Замечание о ядре группового гомоморфизма метода спуска Вейля*

М. А. ЧЕРЕПНЁВ
Московский государственный университет им. М. В. Ломоносова
e-mail: cherepniov@gmail.com

УДК 512.624

Ключевые слова: эллиптические кривые, дискретный логарифм, спуск Вейля.

Аннотация

В статье при выполнении некоторых условий доказываются невырожденность, а также некоторые другие свойства ядра группового гомоморфизма, построенного методом спуска Вейля для атаки на дискретное логарифмирование на эллиптических кривых над полем характеристики 2.

Abstract

M. A. Cherepniov, A note on the kernel of group homomorphism from the Weil descent method, Fundamentalnaya i prikladnaya matematika, vol. 19 (2014), no. 6, pp. 213—224.

In this article, we demonstrate some properties of the kernel of homomorphism, obtained from the Weil descent attack on the elliptic curves over a field of characteristic 2, in particular, its nondegeneracy under some conditions.

Для решения задачи дискретного логарифмирования на эллиптической кривой над конечным полем характеристики 2 может быть применён спуск Вейля, а именно гомоморфизм исходной кривой на группу классов дивизоров некоторой гиперэллиптической кривой над значительно меньшим по мощности подполем. С основными свойствами и определениями можно познакомиться по [1, 4, 5, 14]. Вместо эллиптических могут быть рассмотрены и гиперэллиптические кривые. Некоторые примеры и оценки получены в [6, 10].

Метод спуска Вейля [7—9, 12] в случае эллиптической кривой над полем K характеристики 2 заключается в построении гомоморфизма ϕ из группы точек $E(K)$ эллиптической кривой E

$$y^2 + xy + x^3 + \alpha x^2 + \beta = 0, \quad \alpha, \beta \in K, \tag{1}$$

над бóльшим полем $K = GF(2^{nr})$ в группу классов дивизоров некоторой гиперэллиптической кривой над относительно меньшим подполем $k = GF(2^r) \subset K$.

*Работа поддержана грантом офи м2 13-01-12420 и Минобрнауки России, соглашение от 17 июня 2014 г. № 14.604.21.0034.

© 2014 *Национальный Открытый Университет «ИНТУИТ»*

Отображение ϕ индуцировано композицией следующих замен переменных. Пусть

$$x = \frac{1}{f(u)}, \quad y = \sqrt{\beta} + \frac{v}{f^2(u)} \tag{2}$$

для некоторого многочлена

$$f(u) = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i u^{2^i}, \quad \lambda_i \in K, \quad \lambda_0 \neq 0, \quad \lambda_{m-1} \neq 0.$$

В новых координатах кривая E будет иметь вид

$$v^2 + f(u)v + h(u) = 0, \tag{3}$$

где

$$h(u) = f(u) + \alpha f(u)^2 + \sqrt{\beta} f(u)^3.$$

Сделаем замену переменных

$$\begin{cases} \tilde{u} = \lambda_0 u + \lambda'', \\ \tilde{v} = v + g(\tilde{u})t(\tilde{u}), \end{cases}$$

где

$$g(\tilde{u}) = f\left(\frac{\tilde{u} - \lambda''}{\lambda_0}\right),$$

а $\lambda'' \in K$ выбрано так, что $g(\tilde{u}) \in k[\tilde{u}]$,

$$t(\tilde{u}) = \mathrm{Tr}_{K/k}\left(\frac{v}{g(\tilde{u})}\right) + \frac{v}{g(\tilde{u})}.$$

В новых переменных кривая (3) запишется следующим уравнением над k:

$$\tilde{v}^2 + g(\tilde{u})\tilde{v} + g(\tilde{u})(1 + ag(\tilde{u}) + bg(\tilde{u})^2) = 0, \quad \text{где} \quad a, b \in k. \tag{4}$$

Теорема 1. *Пусть n — нечётное число и род кривой* (4) *не равен $2^{m-1} - 1$ (в этом случае он равен 2^m). Тогда для построенного методом спуска Вейля гомоморфизма ϕ выполнено следующее: $P(0, \sqrt{\beta}) \notin \mathrm{Ker}\,\phi$ и степени вхождения двойки в порядки точек кривой E и их образов совпадают.*

Отметим, что согласно [9, с. 15] в случае когда n простое, $r = 1$, ожидаемый род гиперэллиптической кривой, полученной в результате применения спуска Вейля, равен 2^{n-1}.

С точки зрения практики, данная теорема подтверждает эффективность применения спуска Вейля для решения задачи дискретного логарифмирования на эллиптических кривых над полем характеристики 2. Помимо упрощения арифметики, связанного с переходом в меньшее поле, мы можем применять на гиперэллиптической кривой алгоритм с факторной базой, который имеет субэкспоненциальную сложность.

1. Основные понятия и определения

Любой определённый над F_q дивизор эквивалентен (с точностью до дивизора функции) некоторому полуприведённому дивизору $D = \sum m_P P$, определённому над F_q, т. е. для всех конечных точек P выполнено следующее: $m_P \geqslant 0$, а если $m_P > 0$, то для сопряжённой точки $\bar{P}$ имеем $m_{\bar{P}} = 0$ при $\bar{P} \neq P$, $m_{\bar{P}} = 1$ при $\bar{P} = P$ [11, приложение, лемма 4.2].

Пусть даны два дивизора: $D_1 = \sum m_P P$, $D_2 = n_P P$. Их наибольшим общим делителем называется дивизор НОД$(D_1, D_2) = \sum \min(m_P, n_P) P$.

Теорема 2 [11, приложение, теорема 5.1]. *Пусть $D = \sum m_i P_i$ — полуприведённый дивизор, $P_i = P_i(x_i, y_i)$, $x_i, y_i \in \bar{F}_q$, $a(x) = \prod (x - x_i)^{m_i}$. Тогда существует единственный многочлен $b(x) \in \bar{F}_q[x]$, такой что выполнены следующие условия*:

1) $\deg b(x) < \deg a(x)$;
2) $b(x_i) = y_i$ *для всех* i, *для которых* $m_i \neq 0$;
3) $a(x) \mid b(x)^2 + b(x)f(x) + h(x)$.

Для так определённых многочленов будем использовать обозначение

$$D = \operatorname{div}(a, b). \tag{5}$$

Алгоритм сложения дивизоров [11].

Вход: полуприведённые дивизоры вида (5), определённые над F_q: $D_1 = \operatorname{div}(a, b)$, $D_2 = \operatorname{div}(c, d)$.

Выход: полуприведённый дивизор $D = \operatorname{div}(s, t)$, определённый над F_q и эквивалентный $D_1 + D_2$: $D \sim D_1 + D_2$.

Шаг 1: при помощи алгоритма Евклида получим $e_1, e_2, l_1 \in F_q[x]$, такие что

$$l_1 = (a, c) = e_1 a + e_2 c.$$

Шаг 2: при помощи алгоритма Евклида получим $g_1, g_2, l \in F_q[x]$, такие что

$$l = (l_1, b + d + f) = g_1 l_1 + g_2 (b + d + f).$$

Шаг 3: пусть $v_1 = g_1 e_1$, $v_2 = g_1 e_2$, $w = g_2$, тогда $l = v_1 a + v_2 c + w(b + d + f)$.

Шаг 4: вычислим $s = ac/l^2$, $t = \big(v_1 ad + v_2 cb + w(bd - h)\big)/l \pmod{s}$.

Полуприведённый дивизор $D = \sum m_P P$ называется приведённым, если $\sum m_P \leqslant g$.

Алгоритм приведения дивизоров [11].

Вход: полуприведённый дивизор вида (5), определённый над F_q: $D = \operatorname{div}(a, b)$.

Выход: приведённый дивизор вида (5) $D' = \operatorname{div}(a', b')$, определённый над F_q: $D \sim D'$.

Шаг 1: вычислим $a_1(x) = b(x)^2 + b(x)f(x) + h(x)/a(x)$, $b_1(x) = -b(x) - f(x) \pmod{a_1(x)}$, $\deg b_1(x) < \deg a_1(x)$.

Шаг 2: если $\deg a_1(x) > g$, положим $a(x) = a_1(x)$, $b(x) = b_1(x)$, переход на шаг 1, иначе разделим $a_1(x)$ на его старший коэффициент, вывод: $D' = \operatorname{div}(a_1, b_1)$.

Пусть $\Upsilon \subset F$ — два поля алгебраических функций. Их поля констант обозначаются соответственно L и K. При этом будет предполагаться, что $L = K \cap \Upsilon$.

Определим теперь отображение конормы из группы дивизоров $\operatorname{Div}(\Upsilon)$ поля Υ в группу $\operatorname{Div}(F)$ дивизоров поля F. Для каждой точки p поля Υ определим её *конорму* равенством

$$\operatorname{Con}_{F/\Upsilon}(p) = \sum_{P|p} e(P \mid p) \cdot P,$$

где $e(P \mid p)$ — индекс ветвления P над p, а суммирование ведётся по всем точкам P поля F, продолжающим точку p. Для каждого дивизора $D = \sum_p n(p)p \in \operatorname{Div}(\Upsilon)$ определим его конорму равенством

$$\operatorname{Con}_{F/\Upsilon}(D) = \sum_p n(p) \operatorname{Con}_{F/\Upsilon}(p).$$

Лемма 1 [13, лемма III.1.10]. *Если a — ненулевой элемент поля Υ и $(a)^\Upsilon \in \operatorname{Div}(\Upsilon)$, $(a)^F \in \operatorname{Div}(F)$ — главные дивизоры, определённые элементом a в полях Υ и F соответственно, то*

$$\operatorname{Con}_{F/\Upsilon}\big((a)^\Upsilon\big) = (a)^F.$$

В частности, эта лемма означает, что образом главного дивизора при отображении конормы является главный дивизор, и потому это отображение может быть определено на группе классов дивизоров.

2. Исследование группового гомоморфизма метода спуска Вейля

Метод спуска Вейля в нашем случае заключается в построении гомоморфизма ϕ как композиции трёх последовательных отображений. Первое из них, ψ, является изоморфизмом $E(K)$ и группы классов дивизоров кривой E:

$$\psi(P_0) = P_0 - P_\infty. \tag{6}$$

Второе задаётся функцией $\operatorname{Con}_{F/\Upsilon}$, где $F = K(u, v)$ для алгебраических над $\Upsilon = K(x, y)$ элементов u и v, удовлетворяющих уравнениям

$$x = \frac{1}{f(u)}, \quad y = \sqrt{\beta} + \frac{v}{f^2(u)} \tag{7}$$

для некоторого многочлена

$$f(u) = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i u^{2^i}, \quad \lambda_i \in K, \quad \lambda_0 \neq 0, \quad \lambda_{m-1} \neq 0.$$

Отметим, что возведение в квадрат и извлечение квадратного корня — невырожденные линейные операторы на K. В новых координатах кривая E будет иметь вид

$$v^2 + f(u)v + h(u) = 0, \tag{8}$$

где

$$h(u) = f(u) + \alpha f(u)^2 + \sqrt{\beta} f(u)^3.$$

Выясним, из каких точек состоит ядро гомоморфизма, определённого на $E(K)$ формулой

$$\varphi(P) = \mathrm{Con}_{F/\Upsilon}(P - P_\infty).$$

Пусть некоторая точка $P(x_0, y_0)$ кривой (1) лежит в ядре φ. Тогда согласно [3, гл. IV, § 7] дивизор

$$N_{F/\Upsilon}\,\mathrm{Con}_{F/\Upsilon}(P - P_\infty) = [F : \Upsilon](P - P_\infty) = 2^m P - 2^m P_\infty, \quad m \geqslant 1, \tag{9}$$

является главным. Этот дивизор можно получить при помощи m-кратного удвоения дивизора $\mathrm{div}(x - x_0, y_0)$.

Если $x_0 = 0$, то из уравнения (1) следует, что $y_0 = \sqrt{\beta}$. Получилась единственная на этой кривой специальная точка, т. е. её вторая координата определяется по первой однозначно. Поэтому дивизор $2P - 2P_\infty$ кривой E является главным дивизором, а точнее — дивизором элемента x, а дивизор (9) является дивизором элемента $x^{2^{m-1}}$.

Пусть теперь $x_0 \neq 0$. Применим последовательно алгоритмы сложения и приведения дивизоров для подсчёта приведённого дивизора в классе $2\,\mathrm{div}(x - x_0, y_0)$. Получим

$$2\,\mathrm{div}(x - x_0, y_0) \sim \mathrm{div}\left((x - x_0)^2, \left[\frac{y_0(x - x_0)}{x_0} + \frac{{y_0}^2 - x^3 - \alpha x^2 - \beta}{x_0}\right]\right) =$$
$$= \mathrm{div}\left((x - x_0)^2, \left[\left(\frac{y_0}{x_0} + x_0\right)x + {x_0}^2\right]\right) \sim \mathrm{div}(a_1, b_1),$$

где

$$a_1 = \frac{x^2(\frac{y_0}{x_0} + x_0)^2 + {x_0}^4 + (\frac{y_0}{x_0} + x_0)x^2 + {x_0}^2 x + x^3 + \alpha x^2 + \beta}{(x - x_0)^2} =$$
$$= x + \frac{\beta}{{x_0}^2} + {x_0}^2, \quad b_1 \in K.$$

Поскольку род кривой (1) равен 1, получившийся дивизор не является главным, так как согласно [11, приложение, теорема 5.1] приведённый вид главного дивизора есть $\mathrm{div}(1, 0)$. Поэтому если обозначить $2^i\,\mathrm{div}(x - x_0, y_0) = \mathrm{div}(x - x_i, y_i)$, то

$$x_{i+1} = \frac{\beta}{{x_i}^2} + {x_i}^2. \tag{10}$$

Таким образом, дивизор (9) будет главным тогда и только тогда, когда $x_j = 0$ для некоторого $j \in \{0, \ldots, m - 1\}$. В частности, при $j \geqslant 1$ получим,

что $x_{j-1} = \sqrt[4]{\beta} \in K$ и уравнение

$$y_{j-1}{}^2 + \sqrt[4]{\beta} y_{j-1} + \sqrt[4]{\beta}^3 + \alpha\sqrt{\beta} + \beta = 0$$

разрешимо в K. Если сделать в этом уравнении замену переменных $y_{j-1} = \sqrt[4]{\beta}(u + \sqrt[4]{\beta})$, то его разрешимость будет равносильна разрешимости уравнения

$$u^2 + u = \alpha, \quad u \in K. \tag{11}$$

Поскольку левая часть этого уравнения является линейным оператором с ядром порядка 2, то для половины $\alpha \in K$ оно неразрешимо. Таким образом, справедлива следующая теорема.

Теорема 3. *Для кривых вида* (1), *где уравнение* (11) *не является разрешимым в* K, *ядро гомоморфизма* φ *состоит из точки* P_∞ *и, возможно, точки* $P(0, \sqrt{\beta})$.

Если уравнение (11) разрешимо, то в рассматриваемое ядро, возможно, попадёт ещё точка с координатами $(x_{j-1}, y_{j-1}) = \left(\sqrt[4]{\beta}, \sqrt[4]{\beta}(u_i + \sqrt[4]{\beta})\right)$ и сопряжённая к ней $(x_{j-1}, y_{j-1} + x_{j-1})$. При $m \geqslant 2$ для x_{j-2} получим уравнение

$$\beta + \sqrt[4]{\beta} x_{j-2}{}^2 + x_{j-2}{}^4 = 0.$$

Замена $x_{j-2}{}^2 = \sqrt[4]{\beta} z$ показывает, что разрешимость этого уравнения равносильна разрешимости в K уравнения $z^2 + z = \sqrt{\beta}$, что, ввиду того что возведение в квадрат и извлечение квадратного корня являются невырожденными линейными операторами на K, равносильно разрешимости уравнения

$$z^2 + z = \beta, \quad z \in K. \tag{12}$$

Таким образом, для 3/4 всех пар (α, β) из поля K одно из уравнений (11), (12) неразрешимо и в рассматриваемом ядре лежит не более четырёх уже рассмотренных точек.

В общем случае точки, которые могут лежать в ядре, могут быть последовательно построены при помощи уравнения (10), которое сводится к линейному относительно x_i, и уравнения кривой. Поскольку при фиксированном x_{i+1} уравнение (10) в случае его разрешимости в K имеет два решения (или одно в случае $x_{i+1} = 0$), то справедлива следующая теорема.

Теорема 4. *Ядро гомоморфизма* φ *содержит не более* $1 + 2^{m-1}$ *точек.*

Замечание 1. Из равенства (10) следует, что порядок 2 может быть только у точки $P(0, \sqrt{\beta})$. Так как дивизор функции x равен $2P - 2P_\infty$ и отображение (6) является изоморфизмом, эта точка действительно имеет порядок 2.

Лемма 2. *Пусть* $P_0 = P(x_0, y_0)$ — *конечная точка кривой* $E(K)$. *Тогда*

$$\mathrm{Con}_{F/\Upsilon}(P_0 - P_\infty) = \mathrm{div}\left(f(u) + \frac{x_0}{\sqrt{\beta}}, \frac{x_0 + y_0 + \sqrt{\beta}}{\sqrt{\beta}}\right).$$

Доказательство. Многочлен $f(u)$ не имеет кратных корней, поэтому индекс ветвления P равен 1. Легко понять, что

$$\mathrm{Con}_{F/\Upsilon}(P_0) = \mathrm{div}(1 - x_0 f(u), v_0), \quad v_0 = \frac{\sqrt{\beta} + y_0}{{x_0}^2}.$$

Вычислим теперь $\mathrm{Con}_{F/\Upsilon}(P_\infty)$. Если P — точка поля F, лежащая над P_∞, то она лежит и над бесконечной точкой поля $K(x)$, т. е. $1/x = f(u) \in P$ как в идеале. Отсюда следует, что P — конечная точка поля F. Равенство (8) и включение $f(u) \in P$ означают, что $v^2 \in P$. Так как P — простой идеал, заключаем, что $v \in P$. Таким образом, справедливо включение $(f(u), v) \subset P$.

Обратно, если P — точка поля F, порождённая простым идеалом кольца $K[u, v]$, содержащим идеал $(f(u), v) \subset K[u, v]$, то $1/x = f(u) \in P$, и значит, $1/x \in P \cap E(K)$. Согласно [13, предложение III.1.4, гл. 3] пересечение $p = P \cap E(K)$ есть точка поля $E(K)$. Поскольку она содержит $1/x$, она является бесконечно удалённой точкой поля $E(K)$, т. е. P_∞ (так как она единственна), что следует из канонического вида кривой (1). Поэтому образ $P_0 - P_\infty$ после применения конормы будет классом дивизоров кривой (8) над полем F с представителем

$$\mathrm{div}(1 - x_0 f(u), v_0) - \mathrm{div}(f(u), 0). \tag{13}$$

Поскольку $\mathrm{div}\big(f(u)\big) = 2\,\mathrm{div}(f(u), 0)$, дивизор (13) можно представить в форме

$$\mathrm{div}(1 - x_0 f(u), v_0) + \mathrm{div}(f(u), 0).$$

Применим к этому выражению алгоритм сложения классов дивизоров. Последовательно получим $l_1 = 1$, $l = 1$, $e_1 = 1$, $e_2 = x_0$, $g_1 = 1$, $g_2 = 0 = w$. Результат сложения можно представить следующим образом:

$$\mathrm{div}\big(f(u)\big(1 - x_0 f(u)\big), \big[f(u)\big(1 - x_0 f(u)\big) + x_0 f(u) v_0\big]\big) = \\ = \mathrm{div}\big(f(u)\big(1 - x_0 f(u)\big), x_0 v_0 f(u)\big).$$

Последнее равенство справедливо, потому что взятие второй компоненты по модулю первой не меняет класса дивизоров. Род g кривой (8) согласно [9, лемма 9] равен 2^{m-1} или $2^{m-1} - 1$. Поэтому полученный в результате сложения полуприведённый дивизор не является приведённым. Хотя запись (8) не является каноническим видом кривой, к ней можно применять стандартный алгоритм приведения. Результат его работы будет лежать в том же классе, однако не обязательно будет приведённым дивизором. Применив один шаг алгоритма приведения, получим

$$
\begin{aligned}
a_1(u) &= \frac{\bigl(x_0v_0f(u)\bigr)^2 + x_0v_0f(u)^2 + h}{f(u)\bigl(1 - x_0f(u)\bigr)} = \\
&= \frac{f(u)\bigl((x_0v_0)^2 + x_0v_0\bigr) + 1 + \alpha f(u) + \sqrt{\beta}f(u)^2}{1 - x_0f(u)} = \\
&= \frac{1 + \bigl((x_0v_0)^2 + x_0v_0 + \alpha + \frac{\sqrt{\beta}}{x_0}\bigr)f(u) - f(u)\frac{\sqrt{\beta}}{x_0}\bigl(1 - x_0f(u)\bigr)}{1 - x_0f(u)} = \\
&= \frac{\sqrt{\beta}}{x_0}f(u) + \frac{1 + f(u)\bigl(\alpha + \frac{y_0+\sqrt{\beta}}{x_0} + \frac{{y_0}^2+\beta}{{x_0}^2} + \frac{\sqrt{\beta}}{x_0}\bigr)}{1 - x_0f(u)} = \frac{\sqrt{\beta}}{x_0}f(u) + 1,
\end{aligned}
$$

$$
b_1(u) \equiv (1 + x_0v_0)f(u) \equiv \left(1 + \frac{y_0 + \sqrt{\beta}}{x_0}\right)\frac{x_0}{\sqrt{\beta}} \pmod{a_1(u)}
$$

или

$$
b_1(u) \equiv \frac{x_0 + y_0 + \sqrt{\beta}}{\sqrt{\beta}} \pmod{a_1(u)}.
$$

Следовательно, образ отображения $\mathrm{Con}_{F/\Upsilon}$ примет вид

$$
\operatorname{div}\left(f(u) + \frac{x_0}{\sqrt{\beta}}, \frac{x_0 + y_0 + \sqrt{\beta}}{\sqrt{\beta}}\right). \tag{14}
$$

Лемма 2 доказана. □

Заметим, что, если $g = 2^{m-1}$, этот дивизор является нетривиальным приведённым дивизором для любой конечной точки P_0.

Спуск Вейля завершает замена переменных

$$
\begin{cases}
\tilde{u} = \lambda_0 u + \lambda'', \\
\tilde{v} = v + g(\tilde{u})t(\tilde{u}),
\end{cases}
$$

где

$$
g(\tilde{u}) = f\left(\frac{\tilde{u} - \lambda''}{\lambda_0}\right),
$$

а $\lambda'' \in K$ выбрано так, что $g(\tilde{u}) \in k[\tilde{u}]$, а затем взята норма.

В новых переменных кривая (8) запишется следующим уравнением над k:

$$
\tilde{v}^2 + g(\tilde{u})\tilde{v} + g(\tilde{u})(1 + ag(\tilde{u}) + bg(\tilde{u})^2) = 0, \quad \text{где} \quad a, b \in k. \tag{15}
$$

Дивизор (14) в новых переменных запишется следующим образом:

$$
\begin{aligned}
&\operatorname{div}\left(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}, \left[\frac{x_0 + y_0 + \sqrt{\beta}}{\sqrt{\beta}} + g(\tilde{u})t(\tilde{u})\right]\right) = \\
&\qquad = \operatorname{div}\left(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}, \left[\frac{x_0 + y_0 + \sqrt{\beta}}{\sqrt{\beta}} + \frac{x_0}{\sqrt{\beta}}t(\tilde{u})\right]\right).
\end{aligned} \tag{16}
$$

Поскольку многочлен g получен из многочлена f при помощи линейной замены переменных, то коэффициент в одночлене первой степени у него умножится на ненулевую константу (легко понять, что это будет 1), а все остальные одночлены будут иметь степени, равные степеням двойки. Поэтому многочлен $g(\tilde{u}) + x_0/\sqrt{\beta}$ не имеет кратных корней.

Обозначим через $f_u(x)$ минимальный многочлен элемента u над k.

Теорема 5. *Пусть n — простое нечётное число и $x_0/\sqrt{\beta} \notin k$. Тогда для построенного методом спуска Вейля гомоморфизма ϕ*

$$\phi\big(P(x_0, y_0)\big) = \operatorname{div}\left(f_{\frac{x_0}{\sqrt{\beta}}}\big(g(\tilde{u})\big), G(\tilde{u})\right),$$

для некоторого $G(\tilde{u}) \in k[\tilde{u}]$. Если $P_0 = P(x_0, y_0)$, $P_1 = P(x_1, y_1)$ и для некоторого $i \in \{0, 1, \ldots, n-1\}$ выполнено

$$x_1 = \sqrt{\beta}\sigma^i \frac{x_0}{\sqrt{\beta}},$$

то $\phi(P_0) = \phi(P_1)$.

Доказательство. По условию теоремы

$$\deg_k \frac{x_0}{\sqrt{\beta}} = n.$$

Обозначим через $u_1, \ldots, u_{2^{m-1}}$ однократные корни многочлена $g(\tilde{u}) + x_0/\sqrt{\beta}$. Корни сопряжённого к нему многочлена

$$\sigma\left(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}\right) = g(\tilde{u}) + \sigma\left(\frac{x_0}{\sqrt{\beta}}\right),$$

где σ — некоторое произвольное продолжение автоморфизма σ: $\sigma w = w^{2^r}$, $w \in K$, на $\bar{K}$, имеют вид $\sigma u_1, \ldots, \sigma u_{2^{m-1}}$. В рассматриваемом случае

$$\sigma^j\left(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}\right) - \left(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}\right) = \sigma^j\left(\frac{x_0}{\sqrt{\beta}}\right) - \frac{x_0}{\sqrt{\beta}},$$

поэтому $\sigma^j u_i \notin \{u_1, \ldots, u_{2^{m-1}}\}$ для любых $i \in 1, \ldots, 2^{m-1}$ при $n \nmid j$. Это также означает, что минимальные многочлены элементов u_i над k различны. Дивизор (16) имеет вид

$$\sum_{i=1}^{2^{m-1}} \operatorname{div}(\tilde{u} - u_i, v_i), \quad u_i, v_i \in \bar{K},$$

а его норма над $k[\tilde{u}, \tilde{v}]$ —

$$\sum_{j=1}^{n} \sum_{i=1}^{2^{m-1}} \operatorname{div}(\tilde{u} - \sigma^j u_i, \sigma^j v_i), \tag{17}$$

(см. [2, следствие 3 предложения 2.1, гл. 1]). Все точки этого дивизора однократны, их первые координаты различны, поэтому он полуприведённый. Значит,

существует многочлен $G(x) \in k[x]$, такой что этот дивизор имеет вид

$$\operatorname{div}\left(N(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}), G(x)\right). \tag{18}$$

Многочлен G может быть найден при помощи метода неопределённых коэффициентов из уравнений

$$G(u_i) = \frac{x_0 + y_0 + \sqrt{\beta}}{\sqrt{\beta}} + \frac{x_0}{\sqrt{\beta}} t(u_i), \quad i = 1, \ldots, 2^{m-1}.$$

Поскольку коэффициенты многочлена g лежат в k, то

$$N\left(g(\tilde{u}) + \frac{x_0}{\sqrt{\beta}}\right) = \prod_{j=1}^{n}\left(g(\tilde{u}) + \sigma^j \frac{x_0}{\sqrt{\beta}}\right) = f_{\frac{x_0}{\sqrt{\beta}}}\big(g(\tilde{u})\big) = \prod_{i=1}^{2^{m-1}} f_{u_i}(\tilde{u}),$$

где $f_{\frac{x_0}{\sqrt{\beta}}}(z) \in k[z]$ — минимальный многочлен элемента $x_0/\sqrt{\beta} \in K$, а в последнем произведении стоят минимальные многочлены элементов $u_1, \ldots, u_{2^{m-1}}$, которые лежат в $k[x]$, неприводимы и в нашем случае различны. Значит, дивизор (18) является суммой 2^{m-1} точек поля $k(\tilde{u}, \tilde{v})$ вида $\operatorname{div}\big(f_{u_i}(\tilde{u}), G_i(\tilde{u})\big)$.

Отметим, что образ точки $P_1 = P(x_1, y_1)$, где для некоторого i

$$\sigma^i \frac{x_0}{\sqrt{\beta}} = \frac{x_1}{\sqrt{\beta}},$$

может отличаться от полученного образа точки P_0 только вторыми координатами: пусть это будут многочлены $G'_i(\tilde{u}) \in k[\tilde{u}]$, которые в рассматриваемом случае, как и G_i, являются решениями сравнений

$$G'^{\,2}_i + gG'_i + g(1 + ag + bg^2) \equiv 0 \pmod{f_{u_i}}.$$

Отсюда следует, что

$$(G_i - G'_i)^2 + g(G_i - G'_i) \equiv 0 \pmod{f_{u_i}}.$$

Поэтому ввиду неприводимости над k многочленов f_{u_i} и того, что $\deg G_i < \deg f_{u_i}$, $\deg G'_i < \deg f_{u_i}$, имеем, что $G'_i \in \{G_i, G_i + g\}$. Таким образом, точки в образе P_1 либо совпадают с точками образа P_0, либо совпадают с сопряжёнными к ним, поэтому в классе дивизоров получим тот же образ.

Пусть теперь n нечётное и $x_0/\sqrt{\beta} \in k$ (например, $(x_0, y_0) = (0, \sqrt{\beta})$). Тогда уравнение (1) перепишем в виде

$$\left(\frac{y_0}{\sqrt{\beta}}\right)^2 + \frac{y_0}{\sqrt{\beta}}\frac{x_0}{\sqrt{\beta}} + 1 + \alpha\left(\frac{x_0}{\sqrt{\beta}}\right)^2 + \sqrt{\beta}\left(\frac{x_0}{\sqrt{\beta}}\right)^3 = 0,$$

откуда для

$$v = \operatorname{Tr}_{K/k}\left(\frac{y_0}{\sqrt{\beta}}\right) + 1$$

имеем

$$v^2 + v\frac{x_0}{\sqrt{\beta}} + \frac{x_0}{\sqrt{\beta}} + \operatorname{Tr}_{K/k}(\alpha)\left(\frac{x_0}{\sqrt{\beta}}\right)^2 + \operatorname{Tr}_{K/k}(\sqrt{\beta})\left(\frac{x_0}{\sqrt{\beta}}\right)^3 = 0.$$

Значит (см. уравнение (15)), вторые координаты точек дивизора (18) принадлежат k и равны

$$\mathrm{Tr}_{K/k}\left(\frac{y_0}{\sqrt{\beta}}\right)+1$$

или

$$\mathrm{Tr}_{K/k}\left(\frac{y_0}{\sqrt{\beta}}\right)+1+\frac{x_0}{\sqrt{\beta}}.$$

В частности, при $x_0=0$ они совпадают и равны нулю. В то же время σ осуществляет перестановку их первых координат, поэтому рассматриваемая норма (17) при $x_0=0$ равна

$$n\sum_{i=1}^{2^{m-1}}\mathrm{div}(\tilde{u}-u_i,0).$$

Поскольку все точки в этой сумме специальные, а n нечётное, то этот дивизор эквивалентен

$$\sum_{i=1}^{2^{m-1}}\mathrm{div}(\tilde{u}-u_i,0)$$

(переход осуществляется дивизором элемента $g(u)^{(n-1)/2}$). Согласно [9] если род кривой (15) не равен $2^{m-1}-1$, то он равен 2^{m-1} и этот дивизор является приведённым, а значит, не является главным, т. е. не лежит в ядре.

Если исходная точка P_0 имела чётный порядок $2^r s$, s нечётно, $r\geqslant 1$, то $2^{r-1}sP_0$ — точка порядка 2. Поэтому согласно приведённому выше замечанию это точка с координатами $(0,\sqrt{\beta})$, которая по доказанному не лежит в ядре. Значит, степень вхождения двойки в порядок образа точки P_0 равна r.

Теорема 1 доказана. □

Литература

[1] Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1985.

[2] Ленг С. Алгебраические числа. — М.: Мир, 1966.

[3] Шевалле К. Введение в теорию алгебраических функций от одной переменной. — М.: Физматгиз, 1959.

[4] Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. — Cambridge: Cambridge Univ. Press, 1999. — (London Math. Soc. Lect. Note Ser.; Vol. 265).

[5] Cassels J. W. S. Diophantine equations with special reference to elliptic curves // J. London Math. Soc. — 1966. — Vol. 41. — P. 193—291.

[6] Galbraith S. D. Weil descent of Jacobians. — `https://www.math.auckland.ac.nz/~sgal018/dec.pdf`.

[7] Galbraith S. D., Hess F., Smart N. P. Extending the GHS Weil descent attack // Advances in Cryptology — EUROCRYPT 2002. — Berlin: Springer, 2002. — (Lect. Notes Comp. Sci.; Vol. 2332). — P. 29—44.

[8] Galbraith S. D., Smart N. P. A cryptographic application of Weil descent // Cryptography and Coding (7th IMA Int. Conf. Cirencester, UK, December 20—22, 1999. Proc. — Berlin: Springer, 1999. — (Lect. Notes Comp. Sci.; Vol. 1746). — P. 191—200. — The full version of the paper is HP Labs Technical Report, HPL-1999-70.

[9] Gaudry P., Hess F., Smart N. P. Constructive and Destructive Facets of Weil Descent on Elliptic Curves: Hewlett Packard Laboratories Technical Report. — 2000. — `http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/papers.html`.

[10] Karabina K., Menezes A., Pomerance C., Shparlinski I. E. On the asymptotic effectiveness of Weil descent attacks // J. Math. Cryptology. — 2010. — Vol. 4, no. 2. — P. 175—191.

[11] Koblitz N. Algebraic Aspects of Cryptography. — Berlin: Springer, 1998.

[12] Menezes A., Qu M. Analysis of the Weil descent attack of Gaudry, Hess and Smart // Topics in Cryptology — CT-RSA 2001. — Berlin: Springer, 2001. — (Lect. Notes Comp. Sci.; Vol. 2020). — P. 308—318.

[13] Stichtenoth H. Algebraic Function Fields and Codes. — Berlin: Springer, 1998.

[14] Weber H. Lehrbuch der Algebra. Vols. I—III. — New York: Chelsea Publ. Comp., 1902.