УДК 512.552+519.713

©2011. **В.В. Скобелев**

АНАЛИЗ КРИВЫХ 2-ГО ПОРЯДКА НАД КОНЕЧНЫМ КОЛЬЦОМ

Исследованы кривые линии 2-го порядка над конечным ассоциативно-коммутативным кольцом с единицей. Установлен ряд характеристик структуры множества точек анализируемых кривых, определяемых в терминах факторизации полинома. Охарактеризовано множество особых точек анализируемых кривых. Исследованы методы приведения анализируемых кривых к канонической форме.

Ключевые слова: *ассоциативно-коммутативные кольца, линии 2-го порядка, особые точки, факторизация полинома, канонические формы.*

1. Введение. Для современного этапа развития криптографии характерен систематический переход от «чисто» комбинаторных моделей к комбинаторно-алгебраическим моделям [1, 2]. Достижения асимметричной криптографии основаны на теоретико-числовых алгоритмах [3], а также на использовании эллиптических кривых над конечными полями [4]. Кроме того, при построении практически всех кандидатов на современные поточные шифры фрагментарно используются вычисления в кольцах вычетов. Все эти обстоятельства указывают на актуальность исследования кривых линий над конечными кольцами как с позиции алгебры, так и с позиции их возможного использования при решении задач криптографии. Сложность этой задачи обусловлена тем, что наиболее значимые результаты алгебраической геометрии получены для алгебраически замкнутого поля [5, 6], которое, как известно, является бесконечным.

В настоящей работе исследуются кривые линии 2-го порядка над конечным ассоциативно-коммутативным кольцом $\mathcal{K} = (K, +, \cdot)$ с единицей.

Если полугруппа $(K\backslash\{0\}, \cdot)$ является гауссовой [7], то исследование кривой линии 2-го порядка может быть осуществлено за счет перехода к полю дробей $\overline{\mathcal{K}}$ и применения обычных методов алгебраической геометрии. Все сложности возникают, если полугруппа $(K\backslash\{0\}, \cdot)$ не является гауссовой. Особенно эти сложности проявляются при наличии в кольце делителей нуля.

Структура настоящей работы следующая. В п.2 представлена исследуемая модель. В п.3 множество точек исследуемых кривых линий представлено в терминах множеств решений семейств систем линейных уравнений. В п.4 анализируется множество особых точек исследуемых кривых линий. В п.5. охарактеризованы множества точек исследуемых кривых линий, принадлежащих нетривиальным подклассам. В п.6 исследуются методы приведения анализируемых кривых к канонической форме.

2. Исследуемая модель. Общее уравнение кривой линии 2-го порядка Γ над кольцом $\mathcal{K}$ имеет вид

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0, \qquad (1)$$

где $a_{11}, a_{12}, a_{22}, a_1, a_2, a_0 \in K$, причем $(a_{11}, a_{12}, a_{22}) \neq (0, 0, 0)$.

Для многочлена $f(x, y) = a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0$ возможны следующие три ситуации.

Ситуация 1. Многочлен $f(x, y)$ неразложим над кольцом $\mathcal{K}$.

Ситуация 2. Для любых таких многочленов $f_i \in \mathcal{K}[x, y]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, что $f(x, y) = f_1(x, y)f_2(x, y)$, истинно неравенство $m_1 + m_2 > 2$.

Ситуация 3. Существуют многочлены $f_i \in \mathcal{K}[x, y]$ $(i = 1, 2)$ степени $m_i = 1$ $(i = 1, 2)$, удовлетворяющие равенству $f(x, y) = f_1(x, y)f_2(x, y)$.

Если имеет место ситуация 2, то $f(x, y)$ – многочлен наименьшей степени, определяющий кривую Γ. Поэтому, в этой ситуации анализ кривой Γ осуществляется непосредственно на основе уравнения (1). Если имеет место ситуация 3, то при известном разложении многочлена $f(x, y)$ уравнение (1) естественно представить в виде

$$(b_1x + b_2y + b_0)(c_1x + c_2y + c_0) = 0. \tag{2}$$

3. Множество точек исследуемых кривых линий. Множество точек кривой Γ, определенной уравнением (2), может быть представлено в виде

$$\Gamma = S_1 \cup S_2 \cup S_3,$$

где S_1 – объединение множеств решений семейства F_α $(\alpha \in K)$ систем линейных уравнений

$$F_\alpha : \begin{cases} b_1x + b_2y + b_0 = 0 \\ c_1x + c_2y + c_0 = \alpha, \end{cases}$$

S_2 – объединение множеств решений семейства G_β $(\beta \in K\backslash\{0\})$ систем линейных уравнений

$$G_\beta : \begin{cases} b_1x + b_2y + b_0 = \beta \\ c_1x + c_2y + c_0 = 0, \end{cases}$$

а S_3 – объединение множеств решений семейства $H_{\alpha,\beta}$ $(\alpha, \beta \in K\backslash\{0\}, \alpha\beta = 0)$ систем линейных уравнений

$$H_{\alpha,\beta} : \begin{cases} b_1x + b_2y + b_0 = \alpha \\ c_1x + c_2y + c_0 = \beta. \end{cases}$$

Таким образом, в случае конечного кольца построение в явном виде множества точек коники Γ в ситуациях 1 и 2 эквивалентно поиску множества решений нелинейного уравнения (1) от двух переменных, а в ситуации 3 – поиску множеств решений трех семейств F_α $(\alpha \in K)$, G_β $(\beta \in K\backslash\{0\})$ и $H_{\alpha,\beta}$ $(\alpha, \beta \in K\backslash\{0\}, \alpha\beta = 0)$ систем линейных уравнений. Отметим, что если кольцо $\mathcal{K}$ не содержит делителей нуля, то $H_{\alpha,\beta} = \emptyset$.

4. Особые точки исследуемых кривых линий. Из определения особой точки кривой вытекает, что множеством особых точек кривой (1) является множество

решений системы уравнений:

$$\begin{cases} \mathsf{D}_x(a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0) = 0 \\ \mathsf{D}_y(a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0) = 0 \\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 2a_{11}x + a_{12}y + a_1 = 0 \\ a_{12}x + 2a_{22}y + a_2 = 0 \\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0. \end{cases}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 1. Кривая Γ, определяемая уравнением (1), имеет особые точки тогда и только тогда, когда существует такое решение (x_0, y_0) системы линейных уравнений

$$\begin{cases} 2a_{11}x + a_{12}y = -a_1 \\ a_{12}x + 2a_{22}y = -a_2, \end{cases} \tag{3}$$

что истинно равенство

$$a_{11}x_0^2 + a_{12}x_0y_0 + a_{22}y_0^2 + a_1x_0 + a_2y_0 + a_0 = 0.$$

Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда система уравнений (3) принимает вид

$$\begin{cases} a_{12}y = -a_1 \\ a_{12}x = -a_2. \end{cases}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2. Если характеристика кольца $\mathcal{K}$ равна 2, то кривая Γ, определяемая уравнением (1):

1) имеет единственную особую точку, если $a_{12} \in K^{inv}$ и

$$a_{11}a_2^2 - a_{12}a_1a_2 + a_{22}a_1^2 + a_0a_{12}^2 = 0;$$

2) является гладкой кривой, если либо $a_{12} \in K^{inv}$ и

$$a_{11}a_2^2 - a_{12}a_1a_2 + a_{22}a_1^2 + a_0a_{12}^2 \neq 0,$$

либо $a_{12} \notin K^{inv}$ и, кроме того, $a_1 \in K^{inv}$ или $a_2 \in K^{inv}$.

5. Характеристика множеств точек исследуемых кривых. Рассмотрим следующие специальные случаи уравнения (1), определяющего кривую Γ.

1. Пусть

$$\begin{cases} a_{3-i,3-i} \neq 0 \\ a_{ii} = a_{12} = a_i = 0, \end{cases} \tag{4}$$

где либо $i = 1$, либо $i = 2$.

Если (4) истинно при $i = 1$, то уравнение (1) принимает вид

$$a_{22}y^2 + a_2y + a_0 = 0, \tag{5}$$

а если при $i = 2$, то – вид

$$a_{11}x^2 + a_1x + a_0 = 0. \tag{6}$$

Следовательно, кривая Γ состоит из всех таких точек $(x_0, y_0) \in K^2$, что y_0 (соответственно, x_0) – корень уравнения (5) (соответственно, уравнения (6)) над кольцом $\mathcal{K}$, если (4) истинно при $i = 1$ (соответственно, при $i = 2$). В частности, если уравнение (5) (соответственно, уравнение (6)) не имеет решений над кольцом $\mathcal{K}$, то $\Gamma = \emptyset$.

2. Пусть

$$\begin{cases} a_{3-i,3-i} \neq 0 \\ a_{ii} = a_{12} = 0 \\ a_i \neq 0, \end{cases} \tag{7}$$

где либо $i = 1$, либо $i = 2$.

Если (7) истинно при $i = 1$, то имеет место следующая теорема.

Теорема 1. *Если характеристика кольца $\mathcal{K}$ отлична от 2, $a_{22} \neq 0$, $a_{11} = a_{12} = 0$, $a_1 \neq 0$, и существуют такие элементы $b, c \in K\backslash\{0\}$, что*

$$\begin{cases} a_{22} = cb^2 \\ a_2 = 2cb, \end{cases} \tag{8}$$

то кривая Γ, определяемая уравнением (1), состоит из таких точек $(x_0, y_0) \in K^2$, что $(w_0, u_0) = (by_0 + 1, x_0)$ является корнем уравнения

$$cw^2 + a_1u + (a_0 - c) = 0 \tag{9}$$

над кольцом $\mathcal{K}$.

Доказательство. Пусть характеристика кольца $\mathcal{K}$ отлична от 2.

Если $a_{22} \neq 0$, $a_{11} = a_{12} = 0$ и $a_1 \neq 0$, то уравнение (1) принимает вид

$$a_{22}y^2 + a_1x + a_2y + a_0 = 0. \tag{10}$$

Подставив (8) в (10), получим уравнение

$$c(by + 1)^2 + a_1x + (a_0 - c) = 0. \tag{11}$$

Положив $w = by + 1$ и $u = x$ в (11), получим уравнение (9).

Следовательно, $(x_0, y_0) \in \Gamma$ тогда и только тогда, когда $(w_0, u_0) = (by_0 + 1, x_0)$ является корнем уравнения (9) над кольцом $\mathcal{K}$.

□

Если (7) истинно при $i = 2$, то имеет место следующая теорема.

Теорема 2. *Если характеристика кольца $\mathcal{K}$ отлична от 2, $a_{11} \neq 0$, $a_{22} = a_{12} = 0$, $a_2 \neq 0$, и существуют такие элементы $b, c \in K\backslash\{0\}$, что $a_{11} = cb^2$ и $a_1 = 2cb$, то кривая Γ, определяемая уравнением (1), состоит из таких точек $(x_0, y_0) \in K^2$, что $(w_0, u_0) = (bx_0 + 1, y_0)$ является корнем уравнения*

$$cw^2 + a_1 u + (a_0 - c) = 0$$

над кольцом $\mathcal{K}$.

Доказательство теоремы 2 аналогично доказательству теоремы 1.

3. Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Имеет место следующая теорема.

Теорема 3. *Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Тогда:*

1) если $a_1 = a_2 = 0$, то кривая Γ, определяемая уравнением (1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения

$$a_{12}xy + a_0 = 0 \tag{12}$$

над кольцом $\mathcal{K}$;

2) если $a_2 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_2 = ca_{12}$, то кривая Γ, определяемая уравнением (1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}y_0 + a_1, x_0 + c)$ является корнем уравнения

$$uv + (a_0 - ca_1) = 0 \tag{13}$$

над кольцом $\mathcal{K}$;

3) если $a_1 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_1 = ca_{12}$, то кривая Γ, определяемая уравнением (1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}x_0 + a_2, y_0 + c)$ является корнем уравнения

$$uv + (a_0 - ca_2) = 0 \tag{14}$$

над кольцом $\mathcal{K}$.

Доказательство. Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Тогда уравнение (1) принимает вид

$$a_{12}xy + a_1 x + a_2 y + a_0 = 0. \tag{15}$$

Если $a_1 = a_2 = 0$, то уравнение (15) совпадает с уравнением (12). Отсюда вытекает, что кривая Γ состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (12) над кольцом $\mathcal{K}$, что и требовалось показать.

Пусть $a_2 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_2 = ca_{12}$. Тогда

$$a_{12}xy + a_1 x + a_2 y + a_0 = x(a_{12}y + a_1) + ca_{12}y + a_0 =$$

$$= x(a_{12}y + a_1) + c(a_{12}y + a_1) + (a_0 - ca_1) =$$

$$= (a_{12}y + a_1)(x + c) + (a_0 - ca_1).$$

Следовательно, уравнение (15) принимает вид

$$(a_{12}y + a_1)(x + c) + (a_0 - ca_1) = 0. \tag{16}$$

Положив $u = a_{12}y + a_1$ и $v = x + c$ в (16), получим уравнение (13).

Отсюда вытекает, что кривая Γ, определяемая уравнением (1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}y_0+a_1, x_0+c)$ является корнем уравнения (13) над кольцом $\mathcal{K}$, что и требовалось показать.

Пусть $a_1 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_1 = ca_{12}$. Тогда

$$a_{12}xy + a_1x + a_2y + a_0 = y(a_{12}x + a_2) + ca_{12}x + a_0 =$$

$$= y(a_{12}x + a_2) + c(a_{12}x + a_2) + (a_0 - ca_2) =$$

$$= (a_{12}x + a_2)(y + c) + (a_0 - ca_2).$$

Следовательно, уравнение (15) принимает вид

$$(a_{12}x + a_2)(y + c) + (a_0 - ca_2) = 0. \tag{17}$$

Положив $u = a_{12}x + a_2$ и $v = y + c$ в (17), получим уравнение (14).

Отсюда вытекает, что кривая Γ, определяемая уравнением (1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $(u_0, v_0) = (a_{12}x_0+a_2, y_0+c)$ является корнем уравнения (14) над кольцом $\mathcal{K}$, что и требовалось показать.

□

4. Пусть

$$\begin{cases} a_{ii} \neq 0 \ \ (i = 1, 2) \\ a_j \neq 0 \ \ (j = 1, 2). \end{cases}$$

Имеет место следующая теорема.

Теорема 4. *Если характеристика кольца $\mathcal{K}$ отлична от 2, $a_{ii} \neq 0$ $(i = 1, 2)$, $a_j \neq 0$ $(j = 1, 2)$ и существуют такие элементы $b_1, b_2, c, d \in K\backslash\{0\}$, что*

$$\begin{cases} a_{11} = cb_1^2 \\ a_{12} = 2cb_1b_2 \\ a_{22} = cb_2^2 \\ a_1 = db_1 \\ a_2 = db_2, \end{cases} \tag{18}$$

то кривая Γ, определяемая уравнением (1), состоит из таких точек $(x_0, y_0) \in K^2$, что $w_0 = b_1x_0 + b_2y_0$ является корнем уравнения

$$cw^2 + dw + a_0 = 0 \tag{19}$$

над кольцом $\mathcal{K}$.

Доказательство. Предположим, что характеристика кольца $\mathcal{K}$ отлична от 2, $a_{ii} \neq 0$ $(i = 1, 2)$ и $a_j \neq 0$ $(j = 1, 2)$.

Подставив (18) в (1), получим

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow cb_1^2x^2 + 2cb_1b_2xy + cb_2^2y^2 + db_1x + db_2y + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow c(b_1^2x^2 + 2b_1b_2xy + b_2^2y^2) + d(b_1x + b_2y) + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow c(b_1x + b_2y)^2 + d(b_1x + b_2y) + a_0 = 0. \tag{20}$$

Положив $w = b_1x + b_2y$ в (20), получим уравнение (19).

Отсюда вытекает, что кривая Γ, определяемая уравнением (1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что $w_0 = b_1x_0 + b_2y_0$ является корнем уравнения (19) над кольцом $\mathcal{K}$.

□

5. Пусть

$$\begin{cases} a_{ii} \neq 0 \\ a_{3-i,3-i} = 0 \\ a_{12} \neq 0, \end{cases} \tag{21}$$

где либо $i = 1$, либо $i = 2$.

Если (21) истинно при $i = 1$, то уравнение (1) принимает вид

$$x(a_{11}x + a_{12}y) + a_1x + a_2y + a_0 = 0, \tag{22}$$

а если при $i = 2$, то – вид

$$y(a_{22}y + a_{12}x) + a_1x + a_2y + a_0 = 0. \tag{23}$$

Следовательно, кривая Γ состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (22) (соответственно, уравнения (23)) над кольцом $\mathcal{K}$, если (21) истинно при $i = 1$ (соответственно, при $i = 2$). В частности, если уравнение (22) (соответственно, уравнение (23)) не имеет решений над кольцом $\mathcal{K}$, то $\Gamma = \emptyset$.

6. Пусть $a_{ii} \neq 0$ $(i = 1, 2)$ и либо $a_1 = 0$, либо $a_2 = 0$.

Если $a_1 = 0$, то уравнение (1) принимает вид

$$x(a_{11}x + a_{12}y) + a_{22}y^2 + a_2y + a_0 = 0,$$

а если $a_2 = 0$, то – вид

$$y(a_{22}y + a_{12}x) + a_{11}x^2 + a_1x + a_0 = 0.$$

Отсюда вытекает, что если характеристика кольца $\mathcal{K}$ отлична от 2 и существуют такие элементы $b, c, d \in K$, что $a_{22} = db^2$, $a_2 = 2dbc$ и $a_0 = dc^2$, соответственно, $a_{11} = db^2$, $a_1 = 2dbc$ и $a_0 = dc^2$, то при $a_1 = 0$ уравнение (1) принимает вид

$$x(a_{11}x + a_{12}y) + d(by + c)^2 = 0,$$

а при $a_2 = 0$ – вид

$$y(a_{22}y + a_{12}x) + d(bx + c)^2 = 0.$$

6. Канонический вид исследуемых кривых линий. Рассмотрим линейное преобразование

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}, \tag{24}$$

где

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}. \tag{25}$$

Подставив (25) в (24) и выполнив действия, получим

$$\begin{cases} x = \alpha_{11}u + \alpha_{12}v \\ y = \alpha_{21}u + \alpha_{22}v. \end{cases} \tag{26}$$

Будем говорить,что линейная форма $h(x, y) = a_1x + a_2y$ аннулируется в результате применения линейного преобразования (26) тогда и только тогда, когда

$$h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = 0u + 0v.$$

Лемма 1. *Над кольцом $\mathcal{K}$ линейная форма*

$$h(x, y) = a_1x + a_2y \tag{27}$$

аннулируется в результате применения линейного преобразования (26) тогда и только тогда, когда истинны равенства

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0. \end{cases} \tag{28}$$

Доказательство. Подставив (26) в (27), получим

$$h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) == a_1(\alpha_{11}u + \alpha_{12}v) + a_2(\alpha_{21}u + \alpha_{22}v) =$$

$$= (a_1\alpha_{11} + a_2\alpha_{21})u + (a_1\alpha_{12} + a_2\alpha_{22})v. \tag{29}$$

Из (29) вытекает, что равенство

$$h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = 0u + 0v$$

истинно тогда и только тогда, когда истинны равенства (28).

□

Следствие 1. *Если $a_1 \in K^{inv}$ или $a_2 \in K^{inv}$, то любое линейное преобразование (24), аннулирующее линейную форму (27), является необратимым линейным преобразованием над кольцом $\mathcal{K}$.*

Доказательство. Предположим, что линейное преобразование (26) аннулирует линейную форму (27).

Пусть $a_1 \in K^{inv}$. Тогда

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha_{11} = -a_1^{-1}a_2\alpha_{21} \\ \alpha_{12} = -a_1^{-1}a_2\alpha_{22}. \end{cases}$$

Следовательно,

$$\det(A) = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} == -a_1^{-1}a_2\alpha_{21}\alpha_{22} + a_1^{-1}a_2\alpha_{22}\alpha_{21} = 0,$$

откуда вытекает, что линейное преобразование (26), аннулирующее линейную форму (27), является необратимым линейным преобразованием над кольцом $\mathcal{K}$.

В случае, когда $a_2 \in K^{inv}$, доказательство осуществляется аналогичным образом.

□

Выясним, к какому виду в результате применения линейного преобразования (28) над кольцом $\mathcal{K}$ может быть приведена квадратичная форма

$$f(x, y) = a_{11}x^2 + a_{12}xy + a_{22}y^2, \tag{30}$$

где $a_{11}, a_{12}, a_{22} \in K$ $((a_{11}, a_{12}, a_{22}) \neq (0, 0, 0))$.

Теорема 5. *Над кольцом $\mathcal{K}$ квадратичная форма (30) в результате применения линейного преобразования (26) может быть приведена к виду*

$$g(u, v) = b_{11}u^2 + b_{22}v^2 \tag{31}$$

тогда и только тогда, когда существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0. \tag{32}$$

При этом, коэффициенты b_{11} и b_{22} определяются равенствами:

$$b_{11} = a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2, \tag{33}$$

$$b_{22} = a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2. \tag{34}$$

Доказательство. Применив линейное преобразование (26) к квадратичной форме (30), получим

$$\begin{gathered} g(u, v) = f(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = \\ = a_{11}(\alpha_{11}^2u^2 + 2\alpha_{11}\alpha_{12}uv + \alpha_{12}^2v^2) + \\ + a_{12}(\alpha_{11}\alpha_{21}u^2 + (\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21})uv + \alpha_{12}\alpha_{22}v^2) + \\ + a_{22}(\alpha_{21}^2u^2 + 2\alpha_{21}\alpha_{22}uv + \alpha_{22}^2v^2) = \end{gathered}$$

$$= (a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2)u^2 +$$
$$+(2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}))uv +$$
$$+(a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2)v^2. \tag{35}$$

Из (35) вытекает, что истинность равенства (32) является необходимым и достаточным условием приведения квадратичной формы (30) к виду (31). При этом, коэффициенты b_{11} и b_{22} определяются, соответственно, равенством (33) и (34).

□

Из (35) непосредственно вытекает, что истинны следующие три следствия.

Следствие 2. *Над кольцом $\mathcal{K}$ квадратичная форма (30) в результате применения линейного преобразования (26) может быть приведена к виду*

$$g(u, v) = b_{11}u^2 \tag{36}$$

тогда и только тогда, когда существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0. \end{cases} \tag{37}$$

При этом, коэффициент b_{11} определяется равенством (33).

Следствие 3. *Над кольцом $\mathcal{K}$ квадратичная форма (30) в результате применения линейного преобразования (26) может быть приведена к виду*

$$g(u, v) = b_{22}v^2 \tag{38}$$

тогда и только тогда, когда существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0. \end{cases} \tag{39}$$

При этом, коэффициент b_{22} определяется равенством (34).

Следствие 4. *Над кольцом $\mathcal{K}$ квадратичная форма (30) в результате применения линейного преобразования (26) может быть приведена к виду*

$$g(u, v) = b_{12}uv \tag{40}$$

тогда и только тогда, когда существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0. \end{cases} \tag{41}$$

При этом, коэффициент b_{12} определяется равенством

$$b_{12} = 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}). \tag{42}$$

Замечание. Необходимость выделения уравнения $b_{12}uv + a_0 = 0$ в отдельный случай обусловлена тем, что не всегда в кольце многочлен $b_{12}uv + a_0$ с помощью обратимого линейного преобразования $u = \gamma U + \delta V$, $v = \varphi U + \psi V$ может быть приведен к виду $\gamma\varphi U^2 + \delta\psi V^2$. Критерием возможности такого приведения является существование таких $\gamma, \delta, \varphi, \psi \in K$, что $\gamma\psi - \delta\varphi \neq 0$ и $\gamma\psi + \delta\varphi = 0$.

Некоторые из установленных выше равенств упрощаются в случае, когда характеристика кольца $\mathcal{K}$ равна 2. Действительно, равенство (32) принимает вид

$$a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0, \tag{43}$$

а равенство (42) – вид

$$b_{12} = a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}). \tag{44}$$

Из леммы 1, теоремы 5 и следствий 2-4 вытекают следующие достаточные условия приведения к каноническому виду кривой Γ, определяемой над кольцом $\mathcal{K}$ уравнением (1), в результате применения линейного преобразования (26).

Кривая Γ, определяемая уравнением (1) над кольцом $\mathcal{K}$, применением линейного преобразования (26):

1) может быть приведена к виду

$$b_{11}u^2 + b_{22}v^2 + a_0 = 0, \tag{45}$$

если существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0; \end{cases} \tag{46}$$

2) может быть приведена к виду

$$b_{11}u^2 + a_0 = 0, \tag{47}$$

если существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0; \end{cases} \tag{48}$$

3) может быть приведена к виду

$$b_{22}v^2 + a_0 = 0, \tag{49}$$

если существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0; \end{cases} \tag{50}$$

4) может быть приведена к виду

$$b_{12}uv + a_0 = 0, \tag{51}$$

если существуют такие $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in K$, что

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0. \end{cases} \tag{52}$$

Таким образом, системы нелинейных уравнений (46), (48), (50) и (52) могут быть использованы для поиска линейного преобразования, осуществляющего приведение кривой Γ, определяемой уравнением (1) над кольцом $\mathcal{K}$, соответственно, к виду (45), (47), (49) или (51).

Линейное преобразование (24) является биекцией множества K^2 на себя тогда и только тогда, когда 2×2-матрица (25) обратима над кольцом $\mathcal{K}$.

Последнее имеет место тогда и только тогда, когда

$$\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \in K^{inv}. \tag{53}$$

Теорема 6. *Если характеристика кольца $\mathcal{K}$ равна 2, а $a_{12} \in K^{inv}$, то никаким обратимым линейным преобразованием (24) квадратичная форма (30) не может быть приведена ни к виду (36), ни к виду (38).*

Доказательство. Предположим противное, т.е. что характеристика кольца $\mathcal{K}$ равна 2, $a_{12} \in K^{inv}$ и существует обратимое линейное преобразование (24), приводящее квадратичную форму (30) к виду (36) или (38). Тогда истинно равенство (43).

Так как $a_{12} \in K^{inv}$, то равенство (43) эквивалентно равенству

$$\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21} = 0. \tag{54}$$

А так как 2×2-матрица (25) обратима над кольцом $\mathcal{K}$, то истинно условие (53).

Из (53) и (54) вытекает, что

$$2\alpha_{11}\alpha_{22} \in K^{inv} \Leftrightarrow 0 \in K^{inv}.$$

Полученное противоречие показывает, что предположение – ложное.

Отсюда и вытекает, что если характеристика кольца $\mathcal{K}$ равна 2, а $a_{12} \in K^{inv}$, то никаким обратимым линейным преобразованием (24) квадратичная форма (30) не может быть приведена ни к виду (36), ни к виду (38).

□

7. Заключение. В работе исследованы свойства кривых линий 2-го порядка над конечным ассоциативно-коммутативным кольцом с единицей.

Дальнейшие исследования могут быть связаны с анализом сложности построения в явном виде точек этих кривых. Другое направление связано с исследованием существования и сложности построения канонических форм для исследуемых кривых, принадлежащих специальным нетривиальным достаточно узким подмножествам кривых.

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
2. *Харин Ю.С., Берник В.И., Матвеев Г.В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
3. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦМНО, 2003. – 328 с.
4. *Коблиц Н.* Введение в эллиптические и модулярные формы. – М: Мир, 1988. – 320 с.
5. *Шафаревич И.Р.* Основы алгебраической геометрии. Т.1. – М.: Наука, 1988. – 352 с.
6. *Кокс Д., Литтл Дл., О'Ши Д.* Идеалы, многообразия и алгоритмы. – М.: Мир, 2000. – 687 с.
7. *Курош А.Г.* Лекции по общей алгебре. – М. Наука, 1973. – 400 с.

V.V. Skobelev

Analysis of the 2-d order curves over some finite ring.

The 2-d order curves over over a finite associative-commutative ring with the unit are investigated. Some characteristics of the structure of the set of analyzed curves' points determined via polynomial's factorization are established. The structure of the set of irregular points for analyzed curves is characterized. Methods of transforming analyzed curves into canonical form are investigated.

Keywords: *associative-commutative rings, 2-d order curves, irregular points, polynomial factorization, canonical forms.*

В.В. Скобелєв

Аналіз кривих 2-го порядку над скінченним кільцем.

Досліджено криві лінії 2-го порядку над скінченним асоціативно-комутативним кільцем з одиницею. Встановлено ряд характеристик структури множини точок аналізованих кривих, які визначено в термінах факторизації полінома. Охарактеризовано структуру множини особливих точок аналізованих кривих. Досліджено методи зведення аналізованих кривих до канонічної форми.

Ключові слова: *асоціативно-комутативні кільця, лінії 2-го порядку, особливі точки, факторизація полінома, канонічні форми.*

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 24.03.11