $Z = 1$: $(0, 3)$ переходит в $(0, 3, 1)$,
$(X, Y) = (0, 3)$, $Z = 2$: $(0, 3)$ переходит в $(0, 6, 2)$,
$(X, Y) = (0, 3)$, $Z = 3$: $(0, 3)$ переходит в $(0, 9, 3)$,
$(X, Y) = (0, 3)$, $Z = 4$: $(0, 3)$ переходит в $(0, 1, 4)$,
$(X, Y) = (0, 3)$, $Z = 5$: $(0, 3)$ переходит в $(0, 4, 5)$,
$(X, Y) = (0, 3)$, $Z = 6$: $(0, 3)$ переходит в $(0, 7, 6)$,
$(X, Y) = (0, 3)$, $Z = 7$: $(0, 3)$ переходит в $(0, 10, 7)$,
$(X, Y) = (0, 3)$, $Z = 8$: $(0, 3)$ переходит в $(0, 2, 8)$,
$(X, Y) = (0, 3)$, $Z = 9$: $(0, 3)$ переходит в $(0, 5, 9)$,
$(X, Y) = (0, 3)$, $Z = 10$: $(0, 3)$ переходит в $(0, 8, 10)$,

(X, Y) = (0, 6), Z = 1: (0, 6) переходит в (0, 6, 1),

(X, Y) = (0, 6), Z = 2: (0, 6) переходит в (0, 1, 2),

(X, Y) = (0, 6), Z = 3: (0, 6) переходит в (0, 7, 3),

(X, Y) = (0, 6), Z = 4: (0, 6) переходит в (0, 2, 4),

(X, Y) = (0, 6), Z = 5: (0, 6) переходит в (0, 8, 5),

(X, Y) = (0, 6), Z = 6: (0, 6) переходит в (0, 3, 6),

(X, Y) = (0, 6), Z = 7: (0, 6) переходит в (0, 9, 7),

(X, Y) = (0, 6), Z = 8: (0, 6) переходит в (0, 4, 8),

(X, Y) = (0, 6), Z = 9: (0, 6) переходит в (0, 10, 9),

(X, Y) = (0, 6), Z = 10: (0, 6) переходит в (0, 5, 10),

(X, Y) = (1, 4), Z = 1: (1, 4) переходит в (1, 4, 1),

(X, Y) = (1, 4), Z = 2: (1, 4) переходит в (2, 8, 2),

(X, Y) = (1, 4), Z = 3: (1, 4) переходит в (3, 1, 3),

(X, Y) = (1, 4), Z = 4: (1, 4) переходит в (4, 5, 4),

(X, Y) = (1, 4), Z = 5: (1, 4) переходит в (5, 9, 5),

(X, Y) = (1, 4), Z = 6: (1, 4) переходит в (6, 2, 6),

(X, Y) = (1, 4), Z = 7: (1, 4) переходит в (7, 6, 7),

(X, Y) = (1, 4), Z = 8: (1, 4) переходит в (8, 10, 8),

(X, Y) = (1, 4), Z = 9: (1, 4) переходит в (9, 3, 9),

(X, Y) = (1, 4), Z = 10: (1, 4) переходит в (10, 7, 10),

(X, Y) = (1, 6), Z = 1: (1, 6) переходит в (1, 6, 1),

(X, Y) = (1, 6), Z = 2: (1, 6) переходит в (2, 1, 2),

(X, Y) = (1, 6), Z = 3: (1, 6) переходит в (3, 7, 3),

(X, Y) = (1, 6), Z = 4: (1, 6) переходит в (4, 2, 4),

(X, Y) = (1, 6), Z = 5: (1, 6) переходит в (5, 8, 5),

(X, Y) = (1, 6), Z = 6: (1, 6) переходит в (6, 3, 6),

(X, Y) = (1, 6), Z = 7: (1, 6) переходит в (7, 9, 7),

(X, Y) = (1, 6), Z = 8: (1, 6) переходит в (8, 4, 8),

(X, Y) = (1, 6), Z = 9: (1, 6) переходит в (9, 10, 9),

(X, Y) = (1, 6), Z = 10: (1, 6) переходит в (10, 5, 10),

(X, Y) = (3, 4), Z = 1: (3, 4) переходит в (3, 4, 1),

(X, Y) = (3, 4), Z = 2: (3, 4) переходит в (6, 8, 2),

(X, Y) = (3, 4), Z = 3: (3, 4) переходит в (9, 1, 3),

(X, Y) = (3, 4), Z = 4: (3, 4) переходит в (1, 5, 4),

(X, Y) = (3, 4), Z = 5: (3, 4) переходит в (4, 9, 5),

(X, Y) = (3, 4), Z = 6: (3, 4) переходит в (7, 2, 6),

(X, Y) = (3, 4), Z = 7: (3, 4) переходит в (10, 6, 7),

(X, Y) = (3, 4), Z = 8: (3, 4) переходит в (2, 10, 8),
(X, Y) = (3, 4), Z = 9: (3, 4) переходит в (5, 3, 9),
(X, Y) = (3, 4), Z = 10: (3, 4) переходит в (8, 7, 10),
(X, Y) = (3, 8), Z = 1: (3, 8) переходит в (3, 8, 1),
(X, Y) = (3, 8), Z = 2: (3, 8) переходит в (6, 5, 2),
(X, Y) = (3, 8), Z = 3: (3, 8) переходит в (9, 2, 3),
(X, Y) = (3, 8), Z = 4: (3, 8) переходит в (1, 10, 4),
(X, Y) = (3, 8), Z = 5: (3, 8) переходит в (4, 7, 5),
(X, Y) = (3, 8), Z = 6: (3, 8) переходит в (7, 4, 6),
(X, Y) = (3, 8), Z = 7: (3, 8) переходит в (10, 1, 7),
(X, Y) = (3, 8), Z = 8: (3, 8) переходит в (2, 9, 8),
(X, Y) = (3, 8), Z = 9: (3, 8) переходит в (5, 6, 9),
(X, Y) = (3, 8), Z = 10: (3, 8) переходит в (8, 3, 10),
(X, Y) = (4, 0), Z = 1: (4, 0) переходит в (4, 0, 1),
(X, Y) = (4, 0), Z = 2: (4, 0) переходит в (8, 0, 2),
(X, Y) = (4, 0), Z = 3: (4, 0) переходит в (1, 0, 3),
(X, Y) = (4, 0), Z = 4: (4, 0) переходит в (5, 0, 4),
(X, Y) = (4, 0), Z = 5: (4, 0) переходит в (9, 0, 5),
(X, Y) = (4, 0), Z = 6: (4, 0) переходит в (2, 0, 6),
(X, Y) = (4, 0), Z = 7: (4, 0) переходит в (6, 0, 7),
(X, Y) = (4, 0), Z = 8: (4, 0) переходит в (10, 0, 8),
(X, Y) = (4, 0), Z = 9: (4, 0) переходит в (3, 0, 9),
(X, Y) = (4, 0), Z = 10: (4, 0) переходит в (7, 0, 10),
(X, Y) = (4, 2), Z = 1: (4, 2) переходит в (4, 2, 1),
(X, Y) = (4, 2), Z = 2: (4, 2) переходит в (8, 4, 2),
(X, Y) = (4, 2), Z = 3: (4, 2) переходит в (1, 6, 3),
(X, Y) = (4, 2), Z = 4: (4, 2) переходит в (5, 8, 4),
(X, Y) = (4, 2), Z = 5: (4, 2) переходит в (9, 10, 5),
(X, Y) = (4, 2), Z = 6: (4, 2) переходит в (2, 1, 6),
(X, Y) = (4, 2), Z = 7: (4, 2) переходит в (6, 3, 7),
(X, Y) = (4, 2), Z = 8: (4, 2) переходит в (10, 5, 8),
(X, Y) = (4, 2), Z = 9: (4, 2) переходит в (3, 7, 9),
(X, Y) = (4, 2), Z = 10: (4, 2) переходит в (7, 9, 10),
(X, Y) = (5, 1), Z = 1: (5, 1) переходит в (5, 1, 1),
(X, Y) = (5, 1), Z = 2: (5, 1) переходит в (10, 2, 2),
(X, Y) = (5, 1), Z = 3: (5, 1) переходит в (4, 3, 3),
(X, Y) = (5, 1), Z = 4: (5, 1) переходит в (9, 4, 4),

(X, Y) = (5, 1), Z = 5: (5, 1) переходит в (3, 5, 5),

(X, Y) = (5, 1), Z = 6: (5, 1) переходит в (8, 6, 6),

(X, Y) = (5, 1), Z = 7: (5, 1) переходит в (2, 7, 7),

(X, Y) = (5, 1), Z = 8: (5, 1) переходит в (7, 8, 8),

(X, Y) = (5, 1), Z = 9: (5, 1) переходит в (1, 9, 9),

(X, Y) = (5, 1), Z = 10: (5, 1) переходит в (6, 10, 10),

(X, Y) = (5, 2), Z = 1: (5, 2) переходит в (5, 2, 1),

(X, Y) = (5, 2), Z = 2: (5, 2) переходит в (10, 4, 2),

(X, Y) = (5, 2), Z = 3: (5, 2) переходит в (4, 6, 3),

(X, Y) = (5, 2), Z = 4: (5, 2) переходит в (9, 8, 4),

(X, Y) = (5, 2), Z = 5: (5, 2) переходит в (3, 10, 5),

(X, Y) = (5, 2), Z = 6: (5, 2) переходит в (8, 1, 6),

(X, Y) = (5, 2), Z = 7: (5, 2) переходит в (2, 3, 7),

(X, Y) = (5, 2), Z = 8: (5, 2) переходит в (7, 5, 8),

(X, Y) = (5, 2), Z = 9: (5, 2) переходит в (1, 7, 9),

(X, Y) = (5, 2), Z = 10: (5, 2) переходит в (6, 9, 10),

(X, Y) = (6, 6), Z = 1: (6, 6) переходит в (6, 6, 1),

(X, Y) = (6, 6), Z = 2: (6, 6) переходит в (1, 1, 2),

(X, Y) = (6, 6), Z = 3: (6, 6) переходит в (7, 7, 3),

(X, Y) = (6, 6), Z = 4: (6, 6) переходит в (2, 2, 4),

(X, Y) = (6, 6), Z = 5: (6, 6) переходит в (8, 8, 5),

(X, Y) = (6, 6), Z = 6: (6, 6) переходит в (3, 3, 6),

(X, Y) = (6, 6), Z = 7: (6, 6) переходит в (9, 9, 7),

(X, Y) = (6, 6), Z = 8: (6, 6) переходит в (4, 4, 8),

(X, Y) = (6, 6), Z = 9: (6, 6) переходит в (10, 10, 9),

(X, Y) = (6, 6), Z = 10: (6, 6) переходит в (5, 5, 10),

(X, Y) = (6, 9), Z = 1: (6, 9) переходит в (6, 9, 1),

(X, Y) = (6, 9), Z = 2: (6, 9) переходит в (1, 7, 2),

(X, Y) = (6, 9), Z = 3: (6, 9) переходит в (7, 5, 3),

(X, Y) = (6, 9), Z = 4: (6, 9) переходит в (2, 3, 4),

(X, Y) = (6, 9), Z = 5: (6, 9) переходит в (8, 1, 5),

(X, Y) = (6, 9), Z = 6: (6, 9) переходит в (3, 10, 6),

(X, Y) = (6, 9), Z = 7: (6, 9) переходит в (9, 8, 7),

(X, Y) = (6, 9), Z = 8: (6, 9) переходит в (4, 6, 8),

(X, Y) = (6, 9), Z = 9: (6, 9) переходит в (10, 4, 9),

(X, Y) = (6, 9), Z = 10: (6, 9) переходит в (5, 2, 10),

(X, Y) = (8, 3), Z = 1: (8, 3) переходит в (8, 3, 1),

(X, Y) = (8, 3), Z = 2: (8, 3) переходит в (5, 6, 2),

(X, Y) = (8, 3), Z = 3: (8, 3) переходит в (2, 9, 3),

(X, Y) = (8, 3), Z = 4: (8, 3) переходит в (10, 1, 4),

(X, Y) = (8, 3), Z = 5: (8, 3) переходит в (7, 4, 5),

(X, Y) = (8, 3), Z = 6: (8, 3) переходит в (4, 7, 6),

(X, Y) = (8, 3), Z = 7: (8, 3) переходит в (1, 10, 7),

(X, Y) = (8, 3), Z = 8: (8, 3) переходит в (9, 2, 8),

(X, Y) = (8, 3), Z = 9: (8, 3) переходит в (6, 5, 9),

(X, Y) = (8, 3), Z = 10: (8, 3) переходит в (3, 8, 10),

(X, Y) = (9, 2), Z = 1: (9, 2) переходит в (9, 2, 1),

(X, Y) = (9, 2), Z = 2: (9, 2) переходит в (7, 4, 2),

(X, Y) = (9, 2), Z = 3: (9, 2) переходит в (5, 6, 3),

(X, Y) = (9, 2), Z = 4: (9, 2) переходит в (3, 8, 4),

(X, Y) = (9, 2), Z = 5: (9, 2) переходит в (1, 10, 5),

(X, Y) = (9, 2), Z = 6: (9, 2) переходит в (10, 1, 6),

(X, Y) = (9, 2), Z = 7: (9, 2) переходит в (8, 3, 7),

(X, Y) = (9, 2), Z = 8: (9, 2) переходит в (6, 5, 8),

(X, Y) = (9, 2), Z = 9: (9, 2) переходит в (4, 7, 9),

(X, Y) = (9, 2), Z = 10: (9, 2) переходит в (2, 9, 10),

(X, Y) = (9, 5), Z = 1: (9, 5) переходит в (9, 5, 1),

(X, Y) = (9, 5), Z = 2: (9, 5) переходит в (7, 10, 2),

(X, Y) = (9, 5), Z = 3: (9, 5) переходит в (5, 4, 3),

(X, Y) = (9, 5), Z = 4: (9, 5) переходит в (3, 9, 4),

(X, Y) = (9, 5), Z = 5: (9, 5) переходит в (1, 3, 5),

(X, Y) = (9, 5), Z = 6: (9, 5) переходит в (10, 8, 6),

(X, Y) = (9, 5), Z = 7: (9, 5) переходит в (8, 2, 7),

(X, Y) = (9, 5), Z = 8: (9, 5) переходит в (6, 7, 8),

(X, Y) = (9, 5), Z = 9: (9, 5) переходит в (4, 1, 9),

(X, Y) = (9, 5), Z = 10: (9, 5) переходит в (2, 6, 10),

(X, Y) = (10, 3), Z = 1: (10, 3) переходит в (10, 3, 1),

(X, Y) = (10, 3), Z = 2: (10, 3) переходит в (9, 6, 2),

(X, Y) = (10, 3), Z = 3: (10, 3) переходит в (8, 9, 3),

(X, Y) = (10, 3), Z = 4: (10, 3) переходит в (7, 1, 4),

(X, Y) = (10, 3), Z = 5: (10, 3) переходит в (6, 4, 5),

(X, Y) = (10, 3), Z = 6: (10, 3) переходит в (5, 7, 6),

(X, Y) = (10, 3), Z = 7: (10, 3) переходит в (4, 10, 7),

(X, Y) = (10, 3), Z = 8: (10, 3) переходит в (3, 2, 8),

$(X, Y) = (10, 3)$, $Z = 9$: $(10, 3)$ переходит в $(2, 5, 9)$,

$(X, Y) = (10, 3)$, $Z = 10$: $(10, 3)$ переходит в $(1, 8, 10)$,

$(X, Y) = (10, 5)$, $Z = 1$: $(10, 5)$ переходит в $(10, 5, 1)$,

$(X, Y) = (10, 5)$, $Z = 2$: $(10, 5)$ переходит в $(9, 10, 2)$,

$(X, Y) = (10, 5)$, $Z = 3$: $(10, 5)$ переходит в $(8, 4, 3)$,

$(X, Y) = (10, 5)$, $Z = 4$: $(10, 5)$ переходит в $(7, 9, 4)$,

$(X, Y) = (10, 5)$, $Z = 5$: $(10, 5)$ переходит в $(6, 3, 5)$,

$(X, Y) = (10, 5)$, $Z = 6$: $(10, 5)$ переходит в $(5, 8, 6)$,

$(X, Y) = (10, 5)$, $Z = 7$: $(10, 5)$ переходит в $(4, 2, 7)$,

$(X, Y) = (10, 5)$, $Z = 8$: $(10, 5)$ переходит в $(3, 7, 8)$,

$(X, Y) = (10, 5)$, $Z = 9$: $(10, 5)$ переходит в $(2, 1, 9)$,

$(X, Y) = (10, 5)$, $Z = 10$: $(10, 5)$ переходит в $(1, 6, 10)$.

Иногда в дальнейшем нам будет удобнее пользоваться слегка модифицированной формой проективной плоскости, когда проективные координаты (X, Y, Z) представляют аффинную точку $(X / Z^2, Y / Z^3)$.

Рассмотрим представление проективными точками вида (X, Y, Z) модифицированной формы проективной плоскости (в первом примере) над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10), отличными от бесконечно удаленной точки ($Z \neq 0$), аффинных точек вида $(X / Z^2, Y / Z^3)$:

$(X, Y, Z) = (0, 1, 1)$ представляет $(X / Z^2, Y / Z^3) = (0/1^2, 1/1^3) = (0 / 1, 1 / 1) = (0, 1)$,

$(X, Y, Z) = (0, 1, 2)$ представляет $(X / Z^2, Y / Z^3) = (0/2^2, 1/2^3) = (0, 1 / 8 \pmod 3) =$
$= (0, 1 / 2) = (0, 1 \cdot 2^{-1} \pmod 3) = (0, 1 \cdot 2) = (0, 2)$,

$(X, Y, Z) = (0, 2, 1)$ представляет $(X / Z^2, Y / Z^3) = (0/1^2, 2/1^3) = (0 / 1, 2 / 1) = (0, 2)$,

$(X, Y, Z) = (0, 2, 2)$ представляет $(X / Z^2, Y / Z^3) = (0/2^2, 2/2^3) = (0, 2 / 8 \pmod 3) =$
$= (0, 2 / 2) = (0, 2 \cdot 2^{-1} \pmod 3) = (0, 2 \cdot 2 \pmod 3) = (0, 4 \pmod 3) = (0, 1)$,

$(X, Y, Z) = (1, 1, 1)$ представляет $(X / Z^2, Y / Z^3) = (1/1^2, 1/1^3) = (1 / 1, 1 / 1) = (1, 1)$,

$(X, Y, Z) = (1, 1, 2)$ представляет $(X / Z^2, Y / Z^3) = (1/2^2, 1/2^3) =$
$= (1 / 4 \pmod 3, 1 / 8 \pmod 3) = (1 / 1, 1 / 2) =$
$= (1, 1 \cdot 2^{-1} \pmod 3) = (1, 1 \cdot 2) = (1, 2)$,

$(X, Y, Z) = (1, 2, 1)$ представляет $(X / Z^2, Y / Z^3) = (1/1^2, 2/1^3) = (1 / 1, 2 / 1) = (1, 2)$,

$(X, Y, Z) = (1, 2, 2)$ представляет $(X / Z^2, Y / Z^3) = (1/2^2, 2/2^3) =$
$= (1 / 4 \pmod 3, 2 / 8 \pmod 3) = (1 / 1, 2 / 2) = (1, 1)$,

$(X, Y, Z) = (2, 1, 1)$ представляет $(X / Z^2, Y / Z^3) = (2/1^2, 1/1^3) = (2 / 1, 1 / 1) = (2, 1)$,

$(X, Y, Z) = (2, 1, 2)$ представляет $(X/Z^2, Y/Z^3) = (2/2^2, 1/2^3) =$

$= (2 / 4 \pmod 3), 1 / 8 \pmod 3)) = (2 / 1, 1 / 2) = (2, 1 \cdot 2^{-1} \pmod 3))$

$= (2, 1 \cdot 2) = (2, 2),$

$(X, Y, Z) = (2, 2, 1)$ представляет $(X/Z^2, Y/Z^3) = (2/1^2, 2/1^3) = (2 / 1, 2 / 1) = (2, 2),$

$(X, Y, Z) = (2, 2, 2)$ представляет $(X/Z^2, Y/Z^3) = (2/2^2, 2/2^3) =$

$= (2 / 4 \pmod 3), 2 / 8 \pmod 3)) = (2 / 1, 2 / 2) = (2, 1).$

Обобщая рассмотренные (в первом примере) представления проективными точками вида (X, Y, Z) модифицированной формы проективной плоскости над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10), отличными от бесконечно удаленной точки ($Z \neq 0$), аффинных точек вида $(X / Z^2, Y / Z^3)$ имеем:

(0, 1, 1) и (0, 2, 2) представляют (0, 1),
(0, 1, 2) и (0, 2, 1) представляют (0, 2),
(1, 1, 1) и (1, 2, 2) представляют (1, 1),
(1, 1, 2) и (1, 2, 1) представляют (1, 2),
(2, 1, 1) и (2, 2, 2) представляют (2, 1),
(2, 1, 2) и (2, 2, 1) представляют (2, 2).

Во втором примере приведем представление проективными точками вида (X, Y, Z) модифицированной формы проективной плоскости над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.11), отличными от бесконечно удаленной точки ($Z \neq 0$), аффинных точек вида $(X / Z^2, Y / Z^3)$:

(1, 0, 4) представляет (1, 0),
(1, 2, 1) представляет (1, 2),
(1, 3, 2) представляет (4, 1),
(1, 4, 1) представляет (1, 4),
(1, 4, 2) представляет (4, 3),
(1, 4, 4) и (4, 2, 3) представляют (1, 1),
(2, 0, 3) представляет (3, 0),
(2, 1, 4) представляет (2, 4),
(2, 3, 2) представляет (3, 1),
(2, 3, 3) представляет (3, 4),
(2, 3, 4) представляет (2, 2),
(2, 4, 2) представляет (3, 3),
(3, 0, 2) представляет (2, 0),
(3, 1, 3) представляет (2, 3),

(3, 2, 1) представляет (3, 2),

(3, 2, 2) представляет (2, 4),

(3, 2, 3) представляет (2, 1),

(3, 4, 1) представляет (3, 4),

(4, 0, 1) представляет (4, 0),

(4, 1, 1) представляет (4, 1),

(4, 1, 3) представляет (1, 3),

(4, 1, 4) представляет (4, 4),

(4, 3, 4) представляет (4, 2).

В третьем примере приведем представление проективными точками вида (X, Y, Z) модифицированной формы проективной плоскости над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.12), отличными от бесконечно удаленной точки ($Z \neq 0$), аффинных точек вида $(X / Z^2, Y / Z^3)$:

(1, 0, 3) представляет (4, 0),

(1, 1, 6) представляет (1, 6),

(1, 2, 2) представляет (2, 2),

(1, 5, 2) представляет (2, 5),

(1, 6, 6) представляет (1, 1),

(2, 0, 6) представляет (2, 0),

(2, 2, 5) представляет (4, 5),

(2, 3, 4) представляет (1, 3),

(2, 4, 4) представляет (1, 4),

(2, 5, 5) представляет (4, 2),

(3, 0, 2) представляет (6, 0),

(3, 1, 6) представляет (3, 6),

(3, 3, 4) представляет (5, 3),

(3, 4, 4) представляет (5, 4),

(3, 6, 6) представляет (3, 1),

(4, 0, 5) представляет (1, 0),

(4, 1, 1) представляет (4, 1),

(4, 3, 3) представляет (2, 4),

(4, 4, 3) представляет (2, 3),

(4, 6, 1) представляет (4, 6),

(5, 0, 1) представляет (5, 0),

(5, 2, 2) представляет (3, 2),

(5, 3, 3) представляет (6, 4),

(5, 4, 3) представляет (6, 3),

(5, 5, 2) представляет (3, 5),

(6, 0, 4) представляет (3, 0),

(6, 1, 1) представляет (6, 1),

(6, 2, 5) представляет (5, 5),

(6, 5, 5) представляет (5, 2),

(6, 6, 1) представляет (6, 6).

В четвертом примере приведем представление проективными точками вида (*X*, *Y*, *Z*) модифицированной формы проективной плоскости над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.13), отличными от бесконечно удаленной точки ($Z \neq 0$), аффинных точек вида $(X / Z^2, Y / Z^3)$:

(0, 1, 2) и (0, 10, 9) представляют (0, 7),

(0, 1, 4) и (0, 10, 7) представляют (0, 5),

(0, 2, 4) и (0, 9, 7) представляют (0, 10),

(0, 2, 8) и (0, 9, 3) представляют (0, 4),

(0, 3, 1) и (0, 8, 10) представляют (0, 3),

(0, 3, 6) и (0, 8, 5) представляют (0, 2),

(0, 4, 5) и (0, 7, 6) представляют (0, 1),

(0, 4, 8) и (0, 7, 3) представляют (0, 8),

(0, 5, 9) и (0, 6, 2) представляют (0, 9),

(0, 5, 10) и (0, 6, 1) представляют (0, 6),

(1, 0, 3) представляет (5, 0),

(1, 1, 2) представляет (3, 7),

(1, 3, 5), (3, 1, 3), (5, 6, 2) и (9, 4, 4) представляют (4, 9),

(1, 4, 1), (3, 5, 5), (4, 1, 9) и (9, 2, 8) представляют (1, 4),

(1, 5, 4) представляет (9, 3),

(1, 6, 1) и (4, 7, 9) представляют (1, 6),

(1, 6, 3) и (4, 7, 5) представляют (5, 10),

(1, 6, 10) представляет (1, 5),

(1, 7, 2) и (4, 10, 7) представляют (3, 5),

(1, 7, 9) представляет (3, 6),

(1, 8, 10) и (3, 10, 6) представляют (1, 3),

(1, 9, 9), (3, 8, 10), (4, 5, 4) и (5, 4, 3) представляют (3, 3),

(1, 10, 4) и (3, 7, 9) представляют (9, 6),

(1, 10, 5) и (3, 7, 3) представляют (4, 8),

(1, 10, 7), (4, 3, 3), (5, 9, 5) и (9, 5, 1) представляют (9, 5),

(2, 0, 6) представляет (8, 0),
(2, 1, 2) и (8, 3, 7) представляют (6, 7),
(2, 1, 6) и (8, 3, 10) представляют (8, 8),
(2, 1, 9) представляет (6, 4),
(2, 2, 4) представляет (7, 10),
(2, 3, 4) и (8, 9, 3) представляют (7, 4),
(2, 3, 7) представляет (7, 7),
(2, 5, 9) и (6, 9, 1) представляют (6, 9),
(2, 6, 10), (6, 2, 6), (7, 8, 8) и (10, 1, 4) представляют (2, 5),
(2, 7, 7), (6, 5, 9), (8, 10, 8) и (10, 8, 6) представляют (7, 9),
(2, 8, 2), (6, 10, 10), (7, 4, 5) и (8, 2, 7) представляют (6, 1),
(2, 9, 3), (7, 10, 2), (8, 6, 6) и (10, 7, 10) представляют (10, 4),
(2, 9, 8) и (6, 3, 7) представляют (10, 7),
(2, 9, 10) и (6, 3, 6) представляют (2, 2),
(2, 10, 8) представляет (10, 9),
(3, 0, 9) представляет (9, 0),
(3, 2, 8) и (9, 8, 7) представляют (4, 4),
(3, 3, 6) представляет (1, 2),
(3, 4, 1) представляет (3, 4),
(3, 7, 8) представляет (4, 3),
(3, 8, 1) и (9, 10, 5) представляют (3, 8),
(3, 8, 4) и (9, 10, 9) представляют (5, 7),
(3, 9, 4), (4, 7, 6), (5, 1, 1) и (9, 3, 9) представляют (5, 1),
(3, 10, 5) представляет (1, 8),
(4, 0, 1) представляет (4, 0),
(4, 2, 1) и (5, 6, 9) представляют (4, 2),
(4, 2, 4) и (5, 6, 3) представляют (3, 10),
(4, 2, 7) представляет (3, 1),
(4, 4, 8) представляет (9, 8),
(4, 6, 3) представляет (9, 10),
(4, 6, 8) и (5, 7, 6) представляют (9, 1),
(4, 9, 5) представляет (5, 5),
(5, 0, 4) представляет (1, 0),
(5, 2, 1) представляет (5, 2),
(5, 2, 10) и (9, 6, 2) представляют (5, 9),
(5, 3, 9) представляет (4, 1),
(5, 5, 10) представляет (5, 6),
(5, 8, 4) и (9, 2, 3) представляют (1, 7),

(5, 8, 5) и (9, 2, 1) представляют (9, 2),

(5, 8, 6) представляет (9, 9),

(6, 0, 7) представляет (10, 0),

(6, 3, 5) представляет (2, 9),

(6, 4, 5) и (7, 5, 3) представляют (2, 1),

(6, 5, 2) и (7, 9, 10) представляют (7, 2),

(6, 5, 8) и (7, 9, 7) представляют (8, 10),

(6, 6, 1) представляет (6, 6),

(6, 7, 8), (7, 6, 7), (8, 3, 1) и (10, 2, 2) представляют (8, 3),

(6, 8, 2) представляет (7, 1),

(6, 9, 10) представляет (6, 2),

(7, 0, 10) представляет (7, 0),

(7, 1, 4) и (10, 4, 9) представляют (8, 5),

(7, 2, 6) представляет (6, 5),

(7, 4, 2) и (10, 5, 10) представляют (10, 6),

(7, 4, 6) и (10, 5, 8) представляют (6, 10),

(7, 5, 8) представляет (2, 10),

(7, 7, 3) представляет (2, 8),

(7, 9, 4) представляет (8, 1),

(8, 0, 2) представляет (2, 0),

(8, 1, 5) и (10, 3, 1) представляют (10, 3),

(8, 1, 6) представляет (10, 8),

(8, 4, 2) и (10, 1, 7) представляют (2, 6),

(8, 4, 3) представляет (7, 3),

(8, 4, 8) и (10, 1, 6) представляют (7, 8),

(8, 7, 10) представляет (8, 4),

(8, 8, 5) представляет (10, 2),

(9, 0, 5) представляет (3, 0),

(9, 1, 3) представляет (1, 9),

(9, 8, 4) представляет (4, 7),

(9, 9, 7) представляет (4, 10),

(9, 10, 2) представляет (5, 4),

(10, 0, 8) представляет (6, 0),

(10, 4, 2) представляет (8, 6),

(10, 5, 1) представляет (10, 5),

(10, 6, 7) представляет (2, 3),

(10, 10, 9) представляет (8, 7).

Для эллиптических кривых, заданных длинной (2.2) или аффинной (2.14) версиями уравнения Вейерштрасса, введем следующие константы, которые будут использованы в дальнейших формулах для вычисления дискриминантов этих кривых:

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = a_1a_3 + 2a_4,$$

$$b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Дискриминант эллиптической кривой E определяется по формуле

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \qquad (2.19)$$

Заметим, что если характеристика поля $\operatorname{char} K \notin \{2, 3\}$, то дискриминант можно вычислить не только по формуле (2.19), но и по формуле

$$\Delta = \frac{c_4^3 - c_6^2}{1728}. \qquad (2.20)$$

Заметим, что $1728 = 64 \cdot 27 = 2^6 \cdot 3^3$, так что использование формулы (2.20) для вычисления дискриминанта эллиптической кривой имеет смысл только в тех полях, чья характеристика отлична от двух и отлична от трех. В противном случае знаменатель 1728 формулы (2.20) обращается в нуль.

Вычислим дискриминант (первого примера) эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10) по формуле (2.19):

$$b_2 = a_1^2 + 4a_2 \pmod p = 0^2 + 4 \cdot 0 \pmod 3 = 0 + 0 \pmod 3 = 0,$$

$$b_4 = a_1a_3 + 2a_4 \pmod p = 0 \cdot 0 + 2 \cdot 2 \pmod 3 = 0 + 4 \pmod 3 = 1,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 0^2 + 4 \cdot 1 \pmod 3 = 0 + 4 \pmod 3 = 1,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \pmod p =$$

$$= 0^2 \cdot 1 + 4 \cdot 0 \cdot 1 - 0 \cdot 0 \cdot 2 + 0 \cdot 0^2 - 2^2 \pmod 3 =$$

$$= 0 + 0 - 0 + 0 - 4 \pmod 3 = -4 \pmod 3 = 2,$$

$$c_4 = b_2^2 - 24b_4 \pmod p =$$

$$= 0^2 - 24 \cdot 1 \pmod 3 = 0 - 24 \pmod 3 = -24 \pmod 3 = 0,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \pmod p =$$

$$= -0^3 + 36 \cdot 0 \cdot 1 - 216 \cdot 1 \pmod 3 = 0 + 0 - 216 \pmod 3 = -216 \pmod 3 = 0.$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \pmod p =$$

$$= -0^2 \cdot 2 - 8 \cdot 1^3 - 27 \cdot 1^2 + 9 \cdot 0 \cdot 1 \cdot 1 \pmod 3 =$$

$$= 0 - 8 - 27 + 0 \pmod 3 = = -35 \pmod 3 = 1.$$

Поскольку знаменатель 1728 формулы (2.20) по модулю $p = 3$ обращается в нуль, вычислять дискриминант эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10) по формуле (2.20) не имеет смысла.

Представим дискриминант (второго примера) эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.11), вычисленный по формулам (2.19) и (2.20):

$$b_2 = a_1^2 + 4a_2 \pmod p = 12 \pmod 5 = 2,$$

$$b_4 = a_1 a_3 + 2a_4 \pmod p = 0 \pmod 5 = 0,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 28 \pmod 5 = 3,$$

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \pmod p = 84 \pmod 5 = 4,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = 4 \pmod 5 = 4,$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6 \pmod p = -656 \pmod 5 = 4,$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \pmod p = -259 \pmod 5 = 1,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \pmod p = \frac{4^3 - 4^2}{1728} \pmod 5 =$$

$$= \frac{64 - 16 \pmod 5}{1728 \pmod 5} = \frac{48 \pmod 5}{3 \pmod 5} = \frac{3 \pmod 5}{3 \pmod 5} =$$

$$= 3 \cdot 3^{-1} \pmod 5 = 3 \cdot 2 \pmod 5 = 6 \pmod 5 = 1.$$

В третьем примере дискриминант эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.12), вычисленный по формулам (2.19) и (2.20):

$$b_2 = a_1^2 + 4a_2 \pmod p = 0 \pmod 7 = 0,$$

$$b_4 = a_1 a_3 + 2a_4 \pmod p = 2 \pmod 7 = 2,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 12 \pmod 7 = 5,$$

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \pmod p = -1 \pmod 7 = 6,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = -48 \pmod 7 = 1,$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6 \pmod p = -1080 \pmod 7 = 5,$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \pmod p = -739 \pmod 7 = 3,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \pmod p = \frac{1^3 - 5^2}{1728} \pmod 7 = \frac{1 - 25 \pmod 7}{1728 \pmod 7} = \frac{-24 \pmod 7}{6 \pmod 7} = \frac{4 \pmod 7}{6 \pmod 7} =$$

$$= 4 \cdot 6^{-1} \pmod 7 = 4 \cdot 6 \pmod 7 = 24 \pmod 7 = 3.$$

В четвертом примере дискриминант эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.13), вычисленный по формулам (2.19) и (2.20):

$$b_2 = a_1^2 + 4a_2 \pmod p = 116 \pmod{11} = 6,$$

$$b_4 = a_1 a_3 + 2a_4 \pmod p = 20 \pmod{11} = 9,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 20 \pmod{11} = 9,$$

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \pmod p = 480 \pmod{11} = 7,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = -180 \pmod{11} = 7,$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6 \pmod p = -216 \pmod{11} = 4,$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9 b_2 b_4 b_6 \pmod p = -3897 \pmod{11} = 8,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \pmod p = \frac{7^3 - 4^2}{1728} \pmod{11} = \frac{343 - 16 \pmod{11}}{1728 \pmod{11}} = \frac{327 \pmod{11}}{1 \pmod{11}} =$$

$$= \frac{8 \pmod{11}}{1 \pmod{11}} = 8 \cdot 1^{-1} \pmod{11} = 8 \cdot 1 \pmod{11} = 8 \pmod{11} = 8.$$

Известно, что эллиптическая кривая E является неособой тогда и только тогда, когда ее дискриминант $\Delta \neq 0$.

Заметим, что вычисленные дискриминанты Δ первого, второго, третьего и четвертого примеров эллиптических кривых над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10), над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.11), над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.12) и над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.13), равны одному, трем и восьми соответственно. Поэтому каждая из этих (эллиптических) кривых является неособой.

С этого момента будем предполагать, что дискриминант (эллиптических) кривых $\Delta \neq 0$, т.е. рассматривать только неособые кривые.

Для неособых кривых E введем некоторое свойство, остающееся неизменным, так называемый *j-инвариант* или *инвариант j*:

$$j(E) = \frac{c_4^3}{\Delta}. \qquad (2.21)$$

Вычислим j-инвариант (первого примера) эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.10) по формуле (2.21):

$$j(E) = \frac{c_4^3}{\Delta} = \frac{0^3}{1} = \frac{0}{1} = 0.$$

Представим вычисление j-инварианта (второго примера) эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.11) по формуле (2.21):

$$j(E) = \frac{c_4^3}{\Delta} = \frac{4^3 (\mathrm{mod}\, 5)}{1} = \frac{64\,(\mathrm{mod}\, 5)}{1} = \frac{4}{1} = 4.$$

В третьем примере j-инвариант эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.12), вычисленный по формуле (2.21):

$$j(E) = \frac{c_4^3}{\Delta} = \frac{1^3 (\mathrm{mod}\, 7)}{3\,(\mathrm{mod}\, 7)} = \frac{1\,(\mathrm{mod}\, 7)}{3\,(\mathrm{mod}\, 7)} =$$

$$= 1 \cdot 3^{-1} \ (\mathrm{mod}\ 7) = 1 \cdot 5 \ (\mathrm{mod}\ 7) = 5.$$

В четвертом примере j-инвариант эллиптической кривой над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.13), вычисленный по формуле (2.21):

$$j(E) = \frac{c_4^3}{\Delta} = \frac{7^3 (\mathrm{mod} 11)}{8\,(\mathrm{mod} 11)} = \frac{343\,(\mathrm{mod} 11)}{8\,(\mathrm{mod} 11)} = 2 \cdot 8^{-1}\ (\mathrm{mod}\ 11) =$$

$$= 2 \cdot 7 \ (\mathrm{mod}\ 11) = 14\ (\mathrm{mod}\ 11) = 3.$$

Инвариант j тесно связан с понятием *изоморфизма эллиптических кривых*. Говорят, что эллиптическая кривая E с координатами X и Y над полем K изоморфна эллиптической кривой E' с координатами X' и Y' над полем K (обе кривые заданы уравнением Вейерштрасса), если найдутся такие константы $r, s, t \in K$ и $u \in K^*$, что при замене переменных:

$$X = u^2 X' + r,$$

$$Y = u^3 Y' + s u^2 X' + t \qquad (2.22)$$

кривая E перейдет в кривую E'. Отдельно отметим, что изоморфизм двух эллиптических кривых определен относительно одного и того же поля K.

Рассмотрим (первый) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.14):

$$E: \ Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

$$E: \ Y^2 + 0 \cdot XY + 0 \cdot Y = X^3 + 0 \cdot X^2 + 2X + 1,$$

$$E: \ Y^2 = X^3 + 2X + 1. \qquad (2.23)$$

Сделаем замену переменных с набором констант (u, r, s, t), например, равным (2, 1, 2, 2), т.е. в соответствии с (2.22) положим:

$$X = u^2X' + r \pmod p = 2^2 \pmod 3 X' + 1 \pmod 3 = 4 \pmod 3 X' + 1 = X' + 1,$$

$$Y = u^3Y' + su^2X' + t \pmod p = 2^3 \pmod 3 Y' + 2 \cdot 2^2 \pmod 3 X' + 2 =$$

$$= 8 \pmod 3 Y' + 8 \pmod 3 X' + 2 = 2Y' + 2X' + 2.$$

Подставив полученные выражения для X и Y в (2.23), получим изоморфную ей эллиптическую кривую:

$$E': \ (2Y' + 2X' + 2)^2 = (X' + 1)^3 + 2(X' + 1) + 1,$$

$$E': \ (2Y' + 2X')^2 + 2(2Y' + 2X')2 + 2^2 = (X' + 1)^3 + 2(X' + 1) + 1,$$

$$E': \ (2Y')^2 + 2 \cdot 2 \cdot 2 \cdot Y'X' + (2X')^2 + 8Y' + 8X' + 4 =$$

$$= (X')^3 + 3 \cdot (X')^2 \cdot 1 + 3X' \cdot 1^2 + 1^3 + 2X' + 2 + 1,$$

$$E': \ 4(Y')^2 + 8Y'X' + 4(X')^2 + 2Y' + 2X' + 1 =$$

$$= (X')^3 + 3 \cdot (X')^2 + 3X' + 1 + 2X' + 3,$$

$$E': \ (Y')^2 + 2Y'X' + (X')^2 + 2Y' + 2X' + 1 = (X')^3 + 2X' + 1,$$

$$E': \ (Y')^2 + 2Y'X' + (X')^2 + 2Y' = (X')^3,$$

$$E': \ (Y')^2 + 2X'Y' + 2Y' = (X')^3 + (-1) \cdot (X')^2,$$

$$E': \ (Y')^2 + 2X'Y' + 2Y' = (X')^3 + 2 \cdot (X')^2 + 0 \cdot X' + 0,$$

$$E': \ (Y')^2 + 2X'Y' + 2Y' = (X')^3 + 2 \cdot (X')^2. \qquad (2.24)$$

Полученная эллиптическая кривая E' над полем $K = \mathbf{F}_p = \mathbf{F}_3$ (2.24) является изоморфной по отношению к (первому) примеру эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_3$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 2$, $a_6 = 1$ (2.23) и удовлетворяет аффинной версии уравнения Вейерштрасса (2.14) при $a_1 = 2$, $a_2 = 2$, $a_3 = 2$, $a_4 = 0$, $a_6 = 0$. Вычислим ее дискриминант Δ и j-инвариант $j(E')$ по формулам (2.19) и (2.21) соответственно:

$$b_2 = a_1^2 + 4a_2 \pmod p = 2^2 + 4 \cdot 2 \pmod 3 = 12 \pmod 3 = 0,$$

$$b_4 = a_1a_3 + 2a_4 \pmod p = 2 \cdot 2 + 2 \cdot 0 \pmod 3 = 4 \pmod 3 = 1,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 2^2 + 4 \cdot 0 \pmod 3 = 4 \pmod 3 = 1,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \pmod p =$$

$$= 2^2 \cdot 0 + 4 \cdot 2 \cdot 0 - 2 \cdot 2 \cdot 0 + 2 \cdot 2^2 - 0^2 \pmod 3 = 8 \pmod 3 = 2,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = 0^2 - 24\cdot 1 \pmod 3 =$$
$$= 0 - 24 \pmod 3 = -24 \pmod 3 = 0,$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \pmod p =$$
$$= -0^3 + 36\cdot 0\cdot 1 - 216\cdot 1 \pmod 3 = 0 + 0 - 216 \pmod 3 = -216 \pmod 3 = 0.$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \pmod p =$$
$$= -0^2\cdot 2 - 8\cdot 1^3 - 27\cdot 1^2 + 9\cdot 0\cdot 1\cdot 1 \pmod 3 =$$
$$= 0 - 8 - 27 + 0 \pmod 3 = -35 \pmod 3 = 1,$$
$$j(E') = \frac{c_4^3}{\Delta} = \frac{0^3}{1} = \frac{0}{1} = 0.$$

Заметим, что j-инвариант $j(E')$ этой кривой E' (2.24), так же как и j-инвариант $j(E)$ исходной кривой E (2.23), равен нулю.

Рассмотрим (второй) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.14):

$$E:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$
$$E:\ Y^2 + 0\cdot XY + 4\cdot Y = X^3 + 3\cdot X^2 + 0\cdot X + 3,$$
$$E:\ Y^2 + 4\cdot Y = X^3 + 3\cdot X^2 + 3. \qquad (2.25)$$

Сделаем замену переменных с набором констант $(u, r, s, t) = (2, 2, 4, 1)$, т.е. ($u = 2$, $r = 2$, $s = 4$, $t = 1$). Следовательно, в соответствии с (2.22) положим:

$$X = u^2X' + r \pmod p = 2^2 \pmod 5 X' + 2 \pmod 5 = 4 \pmod 5 X' + 2 = 4X' + 2,$$
$$Y = u^3Y' + su^2X' + t \pmod p = 2^3 \pmod 5 Y' + 4\cdot 2^2 \pmod 5 X' + 1 =$$
$$= 8 \pmod 5 Y' + 16 \pmod 5 X' + 1 = 3Y' + 1\cdot X' + 1 = 3Y' + X' + 1.$$

Подставив полученные выражения для X и Y в (2.25), получим изоморфную ей эллиптическую кривую:

$$E':\ (3Y' + X' + 1)^2 + 4\cdot(3Y' + X' + 1) = (4X' + 2)^3 + 3\cdot(4X' + 2)^2 + 3,$$
$$E':\ (3Y' + X')^2 + 2\cdot(3Y' + X')\cdot 1 + 1^2 + 12Y' + 4X' + 4 =$$
$$= ((4X')^3 + 3\cdot(4X')^2\cdot 2 + 3\cdot(4X')\cdot 2^2 + 2^3) +$$
$$+ 3\cdot((4X')^2 + 2\cdot(4X')\cdot 2 + 2^2) + 3,$$
$$E':\ (3Y')^2 + 2\cdot(3Y')\cdot X' + (X')^2 + 2\cdot(3Y') + 2X' + 1 + 12Y' + 4X' + 4 =$$
$$= (4^3\cdot(X')^3 + 3\cdot 4^2\cdot(X')^2\cdot 2 + 3\cdot(4X')\cdot 4 + 8) +$$
$$+ 3\cdot(4^2(X')^2 + 4\cdot 4\cdot X' + 4) + 3,$$

$$E'\colon\ 9\cdot(Y')^2 + 6X'Y' + (X')^2 + 6Y' + 2X' + 1 + 12Y' + 4X' + 4 =$$

$$= 64\cdot(X')^3 + 96\cdot(X')^2 + 48X' + 8 + 3\cdot(16\cdot(X')^2 + 16\cdot X' + 4) + 3,$$

$$E'\colon\ 9\cdot(Y')^2 + 6X'Y' + (X')^2 + 18Y' + 6X' + 5 =$$

$$= 64\cdot(X')^3 + 96\cdot(X')^2 + 48X' + 8 + 3\cdot(16\cdot(X')^2 + 16\cdot X' + 4) + 3,$$

$$E'\colon\ 4\cdot(Y')^2 + X'Y' + (X')^2 + 3Y' + X' + 0 =$$

$$= 4\cdot(X')^3 + (X')^2 + 3X' + 3 + 48\cdot(X')^2 + 48\cdot X' + 12 + 3,$$

$$E'\colon\ 4\cdot(Y')^2 + X'Y' + (X')^2 + 3Y' + X' = 4\cdot(X')^3 + 49\cdot(X')^2 + 51X' + 18,$$

$$E'\colon\ 4\cdot(Y')^2 + X'Y' + (X')^2 + 3Y' + X' = 4\cdot(X')^3 + 4\cdot(X')^2 + X' + 3,$$

$$E'\colon\ 4\cdot(Y')^2 + X'Y' + 3Y' = 4\cdot(X')^3 + 3\cdot(X')^2 + 3,$$

$$E'\colon\ 4\cdot 4^{-1}(Y')^2 + 4^{-1}X'Y' + 3\cdot 4^{-1}Y' = 4\cdot 4^{-1}(X')^3 + 3\cdot 4^{-1}(X')^2 + 3\cdot 4^{-1},$$

$$E'\colon\ (Y')^2 + 4X'Y' + 3\cdot 4\cdot Y' = (X')^3 + 3\cdot 4\cdot(X')^2 + 3\cdot 4,$$

$$E'\colon\ (Y')^2 + 4X'Y' + 2Y' = (X')^3 + 2\cdot(X')^2 + 2. \qquad (2.26)$$

Полученная эллиптическая кривая E' над полем $K = \mathbf{F}_p = \mathbf{F}_5$ (2.26) является изоморфной по отношению к (второму) примеру эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ (2.25) и удовлетворяет аффинной версии уравнения Вейерштрасса (2.14) при $a_1 = 4$, $a_2 = 2$, $a_3 = 2$, $a_4 = 0$, $a_6 = 2$. Вычислим ее дискриминант Δ по формулам (2.19), (2.20) и j-инвариант $j(E')$ по формуле (2.21):

$$b_2 = a_1^2 + 4a_2 \pmod p = 4^2 + 4\cdot 2 \pmod 5 = 24 \pmod 5 = 4,$$

$$b_4 = a_1a_3 + 2a_4 \pmod p = 4\cdot 2 + 2\cdot 0 \pmod 5 = 8 \pmod 5 = 3,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 2^2 + 4\cdot 2 \pmod 5 = 12 \pmod 5 = 2,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \pmod p =$$

$$= 4^2\cdot 2 + 4\cdot 2\cdot 2 - 4\cdot 2\cdot 0 + 2\cdot 2^2 - 0^2 \pmod 5 =$$

$$= 32 + 16 - 0 + 8 - 0 \pmod 5 = 56 \pmod 5 = 1,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = 4^2 - 24\cdot 3 \pmod 5 = 16 - 72 \pmod 5 = -56 \pmod 5 = 4,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \pmod p = -4^3 + 36\cdot 4\cdot 3 - 216\cdot 2 \pmod 5 =$$

$$= -64 + 432 - 432 \pmod 5 = -64 \pmod 5 = 1.$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \pmod p = -4^2\cdot 1 - 8\cdot 3^3 - 27\cdot 2^2 + 9\cdot 4\cdot 3\cdot 2 \pmod 5 =$$

$$= -16 - 216 - 108 + 216 \pmod 5 = -124 \pmod 5 = 1,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \pmod p = \frac{4^3 - 1^2}{1728} \pmod 5 =$$

$$= \frac{64 - 1 \pmod 5}{1728 \pmod 5} = \frac{63 \pmod 5}{1728 \pmod 5} = \frac{3 \pmod 5}{3 \pmod 5} =$$

$$= 3 \cdot 3^{-1} \pmod 5 = 3 \cdot 2 \pmod 5 = 6 \pmod 5 = 1.$$

$$j(E') = \frac{c_4^3}{\Delta} = \frac{4^3}{1} = \frac{64 \pmod 5}{1} = \frac{4 \pmod 5}{1} =$$

$$= 4 \cdot 1^{-1} \pmod 5 = 4 \cdot 1 \pmod 5 = 4 \pmod 5 = 4.$$

Заметим, что j-инвариант $j(E')$ этой кривой (2.26), так же как и j-инвариант $j(E)$ исходной кривой E (2.25), равен четырем.

Рассмотрим (третий) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.14):

$$E: \; Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

$$E: \; Y^2 + 0 \cdot XY + 0 \cdot Y = X^3 + 0 \cdot X^2 + 1 \cdot X + 3,$$

$$E: \; Y^2 = X^3 + X + 3. \qquad (2.27)$$

Сделаем замену переменных с набором констант $(u, r, s, t) = (2, 3, 4, 5)$, т.е. ($u = 2$, $r = 3$, $s = 4$, $t = 5$). Следовательно, в соответствии с (2.22) положим:

$$X = u^2 X' + r \pmod p = 2^2 \pmod 7 X' + 3 \pmod 7 = 4 \pmod 7 X' + 3 = 4X' + 3,$$

$$Y = u^3 Y' + s u^2 X' + t \pmod p = 2^3 \pmod 7 Y' + 4 \cdot 2^2 \pmod 7 X' + 5 =$$

$$= 8 \pmod 7 Y' + 16 \pmod 7 X' + 5 = Y' + 2X' + 5.$$

Подставив полученные выражения для X и Y в (2.27), получим изоморфную ей эллиптическую кривую:

$$E': \; (Y' + 2X' + 5)^2 = (4X' + 3)^3 + (4X' + 3) + 3,$$

$$E': \; (Y' + 2X')^2 + 2 \cdot (Y' + 2X') \cdot 5 + 5^2 =$$

$$= (4X')^3 + 3 \cdot (4X')^2 \cdot 3 + 3 \cdot (4X') \cdot 3^2 + 3^3 + 4X' + 3 + 3,$$

$$E': \; (Y')^2 + 2 \cdot Y' \cdot 2 \cdot X' + (2X')^2 + 10 \cdot (Y' + 2X') + 25 =$$

$$= 64 \cdot (X')^3 + 9 \cdot (4X')^2 + 3 \cdot 9 \cdot (4X') + 27 + 4X' + 6,$$

$$E': \; (Y')^2 + 4 \cdot X' \cdot Y' + 4(X')^2 + 10 \cdot Y' + 20 \cdot X' + 25 =$$

$$= 64 \cdot (X')^3 + 9 \cdot 16 \cdot (X')^2 + 27 \cdot 4 \cdot X' + 4X' + 33,$$

$$E'\colon\ (Y')^2 + 4X'Y' + 4(X')^2 + 10Y' + 20X' + 25 =$$

$$= 1\cdot(X')^3 + 144\cdot(X')^2 + 108X' + 4X' + 5,$$

$$E'\colon\ (Y')^2 + 4X'Y' + 10Y' = (X')^3 + 140\cdot(X')^2 + 92X' - 20,$$

$$E'\colon\ (Y')^2 + 4X'Y' + 3Y' = (X')^3 + 0\cdot(X')^2 + 1\cdot X' + 1,$$

$$E'\colon\ (Y')^2 + 4X'Y' + 3Y' = (X')^3 + X' + 1. \qquad (2.28)$$

Полученная эллиптическая кривая E' над полем $K = \mathbf{F}_p = \mathbf{F}_7$ (2.28) является изоморфной по отношению к (третьему) примеру эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ (2.27) и удовлетворяет аффинной версии уравнения Вейерштрасса (2.14) при $a_1 = 4$, $a_2 = 0$, $a_3 = 3$, $a_4 = 1$, $a_6 = 1$. Вычислим ее дискриминант Δ по формулам (2.19), (2.20) и j-инвариант $j(E')$ по формуле (2.21):

$$b_2 = a_1^2 + 4a_2 \pmod p = 4^2 + 4\cdot 0 \pmod 7 = 16 \pmod 7 = 2,$$

$$b_4 = a_1a_3 + 2a_4 \pmod p = 4\cdot 3 + 2\cdot 1 \pmod 7 = 14 \pmod 7 = 0,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 3^2 + 4\cdot 1 \pmod 7 = 13 \pmod 7 = 6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \pmod p =$$

$$= 4^2\cdot 1 + 4\cdot 0\cdot 1 - 4\cdot 3\cdot 1 + 0\cdot 3^2 - 1^2 \pmod 7 =$$

$$= 16 + 0 - 12 + 0 - 1 \pmod 7 = 3 \pmod 7 = 3,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = 2^2 - 24\cdot 0 \pmod 7 = 4 - 0 \pmod 7 = 4 \pmod 7 = 4,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \pmod p = -2^3 + 36\cdot 2\cdot 0 - 216\cdot 6 \pmod 7 =$$

$$= -8 + 0 - 1296 \pmod 7 = -1304 \pmod 7 = 5.$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \pmod p =$$

$$= -2^2\cdot 3 - 8\cdot 0^3 - 27\cdot 6^2 + 9\cdot 2\cdot 0\cdot 6 \pmod 7 =$$

$$= -12 - 0 - 972 + 0 \pmod 7 = -984 \pmod 7 = 3,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \pmod p = \frac{4^3 - 5^2}{1728} \pmod 7 = \frac{64 - 25 \pmod 7}{1728 \pmod 7} =$$

$$= \frac{39 \pmod 7}{1728 \pmod 7} = \frac{4 \pmod 7}{6 \pmod 7} =$$

$$= 4\cdot 6^{-1} \pmod 7 = 4\cdot 6 \pmod 7 = 24 \pmod 7 = 3 \pmod 7 = 3.$$

$$j(E') = \frac{c_4^3}{\Delta} = \frac{4^3}{3} = \frac{64 \pmod 7}{3} = \frac{1 \pmod 7}{3} =$$

$$= 1\cdot 3^{-1} \pmod 7 = 1\cdot 5 \pmod 7 = 5 \pmod 7 = 5.$$

Заметим, что j-инвариант $j(E')$ этой кривой (2.28), так же как и j-инвариант $j(E)$ исходной кривой E (2.27), равен пяти.

Рассмотрим (четвертый) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.14):

$$E:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

$$E:\ Y^2 + 10\cdot XY + 2\cdot Y = X^3 + 4\cdot X^2 + 0\cdot X + 4,$$

$$E:\ Y^2 + 10\cdot XY + 2\cdot Y = X^3 + 4\cdot X^2 + 4. \qquad (2.29)$$

Сделаем замену переменных с набором констант $(u, r, s, t) = (9, 5, 2, 4)$, т.е. ($u = 9$, $r = 5$, $s = 2$, $t = 4$). Следовательно, в соответствии с (2.22) положим:

$$X = u^2X' + r \pmod p = 9^2 \pmod{11} X' + 5 \pmod{11} = 81 \pmod{11} X' + 5 = 4X' + 5,$$

$$Y = u^3Y' + su^2X' + t \pmod p = 9^3 \pmod{11} Y' + 2\cdot 9^2 \pmod{11} X' + 4 =$$

$$= 729 \pmod{11} Y' + 162 \pmod{11} X' + 4 = 3Y' + 8X' + 4.$$

Подставив полученные выражения для X и Y в (2.29), получим изоморфную ей эллиптическую кривую:

$$E':\ (3Y'+8X'+4)^2 + 10\cdot(4X'+5)\cdot(3Y'+8X'+4) + 2\cdot(3Y' + 8X' + 4) =$$

$$= (4X'+5)^3 + 4\cdot(4X'+5)^2 + 4,$$

$$E':\ (3Y'+8X')^2 + 2\cdot(3Y'+8X')\cdot 4 + 4^2 +$$

$$+ 10\cdot(4X'\cdot 3Y'+4X'\cdot 8X'+4X'\cdot 4+5\cdot 3Y'+5\cdot 8X'+5\cdot 4) +$$

$$+ 6Y' + 16X' + 8 =$$

$$= (4X')^3 + 3\cdot(4X')^2\cdot 5 + 3\cdot(4X')\cdot 5^2 + 5^3 + 4\cdot((4X')^2 + 2\cdot(4X')\cdot 5 + 5^2) + 4,$$

$$E':\ (3Y')^2 + 2\cdot 3Y'\cdot 8X' + (8X')^2 +$$

$$+ 8\cdot(3Y'+8X') + 16 +$$

$$+ 10\cdot(12X'Y'+32(X')^2+16X'+15Y'+40X'+20) +$$

$$+ 6Y' + 16X' + 8 =$$

$$= 64\cdot(X')^3 + 3\cdot 5\cdot 16\cdot(X')^2 + 3\cdot 25\cdot 4\cdot X' + 125 + 4\cdot(16\cdot(X')^2 + 2\cdot 5\cdot 4\cdot X' + 25) + 4,$$

$$E':\ 9\cdot(Y')^2 + 48X'Y' + 64\cdot(X')^2 + 24Y' + 64X' + 16 + 120X'Y' +$$

$$+ 320\,(X')^2 + 160X' + 150Y' + 400X' + 200 + 6Y' + 16X' + 8 =$$

$$= 64\cdot(X')^3 + 240\cdot(X')^2 + 300X' + 125 + 64\cdot(X')^2 + 160\cdot X' + 100 + 4,$$

$$E'\colon\ 9\cdot(Y')^2 + (48+120)X'Y' + (24+150+6)Y' =$$

$$= 64\cdot(X')^3 + (240-320)\cdot(X')^2 + (300-64-400-16)X' + (229-224),$$

$$E'\colon\ 9\cdot(Y')^2 + 168\,(\mathrm{mod}11)\,X'Y' + 180\,(\mathrm{mod}11)\,Y' =$$

$$= 64\,(\mathrm{mod}11)\cdot(X')^3 + (-80)\,(\mathrm{mod}11)\cdot(X')^2 + (-180)\,(\mathrm{mod}11)X' + 5,$$

$$E'\colon\ 9\cdot(Y')^2 + 3X'Y' + 4Y' =$$

$$= 9\cdot(X')^3 + 8\cdot(X')^2 + 7X' + 5,$$

$$E'\colon\ (9\cdot 9^{-1})\cdot(Y')^2 + (3\cdot 9^{-1})X'Y' + (4\cdot 9^{-1})Y' =$$

$$= (9\cdot 9^{-1})\cdot(X')^3 + (8\cdot 9^{-1})\cdot(X')^2 + (7\cdot 9^{-1})X' + (5\cdot 9^{-1}),$$

$$E'\colon\ (Y')^2 + (3\cdot 5)X'Y' + (4\cdot 5)Y' =$$

$$= (X')^3 + (8\cdot 5)\cdot(X')^2 + (7\cdot 5)X' + (5\cdot 5),$$

$$E'\colon\ (Y')^2 + 15\,(\mathrm{mod}11)\,X'Y' + 20\,(\mathrm{mod}11)\,Y' =$$

$$= (X')^3 + 40\,(\mathrm{mod}11)\cdot(X')^2 + 35\,(\mathrm{mod}11)X' + 25\,(\mathrm{mod}11),$$

$$E'\colon\ (Y')^2 + 4X'Y' + 9Y' = (X')^3 + 7\cdot(X')^2 + 2X' + 3. \qquad (2.30)$$

Полученная эллиптическая кривая E' над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ (2.30) является изоморфной по отношению к (четвертому) примеру эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ (2.29) и удовлетворяет аффинной версии уравнения Вейерштрасса (2.14) при $a_1 = 4$, $a_2 = 7$, $a_3 = 9$, $a_4 = 2$, $a_6 = 3$. Вычислим ее дискриминант Δ по формулам (2.19), (2.20) и j-инвариант $j(E')$ по формуле (2.21):

$$b_2 = a_1^2 + 4a_2 \pmod p = 4^2 + 4\cdot 7 \pmod{11} = 44 \pmod{11} = 0,$$

$$b_4 = a_1a_3 + 2a_4 \pmod p = 4\cdot 9 \pmod{11} + 2\cdot 2 \pmod{11} = 40 \pmod{11} = 7,$$

$$b_6 = a_3^2 + 4a_6 \pmod p = 9^2 + 4\cdot 3 \pmod{11} = 93 \pmod{11} = 5,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \pmod p =$$

$$= 4^2\cdot 3 + 4\cdot 7\cdot 3 - 4\cdot 9\cdot 2 + 7\cdot 9^2 - 2^2 \pmod{11} =$$

$$= 48 + 84 - 72 + 567 - 4 \pmod{11} = 623 \pmod{11} = 7,$$

$$c_4 = b_2^2 - 24b_4 \pmod p = 0^2 - 24\cdot 7 \pmod{11} = 0 - 168 \pmod{11} = -168 \pmod{11} = 8,$$

$$c_6 = -b_2^3 + 36\,b_2b_4 - 216\,b_6 \pmod p = -0^3 + 36\cdot 0\cdot 7 - 216\cdot 5 \pmod{11} =$$

$$= 0 + 0 - 1080 \pmod{11} = -1080 \pmod{11} = 9,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \pmod p = -0^2\cdot 7 - 8\cdot 7^3 - 27\cdot 5^2 + 9\cdot 0\cdot 7\cdot 5 \pmod{11} =$$

$$= -0 - 2744 - 675 + 0 \pmod{11} = -3419 \pmod{11} = 2,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \pmod p = \frac{8^3 - 9^2}{1728} \pmod{11} = \frac{512 - 81 \pmod{11}}{1728 \pmod{11}} = \frac{431 \pmod{11}}{1} = \frac{2}{1} = 2.$$

$$j(E') = \frac{c_4^3}{\Delta} = \frac{8^3}{2} = \frac{512 \pmod{11}}{2} = \frac{6 \pmod{11}}{2} = 6 \cdot 2^{-1} \pmod{11} =$$

$$= 6 \cdot 6 \pmod{11} = 36 \pmod{11} = 3.$$

Заметим, что j-инвариант $j(E')$ этой кривой (2.30), так же как и j-инвариант $j(E)$ исходной кривой E (2.29), равен трем.

Изоморфизм эллиптических кривых является отношением эквивалентности. Следующая лемма показывает, что j-инвариант разделяет классы эквивалентности этого отношения над алгебраическим замыканием $\overline{K}$ поля K.

Лемма 2.1. Изоморфные над полем K эллиптические кривые имеют один и тот же j-инвариант. Более того, любые эллиптические кривые с совпадающими j-инвариантами изоморфны над алгебраическим замыканием $\overline{K}$ поля K.

При этом под алгебраическим замыканием поля понимается его (единственное с точностью до изоморфизма) алгебраическое расширение, являющееся алгебраически замкнутым. Например, алгебраическим замыканием поля вещественных чисел является поле комплексных чисел, алгебраическим замыканием конечного поля $\mathbf{F}_{p^k}$ (поля Галуа) является поле $\mathbf{F}_{p^\infty}$.

Заметим, что если изоморфные над полем K эллиптические кривые всегда имеют один и тот же j-инвариант, то эллиптические кривые с одним и тем же j-инвариантом не обязательно изоморфны над (основным) полем K.

Для получения неизоморфной по отношению к (третьему) примеру эллиптической кривой E над полем $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.27), сделаем замену переменных:

$$X = 3X'', \quad Y = \sqrt{6}\,Y''. \tag{2.31}$$

При этом, подставив заявленные в (2.31) выражения для X и Y в (2.27), получим эллиптическую кривую:

$$E'': \ \left(\sqrt{6}\,Y''\right)^2 = \left(3X''\right)^3 + 3X'' + 3,$$

$$E'': \ 6\left(Y''\right)^2 = 27 \pmod 7 \left(X''\right)^3 + 3X'' + 3,$$

$$E'': \ 6\left(Y''\right)^2 = 6\left(X''\right)^3 + 3X'' + 3,$$

$$E'': \ 6 \cdot 6^{-1} \pmod 7 \left(Y''\right)^2 = 6 \cdot 6^{-1} \pmod 7 \left(X''\right)^3 + 3 \cdot 6^{-1} \pmod 7 X'' + 3 \cdot 6^{-1} \pmod 7,$$

$$E'':\ (Y'')^2 = (X'')^3 + 3\cdot 6 (\mathrm{mod} 7)\ X'' + 3\cdot 6 (\mathrm{mod} 7)\ ,$$

$$E'':\ (Y'')^2 = (X'')^3 + 18 (\mathrm{mod} 7)\ X'' + 18 (\mathrm{mod} 7)\ ,$$

$$E'':\ (Y'')^2 = (X'')^3 + 4\ X'' + 4. \qquad (2.32)$$

Полученная эллиптическая кривая E'' над полем $\mathbf{P}^2(K) = \mathbf{P}^2(\mathbf{F}_p) = \mathbf{P}^2(\mathbf{F}_7)$ (2.32) удовлетворяет аффинной версии уравнения Вейерштрасса (2.14) при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 4$, $a_6 = 4$. Вычислим ее дискриминант Δ по формулам (2.19), (2.20) и j-инвариант $j(E'')$ по формуле (2.21):

$$b_2 = a_1^2 + 4a_2 \ (\mathrm{mod}\ p) = 0^2 + 4\cdot 0 \ (\mathrm{mod}\ 7) = 0 \ (\mathrm{mod}\ 7) = 0,$$

$$b_4 = a_1 a_3 + 2a_4 \ (\mathrm{mod}\ p) = 0\cdot 0 + 2\cdot 4 \ (\mathrm{mod}\ 7) = 8 \ (\mathrm{mod}\ 7) = 1,$$

$$b_6 = a_3^2 + 4a_6 \ (\mathrm{mod}\ p) = 0^2 + 4\cdot 4 \ (\mathrm{mod}\ 7) = 16 \ (\mathrm{mod}\ 7) = 2,$$

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \ (\mathrm{mod}\ p) =$$

$$= 0^2\cdot 4 + 4\cdot 0\cdot 4 - 0\cdot 0\cdot 4 + 0\cdot 0^2 - 4^2 \ (\mathrm{mod}\ 7) =$$

$$= 0 + 0 - 0 + 0 - 16 \ (\mathrm{mod}\ 7) = -16 \ (\mathrm{mod}\ 7) = 5,$$

$$c_4 = b_2^2 - 24 b_4 \ (\mathrm{mod}\ p) = 0^2 - 24\cdot 1 \ (\mathrm{mod}\ 7) =$$

$$= 0 - 24 \ (\mathrm{mod}\ 7) = -24 \ (\mathrm{mod}\ 7) = 4,$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6 \ (\mathrm{mod}\ p) = -0^3 + 36\cdot 0\cdot 1 - 216\cdot 2 \ (\mathrm{mod}\ 7) =$$

$$= -0 + 0 - 432 \ (\mathrm{mod}\ 7) = -432 \ (\mathrm{mod}\ 7) = 2,$$

$$\Delta = -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6 \ (\mathrm{mod}\ p) =$$

$$= -0^2\cdot 5 - 8\cdot 1^3 - 27\cdot 2^2 + 9\cdot 0\cdot 1\cdot 2 \ (\mathrm{mod}\ 7) =$$

$$= -0 - 8 - 108 + 0 \ (\mathrm{mod}\ 7) = -116 \ (\mathrm{mod}\ 7) = 3,$$

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \ (\mathrm{mod}\ p) = \frac{4^3 - 2^2}{1728} \ (\mathrm{mod}\ 7) =$$

$$= \frac{64 - 4\ (\mathrm{mod}\ 7)}{1728\ (\mathrm{mod}\ 7)} = \frac{60\ (\mathrm{mod}\ 7)}{1728\ (\mathrm{mod}\ 7)} = \frac{4\ (\mathrm{mod}\ 7)}{6\ (\mathrm{mod}\ 7)} =$$

$$= 4\cdot 6^{-1} \ (\mathrm{mod}\ 7) = 4\cdot 6 \ (\mathrm{mod}\ 7) = 24 \ (\mathrm{mod}\ 7) = 3 \ (\mathrm{mod}\ 7) = 3.$$

$$j(E'') = \frac{c_4^3}{\Delta} = \frac{4^3}{3} = \frac{64\ (\mathrm{mod}\ 7)}{3} = \frac{1\ (\mathrm{mod}\ 7)}{3} =$$

$$= 1\cdot 3^{-1} \ (\mathrm{mod}\ 7) = 1\cdot 5 \ (\mathrm{mod}\ 7) = 5 \ (\mathrm{mod}\ 7) = 5.$$

Заметим, что j-инвариант $j(E'')$ кривой E'' (2.32), так же как и j-инвариант $j(E)$ исходной кривой E (2.27), равен пяти.

Получается, что кривые E (2.27) и E'' (2.32) определены над полем $K = \mathbf{F}_p = \mathbf{F}_7$ и их j-инварианты равны, но они не изоморфны над этим полем, поскольку кривая E''

получена в результате, в частности, некорректной подстановки $Y = \sqrt{6}\,Y''$ из (2.31). Причиной некорректности этой подстановки является то, что коэффициент u^3 при Y'' в соответствии с (2.22) должен принадлежать $K = \mathbf{F}_p = \mathbf{F}_7$. Однако, $\sqrt{6} \notin \mathbf{F}_7$ (см. табл. 2.1), а это противоречит ранее данному определению изоморфных эллиптических кривых, включающему выражения (2.22).

Как следует из табл. 2.1, нет такого $a \in \mathbf{F}_7$, квадрат которого $b = a^2 \pmod 7$ равен шести, а, следовательно, $\sqrt{6}$ в $\mathbf{F}_7$ не существует и тогда, сделанная подстановка $Y = \sqrt{6}\,Y''$ из двух подстановок (2.31) при получении кривой E'' (2.32) из кривой E (2.27) была некорректна.

По такой же причине некорректности подстановки $Y = \sqrt{6}\,Y''$ из (2.31) кривые E (2.27) и E'' (2.32) не будут изоморфными и над некоторыми алгебраическими расширениями поля $\mathbf{F}_7$, например, над полями $\mathbf{F}_{11}$, $\mathbf{F}_{13}$ и $\mathbf{F}_{17}$, поскольку $\sqrt{6} \notin \mathbf{F}_{11}$, $\sqrt{6} \notin \mathbf{F}_{13}$ и $\sqrt{6} \notin \mathbf{F}_{17}$.

Кривые E (2.27) и E'' (2.32) не будут изоморфными, например, и над полем $\mathbf{F}_{19}$, также являющимся алгебраическим расширением поля $\mathbf{F}_7$, поскольку, в нем, хотя и существует $\sqrt{6}$, равный, например, пяти (см. табл. 2.2), но не существует элемента u, куб которого u^3 равен $\sqrt{6}$, т.е. пяти (см. табл. 2.3). Последний факт о несуществовании элемента u, куб которого u^3 равен $\sqrt{6}$, также противоречит определению изоморфных эллиптических кривых, включающему выражения (2.22).

Заметим, что кривые E (2.27) и E'' (2.32) будут изоморфны друг другу, но над любым алгебраическим расширением поля $\mathbf{F}_7$, содержащим как элемент $\sqrt{6}$, так и элемент u, куб которого u^3 равен $\sqrt{6}$.

Таблица 2.1

$a \in \mathbf{F}_7$	$b = a^2 \pmod 7$	$\sqrt{b} \pmod 7$
0	0 (mod 7) = 0	$\sqrt{0} = 0$
1	1 (mod 7) = 1	$\sqrt{1} = 1$
2	4 (mod 7) = 4	$\sqrt{4} = 2$
3	9 (mod 7) = 2	$\sqrt{2} = 3$
4	16 (mod 7) = 2	$\sqrt{2} = 4$
5	25 (mod 7) = 4	$\sqrt{4} = 5$
6	36 (mod 7) = 1	$\sqrt{1} = 6$

Таблица 2.2

$a \in \mathbf{F}_{19}$	$b = a^2 \pmod{19}$	$\sqrt{b} \pmod{19}$
0	0 (mod 19) = 0	$\sqrt{0} = 0$
1	1 (mod 19) = 1	$\sqrt{1} = 1$
2	4 (mod 19) = 4	$\sqrt{4} = 2$
3	9 (mod 19) = 9	$\sqrt{9} = 3$
4	16 (mod 19) = 16	$\sqrt{16} = 4$
5	25 (mod 19) = 6	$\sqrt{6} = 5$
6	36 (mod 19) = 17	$\sqrt{17} = 6$
7	49 (mod 19) = 11	$\sqrt{11} = 7$
8	64 (mod 19) = 7	$\sqrt{7} = 8$
9	81 (mod 19) = 5	$\sqrt{5} = 9$
10	100 (mod 19) = 5	$\sqrt{5} = 10$
11	121 (mod 19) = 7	$\sqrt{7} = 11$
12	144 (mod 19) = 11	$\sqrt{11} = 12$
13	169 (mod 19) = 17	$\sqrt{17} = 13$
14	196 (mod 19) = 6	$\sqrt{6} = 14$
15	225 (mod 19) = 16	$\sqrt{16} = 15$
16	256 (mod 19) = 9	$\sqrt{9} = 16$
17	289 (mod 19) = 4	$\sqrt{4} = 17$
18	324 (mod 19) = 1	$\sqrt{1} = 18$

Таблица 2.3

$u \in \mathbf{F}_{19}$	$u^2 \pmod{19}$
0	$0^3 \pmod{19} = 0 \pmod{19} = 0$
1	$1^3 \pmod{19} = 1 \pmod{19} = 1$
2	$2^3 \pmod{19} = 8 \pmod{19} = 8$
3	$3^3 \pmod{19} = 27 \pmod{19} = 8$
4	$4^3 \pmod{19} = 64 \pmod{19} = 7$
5	$5^3 \pmod{19} = 125 \pmod{19} = 11$
6	$6^3 \pmod{19} = 216 \pmod{19} = 7$
7	$7^3 \pmod{19} = 343 \pmod{19} = 1$

Продолжение табл. 2.3

$u \in \mathbf{F}_{19}$	$u^2 \pmod{19}$
8	$8^3 \pmod{19} = 512 \pmod{19} = 18$
9	$9^3 \pmod{19} = 729 \pmod{19} = 7$
10	$10^3 \pmod{19} = 1000 \pmod{19} = 12$
11	$11^3 \pmod{19} = 1331 \pmod{19} = 1$
12	$12^3 \pmod{19} = 1728 \pmod{19} = 18$
13	$13^3 \pmod{19} = 2197 \pmod{19} = 12$
14	$14^3 \pmod{19} = 2744 \pmod{19} = 8$
15	$15^3 \pmod{19} = 3375 \pmod{19} = 12$
16	$16^3 \pmod{19} = 4096 \pmod{19} = 11$
17	$17^3 \pmod{19} = 4913 \pmod{19} = 11$
18	$18^3 \pmod{19} = 5832 \pmod{19} = 18$

Например, кривые E (2.27) и E'' (2.32) будут изоморфны над полем $\mathbf{F}_{23}$, поскольку, во-первых, существует $\sqrt{6} \in \mathbf{F}_{23}$:

$$11^2 \pmod{23} = 6 \Rightarrow \sqrt{6} \pmod{23} = \sqrt{11^2} \pmod{23} = 11 \in \mathbf{F}_{23},$$

а, вторых, существует $u = 10$ из $\mathbf{F}_{23}$, для которого $u^3 = \sqrt{6}$:

$$10^3 \pmod{23} = 1000 \pmod{23} = 11 = \sqrt{6} \pmod{23}.$$

2.2. ГРУППОВОЙ ЗАКОН

2.2.1. ИЗОМОРФНАЯ ЭЛЛИПТИЧЕСКАЯ КРИВАЯ

Допустим, что характеристика char K поля K не равна двум и не равна трем, и рассмотрим замену переменных:

$$X = X' - \frac{b_2}{12}, \qquad Y = Y' - \frac{a_1}{2} \cdot \left(X' - \frac{b_2}{12} \right) - \frac{a_3}{2}, \tag{2.33}$$

переводящую эллиптическую кривую, заданную длинной (аффинной) формой Вейерштрасса (2.14), в изоморфную ей эллиптическую кривую, определяемую *короткой формой Вейерштрасса*:

$$E: \qquad Y^2 = X^3 + a\,X + b, \tag{2.34}$$

при некоторых $a, b \in K$.

Рассмотрим (второй) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.25), т.е. кривую E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$.

Установим конкретную замену переменных вида (2.33), используя при этом $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$ и коэффициент $b_2 = 2$, определенный при вычислении дискриминанта этой эллиптической кривой:

$$X = X' - \frac{b_2}{12} = X' - \frac{2}{12} = X' - \frac{2}{12 (\mathrm{mod} 5)} =$$

$$= X' - \frac{2}{2 (\mathrm{mod} 5)} = X' - 1, \tag{2.35}$$

$$Y = Y' - \frac{a_1}{2} \cdot \left(X' - \frac{b_2}{12} \right) - \frac{a_3}{2} =$$

$$= Y' - \frac{0}{2} \cdot (X' - 1) - \frac{4}{2} =$$

$$= Y' - 0 \cdot (X' - 1) - 2 =$$

$$= Y' - 0 - 2 =$$

$$= Y' - 2. \tag{2.36}$$

Получим изоморфную кривой E (2.25) кривую E', проведя установленную замену переменных (2.35), (2.36):

$$E: \; Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3,$$

$$E': \; (Y' - 2)^2 + 4 \cdot (Y' - 2) = (X' - 1)^3 + 3 \cdot (X' - 1)^2 + 3,$$

$$E': \; (Y')^2 + 2 \cdot Y' \cdot (-2) + (-2)^2 + 4 \cdot Y' - 8 =$$

$$= (X')^3 + 3 \cdot (X')^2 \cdot (-1) + 3 \cdot X' \cdot (-1)^2 + (-1)^3 + 3 \cdot \left((X')^2 + 2 \cdot X' \cdot (-1) + (-1)^2 \right) + 3,$$

$$E': \ (Y')^2 - 4 \cdot Y' + 4 + 4 \cdot Y' - 8 =$$

$$= (X')^3 - 3 \cdot (X')^2 + 3 \cdot X' - 1 + 3 \cdot \left((X')^2 - 2 \cdot X' + 1 \right) + 3,$$

$$E': \ (Y')^2 - 4 = (X')^3 - 3 \cdot (X')^2 + 3 \cdot X' - 1 + 3 \cdot (X')^2 - 6 \cdot X' + 3 + 3,$$

$$E': \ (Y')^2 - 4 = (X')^3 \ \ 3 \cdot X' - 5 \ (\text{mod } 5),$$

$$E': \ (Y')^2 = (X')^3 + (3) \ (\text{mod } 5) \cdot X' - 0 + 4,$$

$$E': \ (Y')^2 = (X')^3 + 2 \cdot X' + 4. \qquad (2.37)$$

Как мы убедились, полученная кривая E' (2.37), являющаяся изоморфной по отношению к кривой E (2.25), имеет вид короткой формы Вейерштрасса (2.34). При этом $a = 2$ и $b = 4$ ($a, b \in K = \mathbf{F}_p = \mathbf{F}_5 = \{0, 1, 2, 3, 4\}$).

Рассмотрим (третий) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.27), т.е. кривую E: $Y^2 = X^3 + X + 3$.

Установим конкретную замену переменных вида (2.33), используя при этом $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$ и коэффициент $b_2 = 0$, определенный при вычислении дискриминанта этой эллиптической кривой:

$$X = X' - \frac{b_2}{12} = X' - \frac{0}{12} = X' - 0 = X', \qquad (2.38)$$

$$Y = Y' - \frac{a_1}{2} \cdot \left(X' - \frac{b_2}{12} \right) - \frac{a_3}{2} =$$

$$= Y' - \frac{0}{2} \cdot (X' - 0) - \frac{0}{2} =$$

$$= Y' - 0 \cdot X' - 0 = Y' - 0 - 0 = Y'. \qquad (2.39)$$

Получим изоморфную кривой E (2.27) кривую E', проведя установленную замену переменных (2.38), (2.39):

$$E: \ Y^2 = X^3 + X + 3,$$

$$E': \ (Y')^2 = (X')^3 + X' + 3. \qquad (2.40)$$

Как видно, полученная кривая E' (2.40), являющаяся изоморфной по отношению к кривой E (2.27), сразу же приобрела короткую форму Вейерштрасса (2.34). При этом $a = 1$ и $b = 3$ ($a, b \in K = \mathbf{F}_p = \mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$).

Рассмотрим (четвертый) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.29), т.е. кривую E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$.

Установим конкретную замену переменных вида (2.33), используя при этом $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$ и коэффициент $b_2 = 6$, определенный при вычислении дискриминанта этой эллиптической кривой:

$$X = X' - \frac{b_2}{12} = X' - \frac{6}{12} = X' - \frac{6}{12\,(\mathrm{mod}11)} = X' - \frac{6}{1} = X' - 6, \qquad (2.41)$$

$$Y = Y' - \frac{a_1}{2} \cdot \left(X' - \frac{b_2}{12} \right) - \frac{a_3}{2} =$$

$$= Y' - \frac{10}{2} \cdot (X' - 6) - \frac{2}{2} =$$

$$= Y' - 5 \cdot (X' - 6) - 1 =$$

$$= Y' - 5 \cdot X' + 30 - 1 =$$

$$= Y' - 5 \cdot X' + 29 \ (\mathrm{mod}\ 11) =$$

$$= Y' - 5 \cdot X' + 7. \qquad (2.42)$$

Получим изоморфную кривой E (2.29) кривую E', проведя установленную замену переменных (2.41), (2.42):

$$E:\ Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4,$$

$$E':\ (Y' - 5 \cdot X' + 7)^2 + 10 \cdot (X' - 6) \cdot (Y' - 5 \cdot X' + 7) + 2 \cdot (Y' - 5 \cdot X' + 7) =$$

$$= (X' - 6)^3 + 4 \cdot (X' - 6)^2 + 4,$$

$$E':\ (Y' - 5 \cdot X')^2 + 2 \cdot (Y' - 5 \cdot X') \cdot 7 + 7^2 +$$

$$+ 10 \cdot (X'Y' - 5 \cdot (X')^2 + 7 \cdot X' - 6 \cdot Y' + 30 \cdot X' - 42) + 2 \cdot Y' - 10 \cdot X' + 14 =$$

$$= (X')^3 + 3 \cdot (X')^2 \cdot (-6) + 3 \cdot X' \cdot (-6)^2 + (-6)^3 +$$

$$+ 4 \cdot ((X')^2 + 2 \cdot X' \cdot (-6) + (-6)^2) + 4,$$

$$E':\ (Y')^2 + 2 \cdot Y' \cdot (-5 \cdot X') + (-5 \cdot X')^2 + 14 \cdot (Y' - 5 \cdot X') + 49 +$$

$$+ 10 \cdot (X'Y' - 5 \cdot (X')^2 + 37 \cdot X' - 6 \cdot Y' - 42) + 2 \cdot Y' - 10 \cdot X' + 14 =$$

$$= (X')^3 + (-18) \cdot (X')^2 + 108 \cdot X' - 216 +$$

$$+ 4 \cdot ((X')^2 + (-12) \cdot X' + 36) + 4,$$

$$E':\ (Y')^2 - 10 \cdot X' \cdot Y' + 25 \cdot (X')^2 + 14 \cdot Y' - 70 \cdot X' + 49 +$$

$$+ 10 \cdot X'Y' - 50 \cdot (X')^2 + 370 \cdot X' - 60 \cdot Y' - 420 + 2 \cdot Y' - 10 \cdot X' + 14 =$$

$$= (X')^3 - 18 \cdot (X')^2 + 108 \cdot X' - 216 + 4 \cdot (X')^2 - 48 \cdot X' + 144 + 4,$$

$$E':\ (Y')^2 - 25 \cdot (X')^2 - 44 \cdot Y' + 290 \cdot X' - 357 =$$

$$= (X')^3 - 14 \cdot (X')^2 + 60 \cdot X' - 68,$$

$$E' : \ (Y')^2 = (X')^3 + 11 \cdot (X')^2 - 230 \cdot X' + 44 \cdot Y' + 289,$$

$$E' : \ (Y')^2 = (X')^3 + 11 (\mathrm{mod} 11) \cdot (X')^2 - 230 (\mathrm{mod} 11) \cdot X' + 44 (\mathrm{mod} 11) \cdot Y' + 289 (\mathrm{mod}\ 11),$$

$$E' : \ (Y')^2 = (X')^3 + 0 \cdot (X')^2 + 1 \cdot X' + 0 \cdot Y' + 3,$$

$$E' : \ (Y')^2 = (X')^3 + X' + 3. \qquad (2.43)$$

Как видно, полученная кривая E' (2.43), являющаяся изоморфной по отношению к кривой E (2.29), имеет вид короткой формы Вейерштрасса (2.34). При этом $a = 1$ и $b = 3$ (a, $b \in K = \mathbf{F}_p = \mathbf{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$).

2.2.2. ГРУППОВОЙ ЗАКОН ПО МЕТОДУ ХОРД И КАСАТЕЛЬНЫХ

На представителях классов изоморфных эллиптических кривых вида (2.34) можно наглядно ввести групповой закон методом хорд и касательных. При этом *метод хорд и касательных* позволяет выполнять сложение, а, следовательно, и умножение точек эллиптических кривых.

Сложение точек эллиптической кривой реализуется с помощью хорд. Пусть P и Q являются двумя различными точками некоторой кубической кривой E над полем K вида (2.34). Если провести через эти точки P и Q прямую линию, то она обязательно пересечет эллиптическую кривую $E(K)$ в какой-нибудь третьей точке R. Заметим, что полученная таким образом точка R будет определена над тем же полем K, что и сама эллиптическая кривая E, а также исходные точки P и Q. Отразив затем точку R относительно горизонтальной оси, получим точку эллиптической кривой $E(K)$, представляющую сумму $P + Q$ (см. рис. 2.1).

Умножение (сложение одинаковых) точек эллиптической кривой $E(K)$ выполняется с помощью касательных, поскольку сложить точку кривой с собой невозможно с помощью хорды. Пусть P является какой-либо точкой кубической кривой E над полем K вида (2.34). Если провести через точку P касательную к нашей эллиптической кривой $E(K)$, то она пересечет ее в какой-нибудь другой точке (такая прямая должна пересекать эллиптическую кривую ровно в одной другой точке, поскольку кривая определяется кубическим уравнением). Назовем эту точку пересечения точкой R. Отразив точку R относительно горизонтальной оси, получим точку эллиптической кривой $E(K)$ под обозначением [2] P, которая представляет сумму $P + P$, т.е. *удвоенную точку P* или *точку порядка 2* (см. рис. 2.2).

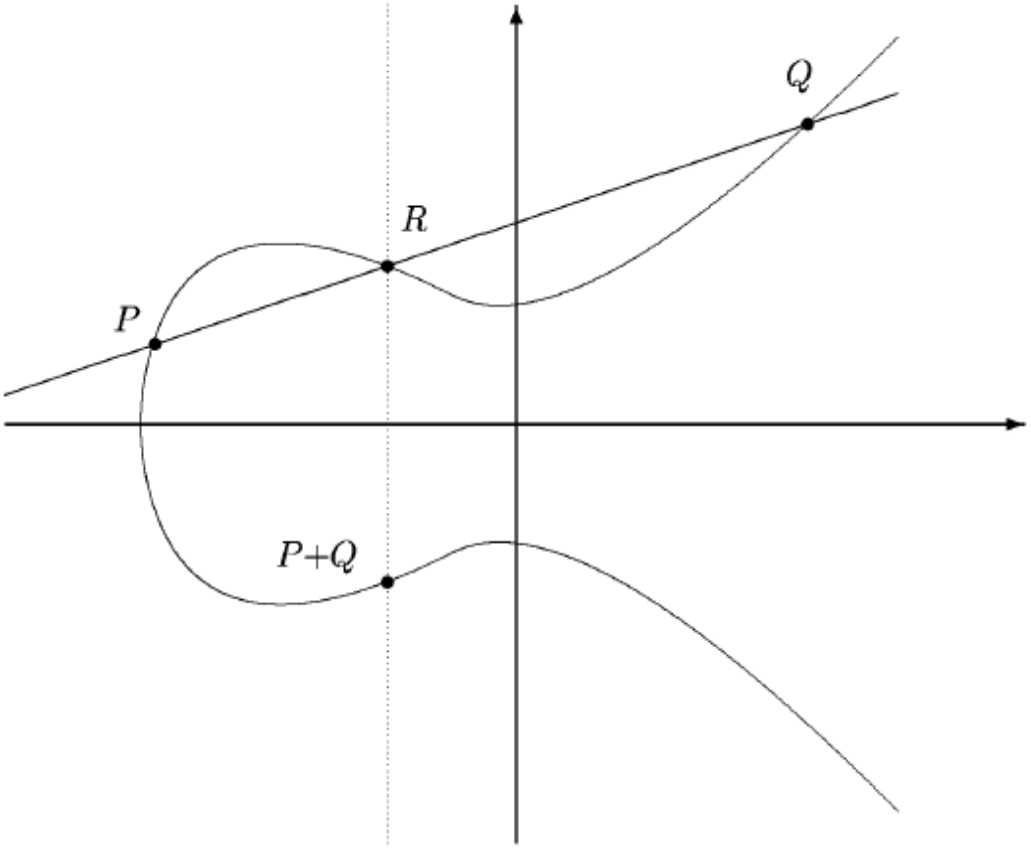


Рис. 2.1

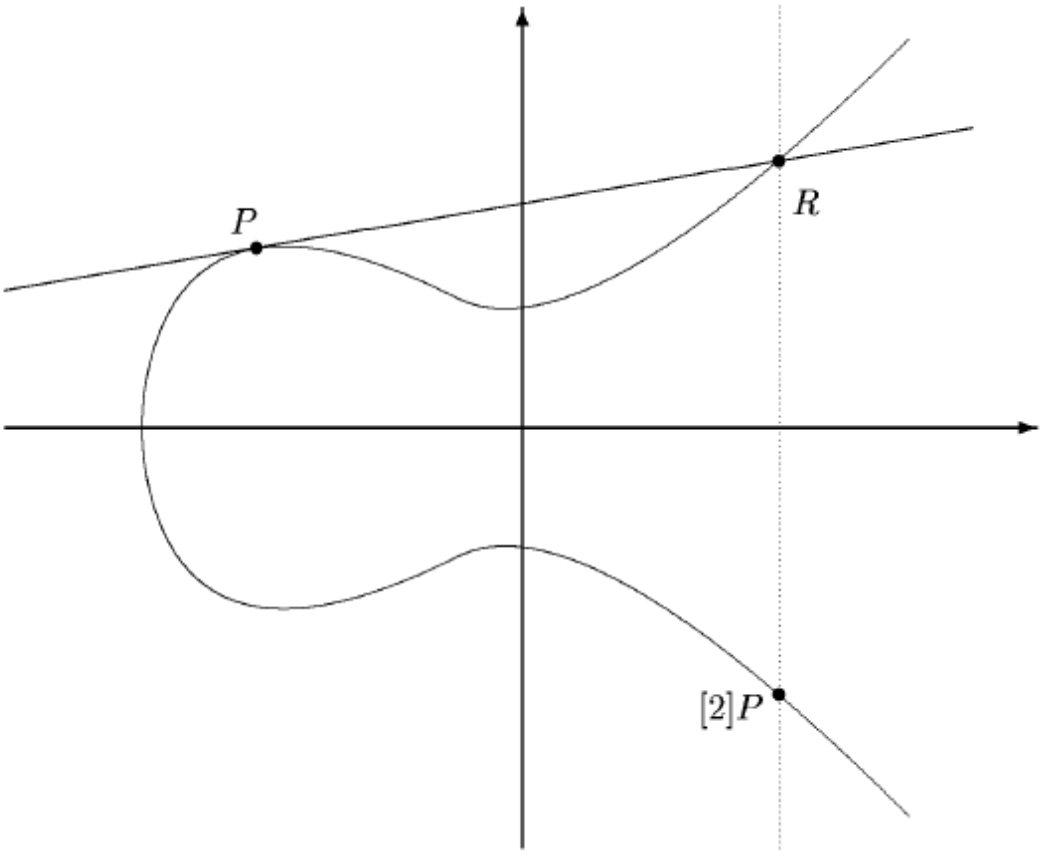


Рис. 2.2

Если же точка P на эллиптической кривой $E(K)$ выбрана так, что проведенная через нее касательная будет вертикальной прямой, то касательная «пересечет» эллиптическую кривую в бесконечно удаленной точке O, т.е. $P + P = O$. Пусть далее $O = (0, 0)$.

Заметим, что метод хорд и касательных наделяет эллиптическую кривую структурой абелевой группы с бесконечно удаленной точкой O в качестве нейтрального элемента по сложению, т.е. нуля. Причем определение операций можно достаточно легко перенести на случай общей эллиптической кривой, заданной длинной формой Вейерштрасса (в частности, с любой характеристикой поля). Только при этом на иллюстрациях выполнения операций необходимо заменить отражение точек эллиптической кривой относительно оси абсцисс на отражение точек относительно прямой:

$$Y = a_1 X + a_3. \tag{2.44}$$

2.2.3. РЕАЛИЗАЦИЯ СЛОЖЕНИЯ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Поскольку вычерчивание диаграмм в поле конечной характеристики является делом почти нереальным, приведем алгебраические формулы, с помощью которых можно реализовать сложение точек эллиптической кривой методом хорд и касательных.

Лемма 2.2. Пусть E является эллиптической кривой, определяемой аффинной версией уравнения Вейерштрасса (2.14):

$$E: \qquad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

и на ней выбраны точки $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$.

Если $P_1 = O$ и $P_2 = O$, то

$$x_3 = 0, \; y_3 = 0; \tag{2.45}$$

иначе, если $P_1 = O$, то:

$$x_3 = x_2 \text{ и } y_3 = y_2; \tag{2.46}$$

иначе, если $P_2 = O$, то:

$$x_3 = x_1 \text{ и } y_3 = y_1; \tag{2.47}$$

иначе, если $x_1 \neq x_2$, то:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \mu = \frac{y_1 \cdot x_2 - y_2 \cdot x_1}{x_2 - x_1} \tag{2.48}$$

и значения x_3 и y_3 вычисляются по формулам:

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2, \qquad y_3 = -(\lambda + a_1) \cdot x_3 - \mu - a_3 \tag{2.49}$$

в противном случае ($x_1 = x_2$) определяется с помощью соотношения (2.44) противоположная к P_1 точка:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) \tag{2.50}$$

и если $P_2 \neq -P_1$, то

$$\lambda = \frac{3 \cdot x_1^2 + 2 \cdot a_2 \cdot x_1 + a_4 - a_1 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3}, \quad \mu = \frac{-x_1^3 + a_4 \cdot x_1 + 2 \cdot a_6 - a_3 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3}, \tag{2.51}$$

и значения x_3 и y_3 вычисляются по формулам (2.49), но если $P_2 = -P_1$, то

$$P_1 + P_2 = O. \tag{2.52}$$

Применим приведенные алгебраические формулы (2.45) – (2.52) для сложения точек эллиптических кривых на примерах.

Рассмотрим (второй) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.25), т.е. кривую E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$.

Ранее нами было установлено, что на этой эллиптической кривой существует шесть точек (2.16):

$$\{(1, 2), (1, 4), (3, 2), (3, 4), (4, 0), (4, 1)\} \tag{2.53}$$

и бесконечно удаленная точка O.

Рассмотрим операцию сложения двух точек эллиптической кривой E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$ ($a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$).

Выберем, например, бесконечно удаленные точки $P_1 = (x_1, y_1) = (0, 0)$ и $P_2 = (x_2, y_2) = (0, 0)$ на этой кривой, т.е. $x_1 = 0$, $y_1 = 0$, $x_2 = 0$, $y_2 = 0$.

Поскольку $P_1 = O = (0, 0)$ и $P_2 = O = (0, 0)$, то в соответствии с (2.45):

$$x_3 = 0, \ y_3 = 0.$$

Следовательно, $O + O = O$.

Выберем, теперь бесконечно удаленную точку $P_1 = (x_1, y_1) = (0, 0)$ и точку $P_2 = (x_2, y_2) = (1, 2)$ на этой же кривой, т.е. $x_1 = 0$, $y_1 = 0$, $x_2 = 1$, $y_2 = 2$.

Поскольку P_1 и P_2 не равны одновременно бесконечно удаленной точке O, но $P_1 = O$, то в соответствии с (2.46):

$$x_3 = x_2 = 1 \text{ и } y_3 = y_2 = 2.$$

Следовательно, $O + (1, 2) = (1, 2)$.

Заметим, что сложение бесконечно удаленной точки O с точками (1, 4), (3, 2), (3, 4), (4, 0) и (4, 1) будет выполнено аналогичным образом, т.е. $O + (1, 4) = (1, 4)$, $O + (3, 2) = (3, 2)$, $O + (3, 4) = (3, 4)$, $O + (4, 0) = (4, 0)$ и $O + (4, 1) = (4, 1)$.

Пусть теперь выберем точку $P_1 = (x_1, y_1) = (1, 2)$ и бесконечно удаленную точку $P_2 = (x_2, y_2) = (0, 0)$ на этой кривой, т.е. $x_1 = 1$, $y_1 = 2$, $x_2 = 0$, $y_2 = 0$.

Поскольку P_1 и P_2 не равны одновременно бесконечно удаленной точке O, но $P_2 = O$, то в соответствии с (2.47):

$$x_3 = x_1 = 1 \text{ и } y_3 = y_1 = 2.$$

Следовательно, (1, 2) + O = (1, 2).

Выполним сложение точек $P_1 = (x_1, y_1) = (1, 2)$ и $P_2 = (x_2, y_2) = (1, 2)$ на этой кривой, т.е. $x_1 = 1,\ y_1 = 2,\ x_2 = 1,\ y_2 = 2$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $x_1 = x_2$, то определим с помощью соотношения (2.50) противоположную к P_1 точку:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) = (1, (-2 - 0 \cdot 1 - 4) \pmod 5) =$$

$$= (1, -6 \pmod 5) = (1, (-6 + 5 + 5) \pmod 5) =$$

$$= (1, 4 \pmod 5) = (1, 4),$$

и так как ($P_2 \neq -P_1$) = ((1, 2) ≠ (1, 4)) = ИСТИНА, то вычислим коэффициенты λ и μ по формулам (2.51):

$$\lambda = \frac{3 \cdot x_1^2 + 2 \cdot a_2 \cdot x_1 + a_4 - a_1 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3} = \frac{(3 \cdot 1^2 + 2 \cdot 3 \cdot 1 + 0 - 0 \cdot 2) \pmod 5}{(2 \cdot 2 + 0 \cdot 1 + 4) \pmod 5} =$$

$$= \frac{(3 \cdot 1 + 6 + 0 - 0) \pmod 5}{(4 + 4) \pmod 5} = \frac{9 \pmod 5}{8 \pmod 5} = \frac{(9 - 5) \pmod 5}{(8 - 5) \pmod 5} =$$

$$= \frac{4 \pmod 5}{3 \pmod 5} = \frac{(4 \cdot 3^{-1}) \pmod 5}{(3 \cdot 3^{-1}) \pmod 5} = \frac{(4 \cdot 2) \pmod 5}{1 \pmod 5} =$$

$$= 8 \pmod 5 = (8 - 5) \pmod 5 = 3 \pmod 5 = 3,$$

$$\mu = \frac{-x_1^3 + a_4 \cdot x_1 + 2 \cdot a_6 - a_3 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3} = \frac{(-1^3 + 0 \cdot 1 + 2 \cdot 3 - 4 \cdot 2) \pmod 5}{(2 \cdot 2 + 0 \cdot 1 + 4) \pmod 5} =$$

$$= \frac{(-1^3 + 0 \cdot 1 + 2 \cdot 3 - 4 \cdot 2) \pmod 5}{(2 \cdot 2 + 0 \cdot 1 + 4) \pmod 5} = \frac{(-1 + 0 + 6 - 8) \pmod 5}{(4 + 0 + 4) \pmod 5} =$$

$$= \frac{(-3) \pmod 5}{8 \pmod 5} = \frac{(-3 + 5) \pmod 5}{(8 - 5) \pmod 5} = \frac{2 \pmod 5}{3 \pmod 5} = \frac{(2 \cdot 3^{-1}) \pmod 5}{(3 \cdot 3^{-1}) \pmod 5} =$$

$$= \frac{(2 \cdot 2) \pmod 5}{1 \pmod 5} = \frac{4 \pmod 5}{1 \pmod 5} = 4 \pmod 5 = 4$$

и вычислим значения x_3 и y_3 по формулам (2.49):

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2 = (3^2 + 0 \cdot 3 - 3 - 1 - 1) \pmod 5 =$$

$$= (9 + 0 - 5) \pmod 5 = 4 \pmod 5 = 4,$$

$$y_3 = -(\lambda + a_1) \cdot x_3 - \mu - a_3 = (-(3 + 0) \cdot 4 - 4 - 4) \pmod 5 =$$

$$= (-3 \cdot 4 - 8) \pmod 5 = (-12 - 8) \pmod 5 = (-20) \pmod 5 =$$

$$= (-20 + 4 \cdot 5) \pmod 5 = (-20 + 20) \pmod 5 = 0 \pmod 5 = 0.$$

Следовательно, (1, 2) + (1, 2) = (4, 0).

Выполним теперь сложение точек $P_1 = (x_1, y_1) = (1, 2)$ и $P_2 = (x_2, y_2) = (1, 4)$ на этой кривой, т.е. $x_1 = 1,\ y_1 = 2,\ x_2 = 1,\ y_2 = 4$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $x_1 = x_2$, то определим с помощью соотношения (2.50) противоположную к P_1 точку:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) = (1, (-2 - 0 \cdot 1 - 4) \,(\mathrm{mod}\, 5)) =$$

$$= (1, (-2 - 0 - 4) \,(\mathrm{mod}\, 5)) = (1, (-6) \,(\mathrm{mod}\, 5)) = (1, (-6 + 2 \cdot 5) \,(\mathrm{mod}\, 5)) =$$

$$= (1, (-6 + 10) \,(\mathrm{mod}\, 5)) = (1, 4 \,(\mathrm{mod}\, 5)) = (1, 4),$$

и так как $(P_2 = -P_1) = ((1, 4) = (1, 4)) =$ ИСТИНА, то в соответствии с (2.52) получим, что (1, 2) + (1, 4) = O.

Выполним теперь сложение точек $P_1 = (x_1, y_1) = (1, 2)$ и $P_2 = (x_2, y_2) = (3, 2)$ на этой кривой, т.е. $x_1 = 1,\ y_1 = 2,\ x_2 = 3,\ y_2 = 2$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $(x_1 \neq x_2) = (1 \neq 3) =$ ИСТИНА, то в соответствии с (2.48) получим:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{(2 - 2) \,(\mathrm{mod} 5)}{(3 - 1) \,(\mathrm{mod} 5)} = \frac{0 \,(\mathrm{mod} 5)}{2 \,(\mathrm{mod} 5)} = \frac{0}{2} = 0,$$

$$\mu = \frac{y_1 \cdot x_2 - y_2 \cdot x_1}{x_2 - x_1} = \frac{(2 \cdot 3 - 2 \cdot 1) \,(\mathrm{mod} 5)}{(3 - 1) \,(\mathrm{mod} 5)} =$$

$$= \frac{(6 - 2) \,(\mathrm{mod} 5)}{2 \,(\mathrm{mod} 5)} = \frac{4 \,(\mathrm{mod} 5)}{2 \,(\mathrm{mod} 5)} = \frac{4}{2} = 2$$

и вычислим значения x_3 и y_3 по формулам (2.49):

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2 = (0^2 + 0 \cdot 0 - 3 - 1 - 3) \,(\mathrm{mod} 5) =$$

$$= (0 + 0 - 7) \,(\mathrm{mod} 5) = (-7) \,(\mathrm{mod} 5) = (-7 + 2 \cdot 5) \,(\mathrm{mod} 5) =$$

$$= (-7 + 10) \,(\mathrm{mod} 5) = 3 \,(\mathrm{mod} 5) = 3,$$

$$y_3 = -(\lambda + a_1) \cdot x_3 - \mu - a_3 = (-(0 + 0) \cdot 3 - 2 - 4) \,(\mathrm{mod} 5) =$$

$$= (-0 \cdot 3 - 6) \,(\mathrm{mod} 5) = -6 \,(\mathrm{mod} 5) = (-6 + 2 \cdot 5) \,(\mathrm{mod} 5) =$$

$$= (-6 + 10) \,(\mathrm{mod} 5) = 4 \,(\mathrm{mod} 5) = 4.$$

Следовательно, (1, 2) + (3, 2) = (3, 4).

Заметим, что сложение точки (1, 2) с точками (3, 4), (4, 0) и (4, 1) будет выполнено аналогичным образом, т.е. (1, 2) + (3, 4) = (4, 1), (1, 2) + (4, 0) = (3, 2) и (1, 2) + (4, 1) = (1, 4).

Проведенные расчеты позволяют заполнить первые две строки таблицы сложения точек эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, которая удовлетворяет аффинной версии уравнения Вейерштрасса (2.25), т.е. кривой E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$. Выполнив остальные расчеты, получим полную таблицу сложения (см. табл. 2.4).

Таблица 2.4

+	O	(1, 2)	(1, 4)	(3, 2)	(3, 4)	(4, 0)	(4, 1)
O	O	(1, 2)	(1, 4)	(3, 2)	(3, 4)	(4, 0)	(4, 1)
(1, 2)	(1, 2)	(4, 0)	O	(3, 4)	(4, 1)	(3, 2)	(1, 4)
(1, 4)	(1, 4)	O	(4, 1)	(4, 0)	(3, 2)	(1, 2)	(3, 4)
(3, 2)	(3, 2)	(3, 4)	(4, 0)	(1, 4)	O	(4, 1)	(1, 2)
(3, 4)	(3, 4)	(4, 1)	(3, 2)	O	(1, 2)	(1, 4)	(4, 0)
(4, 0)	(4, 0)	(3, 2)	(1, 2)	(4, 1)	(1, 4)	(3, 4)	O
(4, 1)	(4, 1)	(1, 4)	(3, 4)	(1, 2)	(4, 0)	O	(3, 2)

Рассмотрим (третий) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.27), т.е. кривую E: $Y^2 = X^3 + X + 3$.

Ранее нами было установлено, что на этой эллиптической кривой существует пять точек (2.17):

$$\{(4, 1), (4, 6), (5, 0), (6, 1), (6, 6)\} \qquad (2.54)$$

и бесконечно удаленная точка O.

Рассмотрим операцию сложения двух точек эллиптической кривой E: $Y^2 = X^3 + X + 3$ ($a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$).

Выберем, например, бесконечно удаленные точки $P_1 = (x_1, y_1) = (0, 0)$ и $P_2 = (x_2, y_2) = (0, 0)$ на этой кривой, т.е. $x_1 = 0$, $y_1 = 0$, $x_2 = 0$, $y_2 = 0$.

Поскольку $P_1 = O = (0, 0)$ и $P_2 = O = (0, 0)$, то в соответствии с (2.45):

$$x_3 = 0, \; y_3 = 0.$$

Следовательно, $O + O = O$.

Выберем теперь бесконечно удаленную точку $P_1 = (x_1, y_1) = (0, 0)$ и точку $P_2 = (x_2, y_2) = (4, 1)$ на этой же кривой, т.е. $x_1 = 0$, $y_1 = 0$, $x_2 = 4$, $y_2 = 1$.

Поскольку P_1 и P_2 не равны одновременно бесконечно удаленной точке O, но $P_1 = O$, то в соответствии с (2.46):

$$x_3 = x_2 = 4 \text{ и } y_3 = y_2 = 1.$$

Следовательно, $O + (4, 1) = (4, 1)$.

Заметим, что сложение бесконечно удаленной точки O с точками (4, 6), (5, 0), (6, 1) и (6, 6) будет выполнено аналогичным образом, т.е. $O + (4, 6) = (4, 6)$, $O + (5, 0) = (5, 0)$, $O + (6, 1) = (6, 1)$ и $O + (6, 6) = (6, 6)$.

Пусть теперь выберем точку $P_1 = (x_1, y_1) = (4, 1)$ и бесконечно удаленную точку $P_2 = (x_2, y_2) = (0, 0)$ на этой кривой, т.е. $x_1 = 4$, $y_1 = 1$, $x_2 = 0$, $y_2 = 0$.

Поскольку P_1 и P_2 не равны одновременно бесконечно удаленной точке O, но $P_2 = O$, то в соответствии с (2.47):

$$x_3 = x_1 = 4 \text{ и } y_3 = y_1 = 1.$$

Следовательно, (4, 1) + O = (4, 1).

Выполним сложение точек $P_1 = (x_1, y_1) = (4, 1)$ и $P_2 = (x_2, y_2) = (4, 1)$ на этой кривой, т.е. $x_1 = 4,\ y_1 = 1,\ x_2 = 4,\ y_2 = 1$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $x_1 = x_2$, то определим с помощью соотношения (2.50) противоположную к P_1 точку:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) = (4, (-1 - 0 \cdot 4 - 0) \pmod 7) =$$
$$= (4, -1 \pmod 7) = (4, (-1 + 7) \pmod 7) =$$
$$= (4, 6 \pmod 7) = (4, 6),$$

и так как $P_2 \neq -P_1$, то вычислим коэффициенты λ и μ по формулам (2.51):

$$\lambda = \frac{3 \cdot x_1^2 + 2 \cdot a_2 \cdot x_1 + a_4 - a_1 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3} = \frac{(3 \cdot 4^2 + 2 \cdot 0 \cdot 4 + 1 - 0 \cdot 1) \pmod 7}{(2 \cdot 1 + 0 \cdot 4 + 0) \pmod 7} =$$
$$= \frac{(3 \cdot 16 + 0 + 1 - 0) \pmod 7}{(2 + 0) \pmod 7} = \frac{49 \pmod 7}{2 \pmod 7} = \frac{0}{2} = 0,$$

$$\mu = \frac{-x_1^3 + a_4 \cdot x_1 + 2 \cdot a_6 - a_3 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3} = \frac{(-4^3 + 1 \cdot 4 + 2 \cdot 3 - 0 \cdot 1) \pmod 7}{(2 \cdot 1 + 0 \cdot 4 + 0) \pmod 7} =$$
$$= \frac{(-64 + 4 + 6) \pmod 7}{2 \pmod 7} = \frac{-54 \pmod 7}{2 \pmod 7} = \frac{(-54 + 7 \cdot 8) \pmod 7}{2} =$$
$$= \frac{(-54 + 56) \pmod 7}{2} = \frac{2 \pmod 7}{2} = \frac{2}{2} = 1$$

и вычислим значения x_3 и y_3 по формулам (2.49):

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2 = (0^2 + 0 \cdot 0 - 0 - 4 - 4) \pmod 7 =$$
$$= (-8) \pmod 7 = (-8 + 7 \cdot 2) \pmod 7 = (-8 + 14) \pmod 7 = 6 \pmod 7 = 6,$$
$$y_3 = -(\lambda + a_1) \cdot x_3 - \mu - a_3 = (-(0 + 0) \cdot 6 - 1 - 0) \pmod 7 =$$
$$= (-1) \pmod 7 = (-1 + 7) \pmod 7 = 6 \pmod 7 = 6.$$

Следовательно, (4, 1) + (4, 1) = (6, 6).

Выполним теперь сложение точек $P_1 = (x_1, y_1) = (4, 1)$ и $P_2 = (x_2, y_2) = (4, 6)$ на этой кривой, т.е. $x_1 = 4,\ y_1 = 1,\ x_2 = 4,\ y_2 = 6$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $x_1 = x_2$, то определим с помощью соотношения (2.50) противоположную к P_1 точку:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) = (4, (-1 - 0 \cdot 4 - 0) \pmod 7) =$$
$$= (4, -1 \pmod 7) = (4, (-1 + 7) \pmod 7) = = (4, 6 \pmod 7) = (4, 6)$$

и так как ($P_2 = -P_1$) = ((4, 6) = (4, 6)) = ИСТИНА, то в соответствии с (2.52) получим, что (4, 1) + (4, 6) = O.

Выполним теперь сложение точек $P_1 = (x_1, y_1) = (4, 1)$ и $P_2 = (x_2, y_2) = (5, 0)$ на этой кривой, т.е. $x_1 = 4,\ y_1 = 1,\ x_2 = 5,\ y_2 = 0$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и ($x_1 \neq x_2$) = ($4 \neq 5$) = ИСТИНА, то в соответствии с (2.48) получим:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{(0-1)\,(\mathrm{mod}7)}{(5-4)\,(\mathrm{mod}7)} = \frac{(-1)\,(\mathrm{mod}7)}{1\,(\mathrm{mod}7)} =$$

$$= \frac{(-1+7)\,(\mathrm{mod}7)}{1} = 6\,(\mathrm{mod}7) = 6,$$

$$\mu = \frac{y_1 \cdot x_2 - y_2 \cdot x_1}{x_2 - x_1} = \frac{(1\cdot 5 - 0\cdot 4)\,(\mathrm{mod}7)}{(5-4)\,(\mathrm{mod}7)} =$$

$$= \frac{5\,(\mathrm{mod}7)}{1\,(\mathrm{mod}7)} = \frac{5}{1} = 5$$

и вычислим значения x_3 и y_3 по формулам (2.49):

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2 = (6^2 + 0\cdot 6 - 0 - 4 - 5)\,(\mathrm{mod}7) =$$

$$= (36-9)\,(\mathrm{mod}7) = 27\,(\mathrm{mod}7) = (27 - 7\cdot 3)\,(\mathrm{mod}7) =$$

$$= (27-21)\,(\mathrm{mod}7) = 6\,(\mathrm{mod}7) = 6,$$

$$y_3 = -(\lambda + a_1)\cdot x_3 - \mu - a_3 = (-(6+0)\cdot 6 - 5 - 0)\,(\mathrm{mod}7) =$$

$$= (-36-5)\,(\mathrm{mod}7) = -41\,(\mathrm{mod}7) = (-41 + 7\cdot 6)\,(\mathrm{mod}7) =$$

$$= (-41+42)\,(\mathrm{mod}7) = 1\,(\mathrm{mod}7) = 1.$$

Следовательно, (4, 1) + (5, 0) = (6, 1).

Заметим, что сложение точки (4, 1) с точками (6, 1) и (6, 6) будет выполнено аналогичным образом, т.е. (4, 1) + (6, 1) = (4, 6) и (4, 1) + (6, 6) = (5, 0).

Проведенные расчеты позволяют заполнить первые две строки таблицы сложения точек эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, которая удовлетворяет аффинной версии уравнения Вейерштрасса (2.27), т.е. кривой E: $Y^2 = X^3 + X + 3$. Выполнив остальные расчеты, получим полную таблицу сложения (см. табл. 2.5).

Рассмотрим (четвертый) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.29), т.е. кривую E: $Y^2 + 10\cdot XY + 2\cdot Y = X^3 + 4\cdot X^2 + 4$.

Таблица 2.5

+	*O*	(4, 1)	(4, 6)	(5, 0)	(6, 1)	(6, 6)
O	*O*	(4, 1)	(4, 6)	(5, 0)	(6, 1)	(6, 6)
(4, 1)	(4, 1)	(6, 6)	*O*	(6, 1)	(4, 6)	(5, 0)
(4, 6)	(4, 6)	*O*	(6, 1)	(6, 6)	(5, 0)	(4, 1)
(5, 0)	(5, 0)	(6, 1)	(6, 6)	*O*	(4, 1)	(4, 6)
(6, 1)	(6, 1)	(4, 6)	(5, 0)	(4, 1)	(6, 6)	*O*
(6, 6)	(6, 6)	(5, 0)	(4, 1)	(4, 6)	*O*	(6, 1)

Ранее нами было установлено, что на этой эллиптической кривой существует семнадцать точек (2.18):

$$\{(0, 3), (0, 6), (1, 4), (1, 6), (3, 4), (3, 8), (4, 0), (4, 2), (5, 1), (5, 2),$$
$$(6, 6), (6, 9), (8, 3), (9, 2), (9, 5), (10, 3), (10, 5)\} \quad (2.55)$$

и бесконечно удаленная точка *O*.

Рассмотрим операцию сложения двух точек эллиптической кривой *E*: $Y^2 + 10 \cdot XY ++ 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$ ($a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$).

Выберем, например, бесконечно удаленные точки $P_1 = (x_1, y_1) = (0, 0)$ и $P_2 = (x_2, y_2) = (0, 0)$ на этой кривой, т.е. $x_1 = 0,\ y_1 = 0,\ x_2 = 0,\ y_2 = 0$.

Поскольку $P_1 = O = (0, 0)$ и $P_2 = O = (0, 0)$, то в соответствии с (2.45):

$$x_3 = 0,\ y_3 = 0.$$

Следовательно, $O + O = O$.

Выберем, теперь бесконечно удаленную точку $P_1 = (x_1, y_1) = (0, 0)$ и точку $P_2 = (x_2, y_2) = (0, 3)$ на этой же кривой, т.е. $x_1 = 0,\ y_1 = 0,\ x_2 = 0,\ y_2 = 3$.

Поскольку P_1 и P_2 не равны одновременно бесконечно удаленной точке *O*, но $P_1 = O$, то в соответствии с (2.46):

$$x_3 = x_2 = 0 \text{ и } y_3 = y_2 = 3.$$

Следовательно, $O + (0, 3) = (0, 3)$.

Заметим, что сложение бесконечно удаленной точки *O* с точками (0, 6), (1, 4), (1, 6), (3, 4), (3, 8), (4, 0), (4, 2), (5, 1), (5, 2), (6, 6), (6, 9), (8, 3), (9, 2), (9, 5), (10, 3) и (10, 5) будет выполнено аналогичным образом, т.е. $O + (0, 6) = (0, 6)$, $O + (1, 4) = (1, 4)$, $O + (1, 6) = = (1, 6)$, $O + (3, 4) = (3, 4)$, $O + (3, 8) = (3, 8)$, $O + (4, 0) = (4, 0)$, $O + (4, 2) = (4, 2)$, $O + (5, 1) = = (5, 1)$, $O + (5, 2) = (5, 2)$, $O + (6, 6) = (6, 6)$, $O + (6, 9) = (6, 9)$, $O + (8, 3) = (8, 3)$, $O + (9, 2) = = (9, 2)$, $O + (9, 5) = (9, 5)$, $O + (10, 3) = (10, 3)$ и $O + (10, 5) = (10, 5)$.

Пусть теперь выберем точку $P_1 = (x_1, y_1) = (0, 3)$ и бесконечно удаленную точку $P_2 = (x_2, y_2) = (0, 0)$ на этой кривой, т.е. $x_1 = 0,\ y_1 = 3,\ x_2 = 0,\ y_2 = 0$.

Поскольку P_1 и P_2 не равны одновременно бесконечно удаленной точке O, но $P_2 = O$, то в соответствии с (2.47):

$$x_3 = x_1 = 0 \text{ и } y_3 = y_1 = 3.$$

Следовательно, (0, 3) + O = (0, 3).

Выполним сложение точек $P_1 = (x_1, y_1) = (0, 3)$ и $P_2 = (x_2, y_2) = (0, 3)$ на этой кривой, т.е. $x_1 = 0,\ y_1 = 3,\ x_2 = 0,\ y_2 = 3$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $x_1 = x_2$, то определим с помощью соотношения (2.50) противоположную к P_1 точку:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) = (0, (-3 - 10 \cdot 0 - 2)\ (\text{mod}11)) =$$

$$= (0, -5\ (\text{mod}11)) = (0, (-5 + 11)\ (\text{mod}11)) = = (0, 6\ (\text{mod}11)) = (0, 6),$$

и так как $P_2 \neq -P_1$, то вычислим коэффициенты λ и μ по формулам (2.51):

$$\lambda = \frac{3 \cdot x_1^2 + 2 \cdot a_2 \cdot x_1 + a_4 - a_1 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3} = \frac{(3 \cdot 0^2 + 2 \cdot 4 \cdot 0 + 0 - 10 \cdot 3)\ (\text{mod}11)}{(2 \cdot 3 + 10 \cdot 0 + 2)\ (\text{mod}11)} =$$

$$= \frac{(0 + 0 + 0 - 30)\ (\text{mod}11)}{(6 + 2)\ (\text{mod}11)} = \frac{(-30 + 3 \cdot 11)\ (\text{mod}11)}{8\ (\text{mod}11)} =$$

$$= \frac{(-30 + 33)\ (\text{mod}11)}{8\ (\text{mod}11)} = \frac{3\ (\text{mod}11)}{8\ (\text{mod}11)} = \frac{(3 \cdot 8^{-1})\ (\text{mod}11)}{(8 \cdot 8^{-1})\ (\text{mod}11)} =$$

$$= \frac{(3 \cdot 7)\ (\text{mod}11)}{1\ (\text{mod}11)} = 21\ (\text{mod}11) = (21 - 11)\ (\text{mod}11) = 10\ (\text{mod}11) = 10,$$

$$\mu = \frac{-x_1^3 + a_4 \cdot x_1 + 2 \cdot a_6 - a_3 \cdot y_1}{2 \cdot y_1 + a_1 \cdot x_1 + a_3} = \frac{(-0^3 + 0 \cdot 0 + 2 \cdot 4 - 2 \cdot 3)\ (\text{mod}11)}{(2 \cdot 3 + 10 \cdot 0 + 2)\ (\text{mod}11)} =$$

$$= \frac{(0 + 0 + 8 - 6)\ (\text{mod}11)}{(6 + 0 + 2)\ (\text{mod}11)} = \frac{2\ (\text{mod}11)}{8\ (\text{mod}11)} = \frac{(2 \cdot 8^{-1})\ (\text{mod}11)}{(8 \cdot 8^{-1})\ (\text{mod}11)} =$$

$$= \frac{(2 \cdot 7)\ (\text{mod}11)}{1\ (\text{mod}11)} = 14\ (\text{mod}11) = (14 - 11)\ (\text{mod}11) = 3$$

и вычислим значения x_3 и y_3 по формулам (2.49):

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2 = (10^2 + 10 \cdot 10 - 4 - 0 - 0)\ (\text{mod}11) =$$

$$= (100 + 100 - 4)\ (\text{mod}11) = 196\ (\text{mod}11) = (196 - 17 \cdot 11)\ (\text{mod}11) =$$

$$= (196 - 187)\ (\text{mod}11) = 9\ (\text{mod}11) = 9,$$

$$y_3 = -(\lambda + a_1) \cdot x_3 - \mu - a_3 = (-(10 + 10) \cdot 9 - 3 - 2)\ (\text{mod}11) =$$

$$= (-180 - 5)\ (\text{mod}11) = -185\ (\text{mod}11) = (-185 + 17 \cdot 11)\ (\text{mod}11) =$$

$$= (-185 + 187)\ (\text{mod}11) = 2\ (\text{mod}11) = 2.$$

Следовательно, (0, 3) + (0, 3) = (9, 2).

Выполним теперь сложение точек $P_1 = (x_1, y_1) = (0, 3)$ и $P_2 = (x_2, y_2) = (0, 6)$ на этой кривой, т.е. $x_1 = 0,\ y_1 = 3,\ x_2 = 0,\ y_2 = 6$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $x_1 = x_2$, то определим с помощью соотношения (2.50) противоположную к P_1 точку:

$$-P_1 = (x_1, -y_1 - a_1 \cdot x_1 - a_3) = (0, (-3 - 10 \cdot 0 - 2)\ (\mathrm{mod}11)) =$$

$$= (0, (-3 - 0 - 2)\ (\mathrm{mod}11)) = (0, -5\ (\mathrm{mod}11)) =$$

$$= (0, (-5 + 11)\ (\mathrm{mod}11)) = (0, 6\ (\mathrm{mod}11)) = (0, 6),$$

и так как $(P_2 = -P_1) = ((0, 6) = (0, 6)) =$ ИСТИНА, то в соответствии с (2.52) получим, что (0, 3) + (0, 6) = 0.

Выполним теперь сложение точек $P_1 = (x_1, y_1) = (0, 3)$ и $P_2 = (x_2, y_2) = (1, 4)$ на этой кривой, т.е. $x_1 = 0,\ y_1 = 3,\ x_2 = 1,\ y_2 = 4$.

Поскольку ни одна из точек P_1 и P_2 не является бесконечно удаленной точкой O и $(x_1 \neq x_2) = (0 \neq 1) =$ ИСТИНА, то в соответствии с (2.48) получим:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{(4 - 3)\ (\mathrm{mod}11)}{(1 - 0)\ (\mathrm{mod}11)} = \frac{1\ (\mathrm{mod}11)}{1\ (\mathrm{mod}11)} = \frac{1}{1} = 1,$$

$$\mu = \frac{y_1 \cdot x_2 - y_2 \cdot x_1}{x_2 - x_1} = \frac{(3 \cdot 1 - 4 \cdot 0)\ (\mathrm{mod}11)}{(1 - 0)\ (\mathrm{mod}11)} =$$

$$= \frac{(3 - 0)\ (\mathrm{mod}11)}{1\ (\mathrm{mod}11)} = \frac{3\ (\mathrm{mod}11)}{1\ (\mathrm{mod}11)} = \frac{3}{1} = 3$$

и вычислим значения x_3 и y_3 по формулам (2.49):

$$x_3 = \lambda^2 + a_1 \cdot \lambda - a_2 - x_1 - x_2 = (1^2 + 10 \cdot 1 - 4 - 0 - 1)\ (\mathrm{mod}11) =$$

$$= (1 + 10 - 5)\ (\mathrm{mod}11) = 6\ (\mathrm{mod}11) = 6,$$

$$y_3 = -(\lambda + a_1) \cdot x_3 - \mu - a_3 = (-(1 + 10) \cdot 6 - 3 - 2)\ (\mathrm{mod}11) =$$

$$= (-66 - 5)\ (\mathrm{mod}11) = (-71)\ (\mathrm{mod}11) = (-71 + 7 \cdot 11)\ (\mathrm{mod}11) =$$

$$= (-71 + 77)\ (\mathrm{mod}11) = 6\ (\mathrm{mod}11) = 6.$$

Следовательно, (0, 3) + (1, 4) = (6, 6).

Заметим, что сложение точки (0, 3) с точками (1, 6), (3, 4), (3, 8), (4, 0), (4, 2), (5, 1), (5, 2), (6, 6), (6, 9), (8, 3), (9, 2), (9, 5), (10, 3) и (10, 5) будет выполнено аналогичным образом, т.е. (0, 3) + (1, 6) = (1, 4), (0, 3) + (3, 4) = (5, 2), (0, 3) + (3, 8) = (10, 3), (0, 3) + (4, 0) = = (5, 1), (0, 3) + (4, 2) = (4, 0), (0, 3) + (5, 1) = (3, 8), (0, 3) + (5, 2) = (4, 2), (0, 3) + (6, 6) = = (9, 5), (0, 3) + (6, 9) = (1, 6), (0, 3) + (8, 3) = (10, 5), (0, 3) + (9, 2) = (6, 9), (0, 3) + (9, 5) = = (0, 6), (0, 3) + (10, 3) = (8, 3) и (0, 3) + (10, 5) = (3, 4).

Проведенные расчеты позволяют заполнить первые две строки таблицы сложения точек эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, которая удовлетворяет аффинной версии уравнения Вейерштрасса (2.29), т.е. кривой E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$. Выполнив остальные расчеты, получим полную таблицу сложения (см. табл. 2.6, 2.7).

Описанный ранее изоморфизм эллиптических кривых сохраняет структуру группы. Поэтому на изоморфных кривых приведенные выше формулы определяют структуры изоморфных абелевых групп.

Таблица 2.6

+	O	(0, 3)	(0, 6)	(1, 4)	(1, 6)	(3, 4)	(3, 8)	(4, 0)	(4, 2)
O	O	(0, 3)	(0, 6)	(1, 4)	(1, 6)	(3, 4)	(3, 8)	(4, 0)	(4, 2)
(0, 3)	(0, 3)	(9, 2)	O	(6, 6)	(1, 4)	(5, 2)	(10, 3)	(5, 1)	(4, 0)
(0, 6)	(0, 6)	O	(9, 5)	(1, 6)	(6, 9)	(10, 5)	(5, 1)	(4, 2)	(5, 2)
(1, 4)	(1, 4)	(6, 6)	(1, 6)	(0, 3)	O	(3, 8)	(5, 2)	(10, 5)	(8, 3)
(1, 6)	(1, 6)	(1, 4)	(6, 9)	O	(0, 6)	(5, 1)	(3, 4)	(8, 3)	(10, 3)
(3, 4)	(3, 4)	(5, 2)	(10, 5)	(3, 8)	(5, 1)	(1, 6)	O	(9, 5)	(6, 6)
(3, 8)	(3, 8)	(10, 3)	(5, 1)	(5, 2)	(3, 4)	O	(1, 4)	(6, 9)	(9, 2)
(4, 0)	(4, 0)	(5, 1)	(4, 2)	(10, 5)	(8, 3)	(9, 5)	(6, 9)	(0, 3)	O
(4, 2)	(4, 2)	(4, 0)	(5, 2)	(8, 3)	(10, 3)	(6, 6)	(9, 2)	O	(0, 6)
(5, 1)	(5, 1)	(3, 8)	(4, 0)	(3, 4)	(10, 5)	(0, 6)	(1, 6)	(9, 2)	(0, 3)
(5, 2)	(5, 2)	(4, 2)	(3, 4)	(10, 3)	(3, 8)	(1, 4)	(0, 3)	(0, 6)	(9, 5)
(6, 6)	(6, 6)	(9, 5)	(1, 4)	(9, 2)	(0, 3)	(10, 3)	(4, 2)	(3, 4)	(10, 5)
(6, 9)	(6, 9)	(1, 6)	(9, 2)	(0, 6)	(9, 5)	(4, 0)	(10, 5)	(10, 3)	(3, 8)
(8, 3)	(8, 3)	(10, 5)	(10, 3)	(4, 0)	(4, 2)	(9, 2)	(9, 5)	(1, 4)	(1, 6)
(9, 2)	(9, 2)	(6, 9)	(0, 3)	(9, 5)	(6, 6)	(4, 2)	(8, 3)	(3, 8)	(5, 1)
(9, 5)	(9, 5)	(0, 6)	(6, 6)	(6, 9)	(9, 2)	(8, 3)	(4, 0)	(5, 2)	(3, 4)
(10, 3)	(10, 3)	(8, 3)	(3, 8)	(4, 2)	(5, 2)	(0, 3)	(6, 6)	(1, 6)	(6, 9)
(10, 5)	(10, 5)	(3, 4)	(8, 3)	(5, 1)	(4, 0)	(6, 9)	(0, 6)	(6, 6)	(1, 4)

Таблица 2.7

+	(5, 1)	(5, 2)	(6, 6)	(6, 9)	(8, 3)	(9, 2)	(9, 5)	(10, 3)	(10, 5)
O	(5, 1)	(5, 2)	(6, 6)	(6, 9)	(8, 3)	(9, 2)	(9, 5)	(10, 3)	(10, 5)
(0, 3)	(3, 8)	(4, 2)	(9, 5)	(1, 6)	(10, 5)	(6, 9)	(0, 6)	(8, 3)	(3, 4)
(0, 6)	(4, 0)	(3, 4)	(1, 4)	(9, 2)	(10, 3)	(0, 3)	(6, 6)	(3, 8)	(8, 3)
(1, 4)	(3, 4)	(10, 3)	(9, 2)	(0, 6)	(4, 0)	(9, 5)	(6, 9)	(4, 2)	(5, 1)
(1, 6)	(10, 5)	(3, 8)	(0, 3)	(9, 5)	(4, 2)	(6, 6)	(9, 2)	(5, 2)	(4, 0)
(3, 4)	(0, 6)	(1, 4)	(10, 3)	(4, 0)	(9, 2)	(4, 2)	(8, 3)	(0, 3)	(6, 9)
(3, 8)	(1, 6)	(0, 3)	(4, 2)	(10, 5)	(9, 5)	(8, 3)	(4, 0)	(6, 6)	(0, 6)
(4, 0)	(9, 2)	(0, 6)	(3, 4)	(10, 3)	(1, 4)	(3, 8)	(5, 2)	(1, 6)	(6, 6)
(4, 2)	(0, 3)	(9, 5)	(10, 5)	(3, 8)	(1, 6)	(5, 1)	(3, 4)	(6, 9)	(1, 4)
(5, 1)	(6, 9)	*O*	(5, 2)	(8, 3)	(6, 6)	(10, 3)	(4, 2)	(1, 4)	(9, 5)
(5, 2)	*O*	(6, 6)	(8, 3)	(5, 1)	(6, 9)	(4, 0)	(10, 5)	(9, 2)	(1, 6)
(6, 6)	(5, 2)	(8, 3)	(6, 9)	*O*	(5, 1)	(0, 6)	(1, 6)	(4, 0)	(3, 8)
(6, 9)	(8, 3)	(5, 1)	*O*	(6, 6)	(5, 2)	(1, 4)	(0, 3)	(3, 4)	(4, 2)
(8, 3)	(6, 6)	(6, 9)	(5, 1)	(5, 2)	*O*	(3, 4)	(3, 8)	(0, 6)	(0, 3)
(9, 2)	(10, 3)	(4, 0)	(0, 6)	(1, 4)	(3, 4)	(1, 6)	*O*	(10, 5)	(5, 2)
(9, 5)	(4, 2)	(10, 5)	(1, 6)	(0, 3)	(3, 8)	*O*	(1, 4)	(5, 1)	(10, 3)
(10, 3)	(1, 4)	(9, 2)	(4, 0)	(3, 4)	(0, 6)	(10, 5)	(5, 1)	(9, 5)	*O*
(10, 5)	(9, 5)	(1, 6)	(3, 8)	(4, 2)	(0, 3)	(5, 2)	(10, 3)	*O*	(9, 2)

2.2.4. ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Рассмотрим задачу дискретного логарифмирования на эллиптической кривой. Для этого зафиксируем некоторое натуральное число m и обозначим через $[m]P$ результат выполнения одноместной операции $[m]$, вычисляющей сумму из m точек P:

$$[m]:\ P \to \underbrace{P + P + \ldots + P}_{m}. \qquad (2.56)$$

Возьмем (второй) пример эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$. Эта кривая удовлетворяет аффинной версии уравнения Вейерштрасса (2.25), т.е. является кривой E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$. В соответствии с выражением (2.56) вычислим результаты выполнения введенной одноместной операции $[m]$ над P для различных значений P из множества (2.53).

Пусть вначале $P = (1, 2)$, тогда в соответствии с (2.56) получим:

$$m = 1\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([1]\text{: } P \to \underbrace{P + P + \ldots + P}_{1}) =$$

$$= ([1]\text{: } P \to P) = ([1]\text{: } (1, 2) \to (1, 2));$$

$$m = 2\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([2]\text{: } P \to \underbrace{P + P + \ldots + P}_{2}) =$$

$$= ([2]\text{: } P \to P + P) = ([2]\text{: } (1, 2) \to (1, 2) + (1, 2)) = ([2]\text{: } (1, 2) \to (4, 0));$$

$$m = 3\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([3]\text{: } P \to \underbrace{P + P + \ldots + P}_{3}) =$$

$$= ([3]\text{: } P \to P + P + P) = ([3]\text{: } (1, 2) \to (1, 2) + (1, 2) + (1, 2)) =$$

$$= ([3]\text{: } (1, 2) \to (4, 0) + (1, 2)) = ([3]\text{: } (1, 2) \to (3, 2));$$

$$m = 4\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([4]\text{: } P \to \underbrace{P + P + \ldots + P}_{4}) =$$

$$= ([4]\text{: } P \to P + P + P + P) = ([4]\text{: } (1, 2) \to (1, 2) + (1, 2) + (1, 2) + (1, 2)) =$$

$$= ([4]\text{: } (1, 2) \to (3, 2) + (1, 2)) = ([4]\text{: } (1, 2) \to (3, 4));$$

$$m = 5\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([5]\text{: } P \to \underbrace{P + P + \ldots + P}_{5}) =$$

$$= ([5]\text{: } P \to P + P + P + P + P) = ([5]\text{: } (1, 2) \to (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2)) =$$

$$= ([5]\text{: } (1, 2) \to (3, 4) + (1, 2)) = ([5]\text{: } (1, 2) \to (4, 1));$$

$$m = 6\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([6]\text{: } P \to \underbrace{P + P + \ldots + P}_{6}) =$$

$$= ([6]\text{: } P \to P + P + P + P + P + P) =$$

$$= ([6]\text{: } (1, 2) \to (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2)) =$$

$$= ([6]\text{: } (1, 2) \to (4, 1) + (1, 2)) = ([6]\text{: } (1, 2) \to (1, 4));$$

$$m = 7\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([7]\text{: } P \to \underbrace{P + P + \ldots + P}_{7}) =$$

$$= ([7]\text{: } P \to P + P + P + P + P + P + P) =$$

$$= ([7]\text{: } (1, 2) \to (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2)) =$$

$$= ([7]\text{: } (1, 2) \to (1, 4) + (1, 2)) = ([7]\text{: } (1, 2) \to O).$$

Заметим, что в результате выполнения одноместной операции (2.56) над $P = (1, 2)$ получены все элементы (второго примера) эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, т.е. кривой E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$. Поэтому можно говорить о том, что данная эллиптическая кривая представляет собой конечную циклическую группу седьмого порядка, а точка $P = (1, 2)$ является ее образующей (примитивным элементом).

Зададим аналогично (1.15) функцию дискретного логарифмирования (по основанию (1, 2)) в этой группе перечислением ее элементов:

$$\mathrm{dlog}_{(1,\,2)}\, O = 7$$

(дискретный логарифм элемента O = (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) =

= (1, 2) · 7 по основанию (1, 2) равен 7),

$$\mathrm{dlog}_{(1,\,2)}\,(1, 2) = 1$$

(дискретный логарифм элемента (1, 2) = (1, 2) =

= (1, 2) · 1 по основанию (1, 2) равен 1),

$$\mathrm{dlog}_{(1,\,2)}\,(1, 4) = 6$$

(дискретный логарифм элемента (1, 4) = (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) =

= (1, 2) · 6 по основанию (1, 2) равен 6),

$$\mathrm{dlog}_{(1,\,2)}\,(3, 2) = 3$$

(дискретный логарифм элемента (3, 2) = (1, 2) + (1, 2) + (1, 2) =

= (1, 2) · 3 по основанию (1, 2) равен 3),

$$\mathrm{dlog}_{(1,\,2)}\,(3, 4) = 4$$

(дискретный логарифм элемента (3, 4) = (1, 2) + (1, 2) + (1, 2) + (1, 2) =

= (1, 2) · 4 по основанию (1, 2) равен 4),

$$\mathrm{dlog}_{(1,\,2)}\,(4, 0) = 2$$

(дискретный логарифм элемента (4, 0) = (1, 2) + (1, 2) =

= (1, 2) · 2 по основанию (1, 2) равен 2),

$$\mathrm{dlog}_{(1,\,2)}\,(4, 1) = 5$$

(дискретный логарифм элемента (4, 1) = (1, 2) + (1, 2) + (1, 2) + (1, 2) + (1, 2) =

= (1, 2) · 5 по основанию (1, 2) равен 5).

Проверим теперь точку P = (1, 4) эллиптической кривой E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$ на предмет того, является ли она образующей циклической группы. В этом случае в соответствии с (2.56) получим:

$$m = 1\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([1]\text{: } P \to \underbrace{P + P + \ldots + P}_{1}) =$$

$$= ([1]\text{: } P \to P) = ([1]\text{: } (1, 4) \to (1, 4));$$

$$m = 2\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([2]\text{: } P \to \underbrace{P + P + \ldots + P}_{2}) =$$

$$= ([2]\text{: } P \to P + P) = ([2]\text{: } (1, 4) \to (1, 4) + (1, 4)) = ([2]\text{: } (1, 4) \to (4, 1));$$

$$m = 3\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([3]\text{: } P \to \underbrace{P + P + \ldots + P}_{3}) =$$

$$= ([3]\text{: } P \to P + P + P) = ([3]\text{: } (1, 4) \to (1, 4) + (1, 4) + (1, 4)) =$$

$$= ([3]\text{: } (1, 4) \to (4, 1) + (1, 4)) = ([3]\text{: } (1, 4) \to (3, 4));$$

$$m = 4\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([4]\text{: } P \to \underbrace{P + P + \ldots + P}_{4}) =$$

$$= ([4]\text{: } P \to P + P + P + P) = ([4]\text{: } (1, 4) \to (1, 4) + (1, 4) + (1, 4) + (1, 4)) =$$

$$= ([4]\text{: } (1, 4) \to (3, 4) + (1, 4)) = ([4]\text{: } (1, 4) \to (3, 2));$$

$$m = 5\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([5]\text{: } P \to \underbrace{P + P + \ldots + P}_{5}) =$$

$$= ([5]\text{: } P \to P + P + P + P + P) = ([5]\text{: } (1, 4) \to (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4)) =$$

$$= ([5]\text{: } (1, 4) \to (3, 2) + (1, 4)) = ([5]\text{: } (1, 4) \to (4, 0));$$

$$m = 6\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([6]\text{: } P \to \underbrace{P + P + \ldots + P}_{6}) =$$

$$= ([6]\text{: } P \to P + P + P + P + P + P) =$$

$$= ([6]\text{: } (1, 4) \to (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4)) =$$

$$= ([6]\text{: } (1, 4) \to (4, 0) + (1, 4)) = ([6]\text{: } (1, 4) \to (1, 2));$$

$$m = 7\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([7]\text{: } P \to \underbrace{P + P + \ldots + P}_{7}) =$$

$$= ([7]\text{: } P \to P + P + P + P + P + P + P) =$$

$$= ([7]\text{: } (1, 4) \to (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4)) =$$

$$= ([7]\text{: } (1, 4) \to (1, 2) + (1, 4)) = ([7]\text{: } (1, 4) \to O).$$

Заметим, что в результате выполнения одноместной операции (2.56) над $P = (1, 4)$ также получены все элементы (второго примера) эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_5$ при $a_1 = 0$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_6 = 3$, т.е. кривой E: $Y^2 + 4 \cdot Y = X^3 + 3 \cdot X^2 + 3$. Поэтому также можно говорить о том, что данная эллиптическая кривая представляет собой конечную циклическую группу седьмого порядка, а точка $P = (1, 4)$ является ее еще одной образующей (примитивным элементом).

Зададим аналогично (1.15) еще одну функцию дискретного логарифмирования (теперь по основанию (1, 4)) в этой циклической группе:

$$\operatorname{dlog}_{(1, 4)} O = 7$$

(дискретный логарифм элемента $O = (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) =$
$= (1, 4) \cdot 7$ по основанию (1, 4) равен 7),

$$\operatorname{dlog}_{(1, 4)} (1, 2) = 6$$

(дискретный логарифм элемента $(1, 2) = (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) =$
$= (1, 4) \cdot 6$ по основанию (1, 4) равен 6),

$$\operatorname{dlog}_{(1, 4)} (1, 4) = 1$$

(дискретный логарифм элемента $(1, 4) = (1, 4) =$
$= (1, 4) \cdot 1$ по основанию (1, 4) равен 1),

$$\operatorname{dlog}_{(1, 4)} (3, 2) = 4$$

(дискретный логарифм элемента $(3, 2) = (1, 4) + (1, 4) + (1, 4) + (1, 4) =$
$= (1, 4) \cdot 4$ по основанию (1, 4) равен 4),

$$\operatorname{dlog}_{(1, 4)} (3, 4) = 3$$

(дискретный логарифм элемента $(3, 4) = (1, 4) + (1, 4) + (1, 4) =$
$= (1, 4) \cdot 3$ по основанию (1, 4) равен 3),

$$\mathrm{dlog}_{(1,\,4)}\,(4,\,0) = 5$$

(дискретный логарифм элемента (4, 0) = (1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) =

= (1, 4) · 5 по основанию (1, 4) равен 5),

$$\mathrm{dlog}_{(1,\,4)}\,(4,\,1) = 2$$

(дискретный логарифм элемента (4, 1) = (1, 4) + (1, 4) =

= (1, 4) · 2 по основанию (1, 4) равен 2).

Рассмотрим задачу дискретного логарифмирования на (третьем) примере эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.27), т.е. кривой E: $Y^2 = X^3 + X + 3$. В соответствии с (2.56) вычислим результаты выполнения введенной одноместной операции $[m]$ над P для различных значений P из множества (2.54).

Пусть вначале $P = (4, 1)$, тогда в соответствии с (2.56) получим:

$$m = 1\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([1]\text{: } P \to \underbrace{P + P + \ldots + P}_{1}) =$$

$$= ([1]\text{: } P \to P) = ([1]\text{: } (4, 1) \to (4, 1));$$

$$m = 2\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([2]\text{: } P \to \underbrace{P + P + \ldots + P}_{2}) =$$

$$= ([2]\text{: } P \to P + P) = ([2]\text{: } (4, 1) \to (4, 1) + (4, 1)) = ([2]\text{: } (4, 1) \to (6, 6));$$

$$m = 3\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([3]\text{: } P \to \underbrace{P + P + \ldots + P}_{3}) =$$

$$= ([3]\text{: } P \to P + P + P) = ([3]\text{: } (4, 1) \to (4, 1) + (4, 1) + (4, 1)) =$$

$$= ([3]\text{: } (4, 1) \to (6, 6) + (4, 1)) = ([3]\text{: } (4, 1) \to (5, 0));$$

$$m = 4\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([4]\text{: } P \to \underbrace{P + P + \ldots + P}_{4}) =$$

$$= ([4]\text{: } P \to P + P + P + P) = ([4]\text{: } (4, 1) \to (4, 1) + (4, 1) + (4, 1) + (4, 1)) =$$

$$= ([4]\text{: } (4, 1) \to (5, 0) + (4, 1)) = ([4]\text{: } (4, 1) \to (6, 1));$$

$$m = 5\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([5]\text{: } P \to \underbrace{P + P + \ldots + P}_{5}) =$$

$$= ([5]\text{: } P \to P + P + P + P + P) = ([5]\text{: } (4, 1) \to (4, 1) + (4, 1) + (4, 1) + (4, 1) + (4, 1)) =$$

$$= ([5]\text{: } (4, 1) \to (6, 1) + (4, 1)) = ([5]\text{: } (4, 1) \to (4, 6));$$

$$m = 6\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([6]\text{: } P \to \underbrace{P + P + \ldots + P}_{6}) =$$

$$= ([6]\text{: } P \to P + P + P + P + P + P) =$$

$$= ([6]\text{: } (4, 1) \to (4, 1) + (4, 1) + (4, 1) + (4, 1) + (4, 1) + (4, 1)) =$$

$$= ([6]\text{: } (4, 1) \to (4, 6) + (4, 1)) = ([6]\text{: } (4, 1) \to O).$$

Заметим, что в результате выполнения одноместной операции (2.56) над $P = (4, 1)$ получены все элементы (третьего примера) эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$

при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, т.е. кривой E: $Y^2 = X^3 + X + 3$. Поэтому можно говорить о том, что данная эллиптическая кривая представляет собой конечную циклическую группу шестого порядка, а точка $P = (4, 1)$ является ее образующей (примитивным элементом).

Зададим аналогично (1.15) функцию дискретного логарифмирования (по основанию (4, 1)) в этой группе перечислением ее элементов:

$$\mathrm{dlog}_{(4,\,1)}\, O = 6$$

(дискретный логарифм элемента $O = (4, 1) + (4, 1) + (4, 1) + (4, 1) + (4, 1) + (4, 1) =$

$= (4, 1) \cdot 6$ по основанию (4, 1) равен 6),

$$\mathrm{dlog}_{(4,\,1)}\,(4, 1) = 1$$

(дискретный логарифм элемента $(4, 1) = (4, 1) =$

$= (4, 1) \cdot 1$ по основанию (4, 1) равен 1),

$$\mathrm{dlog}_{(4,\,1)}\,(4, 6) = 5$$

(дискретный логарифм элемента $(4, 6) = (4, 1) + (4, 1) + (4, 1) + (4, 1) + (4, 1) =$

$= (4, 1) \cdot 5$ по основанию (4, 1) равен 5),

$$\mathrm{dlog}_{(4,\,1)}\,(5, 0) = 3$$

(дискретный логарифм элемента $(5, 0) = (4, 1) + (4, 1) + (4, 1) =$

$= (4, 1) \cdot 3$ по основанию (4, 1) равен 3),

$$\mathrm{dlog}_{(4,\,1)}\,(6, 1) = 4$$

(дискретный логарифм элемента $(6, 1) = (4, 1) + (4, 1) + (4, 1) + (4, 1) =$

$= (4, 1) \cdot 4$ по основанию (4, 1) равен 4),

$$\mathrm{dlog}_{(4,\,1)}\,(6, 6) = 2$$

(дискретный логарифм элемента $(6, 6) = (4, 1) + (4, 1) =$

$= (4, 1) \cdot 2$ по основанию (4, 1) равен 2).

Проверим теперь точку $P = (4, 6)$ (третьего примера) эллиптической кривой E: $Y^2 = X^3 + X + 3$ на предмет того, является ли она образующей циклической группы. В этом случае в соответствии с (2.56) получим:

$$m = 1\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([1]\text{: } P \to \underbrace{P + P + \ldots + P}_{1}) =$$

$$= ([1]\text{: } P \to P) = ([1]\text{: } (4, 6) \to (4, 6));$$

$$m = 2\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([2]\text{: } P \to \underbrace{P + P + \ldots + P}_{2}) =$$

$$= ([2]\text{: } P \to P + P) = ([2]\text{: } (4, 6) \to (4, 6) + (4, 6)) = ([2]\text{: } (4, 6) \to (6, 1));$$

$$m = 3\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([3]\text{: } P \to \underbrace{P + P + \ldots + P}_{3}) =$$

$$= ([3]\text{: } P \to P + P + P) = ([3]\text{: } (4, 6) \to (4, 6) + (4, 6) + (4, 6)) =$$

$$= ([3]\text{: } (4, 6) \to (6, 1) + (4, 6)) = ([3]\text{: } (4, 6) \to (5, 0));$$

$$m = 4\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([4]\text{: } P \to \underbrace{P + P + \ldots + P}_{4}) =$$

$$= ([4]\text{: } P \to P + P + P + P) = ([4]\text{: } (4, 6) \to (4, 6) + (4, 6) + (4, 6) + (4, 6)) =$$

$$= ([4]\text{: } (4, 6) \to (5, 0) + (4, 6)) = ([4]\text{: } (4, 6) \to (6, 6));$$

$$m = 5\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([5]\text{: } P \to \underbrace{P + P + \ldots + P}_{5}) =$$

$$= ([5]\text{: } P \to P + P + P + P + P) = ([5]\text{: } (4, 6) \to (4, 6) + (4, 6) + (4, 6) + (4, 6) + (4, 6)) =$$

$$= ([5]\text{: } (4, 6) \to (6, 6) + (4, 6)) = ([5]\text{: } (4, 6) \to (4, 1));$$

$$m = 6\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([6]\text{: } P \to \underbrace{P + P + \ldots + P}_{6}) =$$

$$= ([6]\text{: } P \to P + P + P + P + P + P) =$$

$$= ([6]\text{: } (4, 6) \to (4, 6) + (4, 6) + (4, 6) + (4, 6) + (4, 6) + (4, 6)) =$$

$$= ([6]\text{: } (4, 6) \to (4, 1) + (4, 6)) = ([6]\text{: } (4, 6) \to O).$$

Заметим, что в результате выполнения одноместной операции (2.56) над $P = (4, 6)$ также получены все элементы (третьего примера) эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_7$ при $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 1$, $a_6 = 3$, т.е. кривой E: $Y^2 = X^3 + X + 3$. Поэтому также можно говорить о том, что данная эллиптическая кривая представляет собой конечную циклическую группу шестого порядка, а точка $P = (4, 6)$ является ее еще одной образующей (примитивным элементом).

Зададим аналогично (1.15) еще одну функцию дискретного логарифмирования (теперь по основанию (4, 6)) в этой циклической группе:

$$\mathrm{dlog}_{(4, 6)} O = 6$$

(дискретный логарифм элемента $O = (4, 6) + (4, 6) + (4, 6) + (4, 6) + (4, 6) + (4, 6) =$

$= (4, 6) \cdot 6$ по основанию (4, 6) равен 6),

$$\mathrm{dlog}_{(4, 6)} (4, 1) = 5$$

(дискретный логарифм элемента $(4, 1) = (4, 6) + (4, 6) + (4, 6) + (4, 6) + (4, 6) =$

$= (4, 6) \cdot 5$ по основанию (4, 6) равен 5),

$$\mathrm{dlog}_{(4, 6)} (4, 6) = 1$$

(дискретный логарифм элемента $(4, 6) =$

$= (4, 6) \cdot 1$ по основанию (4, 6) равен 1),

$$\mathrm{dlog}_{(4, 6)} (5, 0) = 3$$

(дискретный логарифм элемента $(5, 0) = (4, 6) + (4, 6) + (4, 6) =$

$= (4, 6) \cdot 3$ по основанию (4, 6) равен 3),

$$\mathrm{dlog}_{(4, 6)} (6, 1) = 2$$

(дискретный логарифм элемента $(6, 1) = (4, 6) + (4, 6) =$

$= (4, 6) \cdot 2$ по основанию (4, 6) равен 2),

$$\mathrm{dlog}_{(4,\,6)}\,(6,\,6) = 4$$

(дискретный логарифм элемента (6, 6) = (4, 6) + (4, 6) + (4, 6) + (4, 6) =

= (4, 6) · 4 по основанию (4, 6) равен 4).

Рассмотрим задачу дискретного логарифмирования на (четвертом) примере эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, удовлетворяющей аффинной версии уравнения Вейерштрасса (2.29), т.е. кривой E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$. В соответствии с (2.56) вычислим результаты выполнения введенной одноместной операции $[m]$ над P для различных значений P из множества (2.55).

Пусть вначале $P = (0, 3)$, тогда в соответствии с (2.56) получим:

$$m = 1\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([1]\text{: } P \to \underbrace{P + P + \ldots + P}_{1}) =$$

$$= ([1]\text{: } P \to P) = ([1]\text{: } (0, 3) \to (0, 3));$$

$$m = 2\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([2]\text{: } P \to \underbrace{P + P + \ldots + P}_{2}) =$$

$$= ([2]\text{: } P \to P + P) = ([2]\text{: } (0, 3) \to (0, 3) + (0, 3)) = ([2]\text{: } (0, 3) \to (9, 2));$$

$$m = 3\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([3]\text{: } P \to \underbrace{P + P + \ldots + P}_{3}) =$$

$$= ([3]\text{: } P \to P + P + P) = ([3]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([3]\text{: } (0, 3) \to (9, 2) + (0, 3)) = ([3]\text{: } (0, 3) \to (6, 9));$$

$$m = 4\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([4]\text{: } P \to \underbrace{P + P + \ldots + P}_{4}) =$$

$$= ([4]\text{: } P \to P + P + P + P) = ([4]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([4]\text{: } (0, 3) \to (6, 9) + (0, 3)) = ([4]\text{: } (0, 3) \to (1, 6));$$

$$m = 5\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([5]\text{: } P \to \underbrace{P + P + \ldots + P}_{5}) =$$

$$= ([5]\text{: } P \to P + P + P + P + P) = ([5]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([5]\text{: } (0, 3) \to (1, 6) + (0, 3)) = ([5]\text{: } (0, 3) \to (1, 4));$$

$$m = 6\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([6]\text{: } P \to \underbrace{P + P + \ldots + P}_{6}) =$$

$$= ([6]\text{: } P \to P + P + P + P + P + P) =$$

$$= ([6]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([6]\text{: } (0, 3) \to (1, 4) + (0, 3)) = ([6]\text{: } (0, 3) \to (6, 6));$$

$$m = 7\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([7]\text{: } P \to \underbrace{P + P + \ldots + P}_{7}) =$$

$$= ([7]\text{: } P \to P + P + P + P + P + P + P) =$$

$$= ([7]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([7]\text{: } (0, 3) \to (6, 6) + (0, 3)) = ([7]\text{: } (0, 3) \to (9, 5));$$

$$m = 8\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([8]\text{: } P \to \underbrace{P + P + \ldots + P}_{8}) =$$

$$= ([8]\text{: } P \to P + P + P + P + P + P + P + P) =$$

$$= ([8]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([8]\text{: } (0, 3) \to (9, 5) + (0, 3)) = ([8]\text{: } (0, 3) \to (0, 6));$$

$$m = 9\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([9]\text{: } P \to \underbrace{P + P + \ldots + P}_{9}) =$$

$$= ([9]\text{: } P \to P + P + P + P + P + P + P + P + P) =$$

$$= ([9]\text{: } (0, 3) \to (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3) + (0, 3)) =$$

$$= ([9]\text{: } (0, 3) \to (0, 6) + (0, 3)) = ([9]\text{: } (0, 3) \to O);$$

$$m = 10\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([10]\text{: } P \to \underbrace{P + P + \ldots + P}_{10}) =$$

$$= ([10]\text{: } P \to P + P + P + P + P + P + P + P + P + P) =$$

$$= ([10]\text{: } (0, 3) \to 9 \cdot (0, 3) + (0, 3)) =$$

$$= ([10]\text{: } (0, 3) \to O + (0, 3)) = ([10]\text{: } (0, 3) \to (0, 3)).$$

Заметим, что результат выполнения операции $[m] = [10]$ над элементом (0, 3) повторил результат выполнения операции $[m] = [1]$ над этим же элементом. Из этого следует, что в результате выполнения одноместной операции (2.56) над $P = (0, 3)$ не могут быть получены все элементы (четвертого примера) эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, т.е. кривой E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$, и точка $P = (0, 3)$ не является ее образующей (примитивным элементом).

По аналогичным рассуждениям не являются образующими (примитивными элементами) эллиптической кривой E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$ и точки (0, 6), (1, 4) и (1, 6) этой кривой.

Проверим теперь точку $P = (3, 4)$ (четвертого примера) эллиптической кривой E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$ на предмет того, является ли она образующей циклической группы. В этом случае в соответствии с (2.56) получим:

$$m = 1\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([1]\text{: } P \to \underbrace{P + P + \ldots + P}_{1}) =$$

$$= ([1]\text{: } P \to P) = ([1]\text{: } (3, 4) \to (3, 4));$$

$$m = 2\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([2]\text{: } P \to \underbrace{P + P + \ldots + P}_{2}) =$$

$$= ([2]\text{: } P \to P + P) = ([2]\text{: } (3, 4) \to (3, 4) + (3, 4)) = ([2]\text{: } (3, 4) \to (1, 6));$$

$$m = 3\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([3]\text{: } P \to \underbrace{P + P + \ldots + P}_{3}) =$$

$$= ([3]\text{: } P \to P + P + P) = ([3]\text{: } (3, 4) \to (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([3]: (3, 4) \to (1, 6) + (3, 4)) = ([3]: (3, 4) \to (5, 1));$$

$$m = 4: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([4]: P \to \underbrace{P + P + \ldots + P}_{4}) =$$

$$= ([4]: P \to P + P + P + P) = ([4]: (3, 4) \to (3, 4) + (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([4]: (3, 4) \to (5, 1) + (3, 4)) = ([4]: (3, 4) \to (0, 6));$$

$$m = 5: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([5]: P \to \underbrace{P + P + \ldots + P}_{5}) =$$

$$= ([5]: P \to P + P + P + P + P) = ([5]: (3, 4) \to (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([5]: (3, 4) \to (0, 6) + (3, 4)) = ([5]: (3, 4) \to (10, 5));$$

$$m = 6: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([6]: P \to \underbrace{P + P + \ldots + P}_{6}) =$$

$$= ([6]: P \to P + P + P + P + P + P) =$$

$$= ([6]: (3, 4) \to (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([6]: (3, 4) \to (10, 5) + (3, 4)) = ([6]: (3, 4) \to (6, 9));$$

$$m = 7: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([7]: P \to \underbrace{P + P + \ldots + P}_{7}) =$$

$$= ([7]: P \to P + P + P + P + P + P + P) =$$

$$= ([7]: (3, 4) \to (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([7]: (3, 4) \to (6, 9) + (3, 4)) = ([7]: (3, 4) \to (4, 0));$$

$$m = 8: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([8]: P \to \underbrace{P + P + \ldots + P}_{8}) =$$

$$= ([8]: P \to P + P + P + P + P + P + P + P) =$$

$$= ([8]: (3, 4) \to (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([8]: (3, 4) \to (4, 0) + (3, 4)) = ([8]: (3, 4) \to (9, 5));$$

$$m = 9: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([9]: P \to \underbrace{P + P + \ldots + P}_{9}) =$$

$$= ([9]: P \to P + P + P + P + P + P + P + P + P) =$$

$$= ([9]: (3, 4) \to (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4)) =$$

$$= ([9]: (3, 4) \to (9, 5) + (3, 4)) = ([9]: (3, 4) \to (8, 3));$$

$$m = 10: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([10]: P \to \underbrace{P + P + \ldots + P}_{10}) =$$

$$= ([10]: P \to P + P + P + P + P + P + P + P + P + P) =$$

$$= ([10]: (3, 4) \to 9 \cdot (3, 4) + (3, 4)) =$$

$$= ([10]: (3, 4) \to (8, 3) + (3, 4)) = ([10]: (3, 4) \to (9, 2));$$

$$m = 11: ([m]: P \to \underbrace{P + P + \ldots + P}_{m}) = ([11]: P \to \underbrace{P + P + \ldots + P}_{11}) =$$

$$= ([11]: P \to P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([11]: (3, 4) \to 10 \cdot (3, 4) + (3, 4)) =$$

$$= ([11]: (3, 4) \to (9, 2) + (3, 4)) = ([11]: (3, 4) \to (4, 2));$$

$$m = 12\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([12]\text{: } P \to \underbrace{P + P + \ldots + P}_{12}) =$$

$$= ([12]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([12]\text{: } (3, 4) \to 11 \cdot (3, 4) + (3, 4)) =$$

$$= ([12]\text{: } (3, 4) \to (4, 2) + (3, 4)) = ([12]\text{: } (3, 4) \to (6, 6));$$

$$m = 13\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([13]\text{: } P \to \underbrace{P + P + \ldots + P}_{13}) =$$

$$= ([13]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([13]\text{: } (3, 4) \to 12 \cdot (3, 4) + (3, 4)) =$$

$$= ([13]\text{: } (3, 4) \to (6, 6) + (3, 4)) = ([13]\text{: } (3, 4) \to (10, 3));$$

$$m = 14\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([14]\text{: } P \to \underbrace{P + P + \ldots + P}_{14}) =$$

$$= ([14]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([14]\text{: } (3, 4) \to 13 \cdot (3, 4) + (3, 4)) =$$

$$= ([14]\text{: } (3, 4) \to (10, 3) + (3, 4)) = ([14]\text{: } (3, 4) \to (0, 3));$$

$$m = 15\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([15]\text{: } P \to \underbrace{P + P + \ldots + P}_{15}) =$$

$$= ([15]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([15]\text{: } (3, 4) \to 14 \cdot (3, 4) + (3, 4)) =$$

$$= ([15]\text{: } (3, 4) \to (0, 3) + (3, 4)) = ([15]\text{: } (3, 4) \to (5, 2));$$

$$m = 16\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([16]\text{: } P \to \underbrace{P + P + \ldots + P}_{16}) =$$

$$= ([16]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([16]\text{: } (3, 4) \to 15 \cdot (3, 4) + (3, 4)) =$$

$$= ([16]\text{: } (3, 4) \to (5, 2) + (3, 4)) = ([16]\text{: } (3, 4) \to (1, 4));$$

$$m = 17\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([17]\text{: } P \to \underbrace{P + P + \ldots + P}_{17}) =$$

$$= ([17]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([17]\text{: } (3, 4) \to 16 \cdot (3, 4) + (3, 4)) =$$

$$= ([17]\text{: } (3, 4) \to (1, 4) + (3, 4)) = ([17]\text{: } (3, 4) \to (3, 8));$$

$$m = 18\text{: } ([m]\text{: } P \to \underbrace{P + P + \ldots + P}_{m}) = ([18]\text{: } P \to \underbrace{P + P + \ldots + P}_{18}) =$$

$$= ([18]\text{: } P \to P + P + P + P + P + P + P + P + P + P + P + P + P + P + P + P + P) =$$

$$= ([18]\text{: } (3, 4) \to 17 \cdot (3, 4) + (3, 4)) =$$

$$= ([18]\text{: } (3, 4) \to (3, 8) + (3, 4)) = ([18]\text{: } (3, 4) \to O).$$

Заметим, что в результате выполнения одноместной операции (2.56) над $P = (3, 4)$ получены все элементы (четвертого примера) эллиптической кривой E над полем $K = \mathbf{F}_p = \mathbf{F}_{11}$ при $a_1 = 10$, $a_2 = 4$, $a_3 = 2$, $a_4 = 0$, $a_6 = 4$, т.е. кривой E: $Y^2 + 10 \cdot XY + 2 \cdot Y = X^3 + 4 \cdot X^2 + 4$. Поэтому можно говорить о том, что данная эллиптическая кривая

представляет собой конечную циклическую группу порядка 18, а точка $P = (3, 4)$ является ее образующей (примитивным элементом).

Зададим аналогично (1.15) функцию дискретного логарифмирования (по основанию (3, 4)) в этой группе перечислением ее элементов:

$$\mathrm{dlog}_{(3,\,4)}\, O = 18$$

(дискретный логарифм элемента $O = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +$
$+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 18$ по основанию (3, 4) равен 18),

$$\mathrm{dlog}_{(3,\,4)}\, (0, 3) = 14$$

(дискретный логарифм элемента $(0, 3) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +$
$+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 14$ по основанию (3, 4) равен 14),

$$\mathrm{dlog}_{(3,\,4)}\, (0, 6) = 4$$

(дискретный логарифм элемента $(0, 6) = (3, 4) + (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 4$ по основанию (3, 4) равен 4),

$$\mathrm{dlog}_{(3,\,4)}\, (1, 4) = 16$$

(дискретный логарифм элемента $(1, 4) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +$
$+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 16$ по основанию (3, 4) равен 16),

$$\mathrm{dlog}_{(3,\,4)}\, (1, 6) = 2$$

(дискретный логарифм элемента $(1, 6) = (3, 4) + (3, 4) =$
$= (3, 4) \cdot 2$ по основанию (3, 4) равен 2),

$$\mathrm{dlog}_{(3,\,4)}\, (3, 4) = 1$$

(дискретный логарифм элемента $(3, 4) = (3, 4) =$
$= (3, 4) \cdot 1$ по основанию (3, 4) равен 1),

$$\mathrm{dlog}_{(3,\,4)}\, (3, 8) = 17$$

(дискретный логарифм элемента $(1, 4) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +$
$+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 17$ по основанию (3, 4) равен 17),

$$\mathrm{dlog}_{(3,\,4)}\, (4, 0) = 7$$

(дискретный логарифм элемента $(4, 0) = (3, 4) + (3, 4) + (3, 4) + (3, 4) +$
$+ (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 7$ по основанию (3, 4) равен 7),

$$\mathrm{dlog}_{(3,\,4)}\, (4, 2) = 11$$

(дискретный логарифм элемента $(4, 2) = (3, 4) + (3, 4) + (3, 4) + (3, 4) +$
$+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =$
$= (3, 4) \cdot 11$ по основанию (3, 4) равен 11),

$\mathrm{dlog}_{(3,\,4)}(5,\,1) = 3$

(дискретный логарифм элемента (5, 1) = (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 3 по основанию (3, 4) равен 3),

$\mathrm{dlog}_{(3,\,4)}(5,\,2) = 15$

(дискретный логарифм элемента (5, 2) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +

+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 15 по основанию (3, 4) равен 15),

$\mathrm{dlog}_{(3,\,4)}(6,\,6) = 12$

(дискретный логарифм элемента (6, 6) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +

+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 12 по основанию (3, 4) равен 12),

$\mathrm{dlog}_{(3,\,4)}(6,\,9) = 6$

(дискретный логарифм элемента (6, 9) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 6 по основанию (3, 4) равен 6),

$\mathrm{dlog}_{(3,\,4)}(8,\,3) = 9$

(дискретный логарифм элемента (8, 3) = (3, 4) + (3, 4) + (3, 4) +

+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 9 по основанию (3, 4) равен 9),

$\mathrm{dlog}_{(3,\,4)}(9,\,2) = 10$

(дискретный логарифм элемента (9, 2) = (3, 4) + (3, 4) + (3, 4) +

+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 10 по основанию (3, 4) равен 10),

$\mathrm{dlog}_{(3,\,4)}(9,\,5) = 8$

(дискретный логарифм элемента (9, 5) = (3, 4) + (3, 4) +

+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 8 по основанию (3, 4) равен 8),

$\mathrm{dlog}_{(3,\,4)}(10,\,3) = 13$

(дискретный логарифм элемента (10, 3) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) +

+ (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 13 по основанию (3, 4) равен 13),

$\mathrm{dlog}_{(3,\,4)}(10,\,5) = 5$

(дискретный логарифм элемента (10, 5) = (3, 4) + (3, 4) + (3, 4) + (3, 4) + (3, 4) =

= (3, 4) · 5 по основанию (3, 4) равен 5).

Заметим, что отображение (2.56) является основой криптографических систем, опирающихся на эллиптическую кривую, поскольку значение $[m]\,P = (x', y')$ для известной точки $P = (x, y)$ вычислить легко, а значение (дискретного логарифма по сложению) m по известным $[m]\,P = (x', y')$ и $P = (x, y)$, как мы убедились, найти очень трудно.

ЗАКЛЮЧЕНИЕ

Третья часть учебного пособия посвящена изучению вопросов, связанных с введением в эллиптические кривые и групповому закону, которому удовлетворяют эллиптические кривые.

Через весь учебный материал третьей части пособия проходят четыре примера эллиптических кривых, для которых представлены: проективные плоскости, проективные точки проективных плоскостей, проективные и аффинные формы Вейерштрасса, переходы от проективных форм в аффинные и обратно, модифицированные формы проективных плоскостей, дискриминанты и инварианты эллиптических кривых, изоморфные и неизоморфные эллиптические кривые, метод хорд и касательных для выполнения сложения точек эллиптических кривых, алгоритм и таблицы сложения точек, а также функции дискретного логарифмирования в циклических группах, образованных их примитивными элементами.

Надеемся, что изучение подробных примеров практически к каждому даваемому определению, понятию и алгоритму позволит студентам досконально разобраться с учебным материалом пособия и подготовиться к применению полученных знаний в профессиональной деятельности при решении различных прикладных задач.

Авторы планируют подготовку и четвертой части данного пособия, посвященной также эллиптическим кривым.

СПИСОК ЛИТЕРАТУРЫ

1. **Алгоритмические основы** эллиптической криптографии / А. А. Болотов и др. – М. : МЭИ, 2000. – 100 с.

2. **Василенко, О. Н.** Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

3. **Введение** в криптографию / под общ. ред. Ященко. – 4-е изд., доп. – М. : МЦМНО, 2012. – 348 с.

4. **Глухов, М. М.** Алгебра : учебник : в 2-х т. / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М. : Гелиос АРВ, 2003. – Т. I. – 336 с.

5. **Глухов, М. М.** Алгебра : учебник : в 2-х т. / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М. : Гелиос АРВ, 2003. – 416 с.

6. **Запечников, С. В.** Криптографические методы защиты информации / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – М. : Юрайт, 2019. – 309 с.

7. **Коблиц, Н.** Курс теории чисел и криптографии / Н. Коблиц ; пер. с англ. – М. : Научное изд-во ТВП, 2001. – 254 с.

8. **Коробейников, А. Г.** Математические основы криптологии : учебное пособие / А. Г. Коробейников, Ю. А. Гатчин. – СПб. : СПб ГУ ИТМО, 2004. – 106 с.

9. **Нечаев, В. И.** Элементы криптографии (Основы теории защиты информации) : учебное пособие для ун-тов и пед. вузов / В. И. Нечаев ; под ред. В. А. Садовничего. – М. : Высшая школа, 1999. – 109 с.

10. **Новиков, В. Е.** Введение в криптологию : учебное пособие / В. Е. Новиков, В. В. Ридель. – Саратов : Изд-во Сарат. ун-та, 2000. – 101 с.

11. **Основы** криптографии : учебное пособие / А. П. Алферов и др. – М. : Гелиос АРВ, 2001. – 480 с.

12. **Романьков, В. А.** Введение в криптографию. Курс лекций / В. А. Романьков. – М. : ФОРУМ, 2012. – 240 с.

13. **Ростовцев, А. Г.** Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. – СПб. : НПО «ПРОФЕССИОНАЛ», 2004. – 485 с.

14. **Секей, Г.** Парадоксы в теории вероятностей и математической статистике / Г. Секей ; пер. с англ. – М. : Мир, 1990. – 240 с.

15. **Смарт, Н.** Криптография / Н. Смарт ; пер. с англ. – М. : Техносфера, 2005. – 528 с.

16. **Тилборг, ванн Х. К. А.** Основы криптологии. Профессиональное руководство и интерактивный учебник / Тилборг, ванн Х. К. А. – М. : Мир, 2006. – 471 с.

17. **Харин, Ю. С.** Математические основы криптологии : учебное пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. – Мн. : БГУ, 1999. – 319 с.

18. **Черемушкин, А. В.** Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. – М. : МЦНМО, 2002. – 104 с.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3
2. ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ 5
2.1. Введение в эллиптические кривые 5
2.1.1. Проективная плоскость 5
2.1.2. Проективная точка проективной плоскости 11
2.1.3. Эллиптическая кривая (в проективных координатах) 22
2.1.4. Эллиптическая кривая (в аффинных координатах) 29
2.2. Групповой закон 63
2.2.1. Изоморфная эллиптическая кривая 63
2.2.2. Групповой закон по методу хорд и касательных 66
2.2.3. Реализация сложения точек эллиптической кривой 68
2.2.4. Дискретное логарифмирование на эллиптической кривой 79
ЗАКЛЮЧЕНИЕ 92
СПИСОК ЛИТЕРАТУРЫ 93

Учебное электронное издание

КУЛАКОВ Юрий Владимирович

ВВЕДЕНИЕ В КРИПТОЛОГИЮ

Учебное пособие

В четырех частях

Часть 3

Редактирование И. В. Калистратовой
Графический и мультимедийный дизайнер Т. Ю. Зотова
Обложка, упаковка, тиражирование И. В. Калистратовой

ISBN 978-5-8265-2923-2

Подписано к использованию 16.06.2025.
Тираж 50 шт. Заказ № 83

Издательский центр ФГБОУ ВО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14
Телефон 8(4752) 63-81-08
E-mail: izdatelstvo@tstu.ru