Замечание о ядре группового гомоморфизма метода спуска Вейля.

Черепнёв М.А.
работа поддержана грантом офи м2 13-01-12420 и Минобрнауки России, соглашение от 17 июня 2014 г. № 14.604.21.0034, , идентификатор соглашения RFMEFI60414X0034.
email: cherepniov@gmail.com

В этой статье, при выполнении некоторых условий, доказывается невырожденность, а также некоторые свойства ядра группового гомоморфизма, построенного методом спуска Вейля для атаки на дискретное логарифмирование на эллиптических кривых над полем характеристики 2 [1].

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 гиперэллиптическойю кривой над значительно меньшим по мощности подполем. С основными свойствами и определениями можно познакомиться в [2, 3, 4, 5]. Вместо эллиптических могут быть рассмотрены и гиперэллиптические кривые. Некоторые примеры и оценки получены в [13, 14].

Метод спуска Вейля [6, 7, 1, 8] в случае эллиптической кривой над полем K характеристики 2 заключается в построении гомоморфизма ϕ из группы точек $E(K)$ эллиптической кривой E

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

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

А именно, ϕ индуцировано композицией следующих замен переменных. Пусть

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

для некоторого многочлена $f(u) = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i u^{2^i}, \lambda_i \in K; \lambda_0 \neq 0, \lambda_{m-1} \neq 0$. 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 следующую замену переменных:

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

где $g(\widetilde{u}) = f(\frac{\widetilde{u}-\lambda''}{\lambda_0})$, а $\lambda'' \in K$ выбрано так, что $g(\widetilde{u}) \in k[\widetilde{u}]$,

$$t(\widetilde{u}) = Tr_{K/k}\left(\frac{v}{g(\widetilde{u})}\right) + \frac{v}{g(\widetilde{u})}.$$

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

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

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:*

$P(0, \sqrt{\beta}) \notin Ker\phi$ и степени вхождения двойки в порядки точек кривой E и их образов совпадают.

Отметим, что согласно [1] (стр.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, то есть для всех конечных точек P выполнено: $m_P \geq 0$, а если $m_P > 0$, то для сопряжённой точки $\overline{P}$ имеем $m_{\overline{P}} = 0$ при $\overline{P} \neq P, m_{\overline{P}} = 1$, при $\overline{P} = P$ [9, Appendix Л. 4.2].

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

Теорема 2 *[9, Appendix Теорема 5.1] Пусть* $D = \sum m_i P_i$ - *полуприведённый дивизор,* $P_i = P_i(x_i, y_i); x_i, y_i \in \overline{F}_q; a(x) = \prod (x - x_i)^{m_i}$. *Тогда существует единственный многочлен* $b(x) \in \overline{F}_q[x]$ *такой, что выполнены следующие условия:*

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

Для так определённых многочленов будем использовать обозначение

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

Алгоритм сложения дивизоров[9]

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

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

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

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

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

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

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

4 шаг: Вычислить $s = ac/l^2, t = (v_1 ad + v_2 cb + w(bd - h))/l(mods)$.

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

Алгоритм приведения дивизоров[9]

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

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

1 шаг: вычислить $a_1(x) = b(x)^2 + b(x)f(x) + h(x)/a(x), b_1(x) = -b(x) - f(x)(moda_1(x)), degb_1(x) < dega_1(x)$.

2 шаг: если $dega_1(x) > g$, присвоить $a(x) = a_1(x), b(x) = b_1(x)$, идти на шаг 1. Иначе разделить $a_1(x)$ на его старший коэффициент, вывод: $D' = div(a_1, b_1)$.

Конорма и норма

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 $Div\ (\Upsilon)$ поля Υ в группу $Div\ (F)$ дивизоров поля F. Для каждой точки p поля Υ определим ее *конорму* равенством

$$Con_{F/\Upsilon}(p) = \sum_{P|p} e(P|p) \cdot P,$$

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

$$Con_{F/\Upsilon}(D) = \sum_p n(p) Con_{F/\Upsilon}(p).$$

Лемма 1 *([12], L. III.1.10.) Если a – ненулевой элемент поля Υ и $(a)^\Upsilon \in Div\ (\Upsilon)$, $(a)^F \in Div\ (F)$ – главные дивизоры, определенные элементом a в полях Υ и F соответственно, то*

$$Con_{F/\Upsilon}((a)^{\Upsilon}) = (a)^{F}.$$

В частности, эта лемма означает, что образом главного дивизора при отображении конормы вляется 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 $Con_{F/\Upsilon}$, где $F = K(u, v)$ для алгебраических над $\Upsilon = K(x, y)$ элементов u и v, удовлетворяющих следующим уравнениям:

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

для некоторого многочлена

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

Отметим, что возведение в квадрат и извлечение квадратного корня являются невырожденными линейными операторами 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

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

Пусть некоторая точка $P(x_0, y_0)$ кривой (1) лежит в ядре φ. Тогда, согласно [10, глава IV, §7], следующий дивизор является главным:

$$N_{F/\Upsilon} Con_{F/\Upsilon}(P - P_\infty) = [F : \Upsilon](P - P_\infty) = 2^m P - 2^m P_\infty, m \geq 1. \quad (9)$$

Этот дивизор можно получить при помощи m кратного удвоения дивизора $div(x - x_0, y_0)$.

Если $x_0 = 0$, то из уравнения (1) $y_0 = \sqrt{\beta}$. Получилась единственная на этой кривой специальная точка, то есть 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 $2div(x - x_0, y_0)$. Получим:

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

$$div((x - x_0)^2, \left[(\frac{y_0}{x_0} + x_0)x + {x_0}^2\right])$$

$$\sim div(a_1, b_1),$$

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, то получившийся дивизор не является главным, так как согласно [9, Appendix, Теорема 5.1] приведённый вид главного дивизора есть $div(1, 0)$. Поэтому если обозначить $2^i div(x - x_0, y_0) = div(x - x_i, y_i)$, то

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

Таким образом, дивизор (9) будет главным тогда и только тогда, когда для некоторого $j \in \{0, ..., m-1\}, x_j = 0$. В частности, при $j \geq 1$ получим $x_{j-1} = \sqrt[4]{\beta} \in K$ 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 разрешимо 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 $(x_{j-1}, y_{j-1}) = (\sqrt[4]{\beta}, \sqrt[4]{\beta}(u_i + \sqrt[4]{\beta}))$ и сопряжённая к ней $(x_{j-1}, y_{j-1} + x_{j-1})$. При $m \geq 2$ 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) или (12) неразрешимо, и в рассматриваемом ядре лежит не более, чем 4 уже рассмотренные точки.

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 $Con_{F/\Upsilon}(P_0 - P_\infty) = div(f(u) + \frac{x_0}{\sqrt{\beta}}, \frac{x_0+y_0+\sqrt{\beta}}{\sqrt{\beta}})$*

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

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

Вычислим теперь $Con_{F/\Upsilon}(P_\infty)$. Если P - точка поля F, лежащая над P_∞, то она лежит и над бесконечной точкой поля $K(x)$, то есть

$$\frac{1}{x} = f(u) \in P \text{как в идеале.}$$

Отсюда следует, что P - конечная точка поля F. Равенство (8) и включение $f(u) \in P$ означают, что $v^2 \in P$, и 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 $\frac{1}{x} = f(u) \in P$, и, значит, $\frac{1}{x} \in P \cap E(K)$. Согласно [12, Предложение III.1.4, глава 3], пересечение $p = P \cap E(K)$ есть точка поля $E(K)$. Поскольку она содержит $\frac{1}{x}$, то она является бесконечно удалённой точкой поля $E(K)$, то есть P_∞ в силу её единственности, 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

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

Поскольку $div(f(u)) = 2div(f(u), 0)$, то дивизор (13) можно представить в форме

$$= div(1 - x_0 f(u), v_0) + div(f(u), 0).$$

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:

$$div(f(u)(1 - x_0 f(u)), [f(u)(1 - x_0 f(u)) + x_0 f(u) v_0]) =$$
$$= div(f(u)(1 - x_0 f(u)), x_0 v_0 f(u)).$$

Последнее равенство справедливо, потому что взятие второй компоненты по модулю первой не меняет класс дивизоров. Род кривой (8) - g, согласно [1, 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:

$$a_1(u) = \frac{(x_0 v_0 f(u))^2 + x_0 v_0 f(u)^2 + h}{f(u)(1 - x_0 f(u))} =$$
$$\frac{f(u)((x_0 v_0)^2 + x_0 v_0) + 1 + \alpha f(u) + \sqrt{\beta} f(u)^2}{1 - x_0 f(u)} =$$
$$\frac{1 + ((x_0 v_0)^2 + x_0 v_0 + \alpha + \frac{\sqrt{\beta}}{x_0}) f(u) - f(u) \frac{\sqrt{\beta}}{x_0}(1 - x_0 f(u))}{1 - x_0 f(u)} =$$
$$\frac{\sqrt{\beta}}{x_0} f(u) + \frac{1 + f(u)(\alpha + \frac{y_0 + \sqrt{\beta}}{x_0} + \frac{{y_0}^2 + \beta}{{x_0}^2} + \frac{\sqrt{\beta}}{x_0})}{1 - x_0 f(u)} = \frac{\sqrt{\beta}}{x_0} f(u) + 1$$

$$b_1(u) \equiv (1 + x_0 v_0) f(u) \equiv (1 + \frac{y_0 + \sqrt{\beta}}{x_0}) \frac{x_0}{\sqrt{\beta}} \pmod{a_1(u)},$$

или

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

Следовательно, образ отображения $Con_{F/\Upsilon}$ примет вид:

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

Лемма 2 доказана.

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

Спуск Вейля завершает следующая замена переменных

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

где $g(\widetilde{u}) = f(\frac{\widetilde{u}-\lambda''}{\lambda_0})$, а $\lambda'' \in K$ выбрано так, что $g(\widetilde{u}) \in k[\widetilde{u}]$, а затем взятие нормы.

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

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

Дивизор (14) в новых переменных запишется следующим образом:

$$\begin{array}{c} div(g(\widetilde{u}) + \frac{x_0}{\sqrt{\beta}}, \left[\frac{x_0+y_0+\sqrt{\beta}}{\sqrt{\beta}} + g(\widetilde{u})t(\widetilde{u})\right]) = \\ div(g(\widetilde{u}) + \frac{x_0}{\sqrt{\beta}}, \left[\frac{x_0+y_0+\sqrt{\beta}}{\sqrt{\beta}} + \frac{x_0}{\sqrt{\beta}}t(\widetilde{u})\right]), \end{array} \tag{16}$$

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 увидеть, что это будет 1), а все остальные одночлены будут иметь степени, равные степеням двойки. Поэтому, многочлен $g(\widetilde{u}) + \frac{x_0}{\sqrt{\beta}}$ не имеет кратных корней.

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

Теорема 5 *Пусть n - простое нечётное число и $\frac{x_0}{\sqrt{\beta}} \notin k$. Тогда для построенного методом спуска Вейля гомоморфизма ϕ выполнено: $\phi(P(x_0, y_0)) = div(f_{\frac{x_0}{\sqrt{\beta}}}(g(\widetilde{u})), G(\widetilde{u}))$, для некоторого $G(\widetilde{u}) \in k[\widetilde{u}]$. Если $P_0 = P(x_0, y_0), P_1 = P(x_1, y_1)$ и для некоторого $i \in \{0, 1, ..., n-1\}$, выполнено: $x_1 = \sqrt{\beta}\sigma^i \frac{x_0}{\sqrt{\beta}}$, тогда $\phi(P_0) = \phi(P_1)$.*

Доказательство. По условию теоремы $deg_k \frac{x_0}{\sqrt{\beta}} = n$. Обозначим $u_1, ..., u_{2^{m-1}}$ — однократные корни многочлена $g(\widetilde{u}) + \frac{x_0}{\sqrt{\beta}}$. Корни сопряжённого к нему многочлена $\sigma(g(\widetilde{u}) + \frac{x_0}{\sqrt{\beta}}) = g(\widetilde{u}) + \sigma(\frac{x_0}{\sqrt{\beta}})$, где σ - некоторое произвольное продолжение автоморфизма $\sigma : \sigma w = w^{2^r}, w \in K$ на $\overline{K}$, имеют вид $\sigma u_1, ..., \sigma u_{2^{m-1}}$. В рассматриваемом случае $\sigma^j(g(\widetilde{u})+\frac{x_0}{\sqrt{\beta}})-(g(\widetilde{u})+\frac{x_0}{\sqrt{\beta}}) = \sigma^j(\frac{x_0}{\sqrt{\beta}})-\frac{x_0}{\sqrt{\beta}}$, поэтому $\sigma^j u_i \notin \{u_1, ..., u_{2^{m-1}}\}$ для любых $i \in 1, ..., 2^{m-1}$, при $n \nmid j$. Это также означает, что минимальные многочлены элементов u_i над k различны. Дивизор (16) имеет вид $\sum_{i=1}^{2^{m-1}} div(\widetilde{u} - u_i, v_i); u_i, v_i \in \overline{K}$, а его норма над $k[\widetilde{u}, \widetilde{v}]$ есть

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

(См. [11, Следствие 3 Предложения 2.1, глава 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

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

Многочлен G может быть найден при помощи метода неопределённых коэффициентов из уравнений $G(u_i) = \frac{x_0+y_0+\sqrt{\beta}}{\sqrt{\beta}} + \frac{x_0}{\sqrt{\beta}} t(u_i), \quad i = 1, ..., 2^{m-1}$.

Поскольку коэффициенты многочлена g лежат в k, то

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

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

Отметим, что образ точки $P_1 = P(x_1, y_1)$, где для некоторого i выполнено: $\sigma^i \frac{x_0}{\sqrt{\beta}} = \frac{x_1}{\sqrt{\beta}}$, может отличаться от полученного образа точки P_0 только вторыми координатами: пусть это будут многочлены $G'_i(\widetilde{u}) \in k[\widetilde{u}]$, которые в рассматриваемом случае, также как и G_i, являются решениями сравнений

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

Отсюда

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

Поэтому, ввиду неприводимости над k многочленов f_{u_i} и того, что $degG_i, degG'_i < degf_{u_i}$, имеем $G'_i \in \{G_i, G_i + g\}$. Таким образом, точки в образе P_1 либо совпадают с точками образа P_0, либо совпадают с сопряжёнными к ним, а поэтому в классе дивизоров получим тот же образ. Теорема 5 доказана.

Пусть теперь n - нечётное и $\frac{x_0}{\sqrt{\beta}} \in k$ (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 $v = Tr_{K/k}(\frac{y_0}{\sqrt{\beta}}) + 1$ имеем

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

Значит, (см. уравнение (15)) вторые координаты точек дивизора (18) принадлежат k и равны $Tr_{K/k}(\frac{y_0}{\sqrt{\beta}}) + 1$, или $Tr_{K/k}(\frac{y_0}{\sqrt{\beta}}) + 1 + \frac{x_0}{\sqrt{\beta}}$. В частности, при $x_0 = 0$ они совпадают и равны нулю. В тоже время, σ осуществляет перестановку их первых координат, поэтому рассматриваемая норма (17) при $x_0 = 0$ равна

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

Поскольку все точки в этой сумме специальные, а n - нечётное, то этот дивизор эквивалентен $\sum_{i=1}^{2^{m-1}} div(\widetilde{u} - u_i, 0)$ (переход осуществляется дивизором элемента $g(u)^{\frac{n-1}{2}}$). Согласно [1], 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, то есть не лежит в ядре.

Если исходная точка P_0 имела чётный порядок $2^r s$, s - нечётно, $r \geq 1$, 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.

Список литературы

[1] P. Gaudry, F. Hess, N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. http://Hewlett Packard Laboratories Technical Report, 2000.-20p.(ultralix.polytechnique.fr/Labo/Pierrick.Gaudry/papers.html)

[2] Blake I.,Seroussi G., Smart N. Elliptic curves in cryptography.London, Mathematical Society 265, Cambridge University Press,1999.

[3] Боревич З.И.,Шафаревич И.Р. Теория чисел.-М.:Наука,1985,-495с.

[4] Cassels J. W. S. Diophantine equations with special reference to elliptic curves.// J. LMS,1966,v.41,p.193-291.

[5] Weber H. Lehrbuch der Algebra. v.I,II,III. New York, Chelsea Publishing Company,1902,-722p.

[6] Galbraith S.D., Smart N.P. A cryptographic application of Weil descent. Cryptography and Coding.// 7th IMA Conference, Springer-Verlag, LNCS,1999,v.1746,p.191-200. (The full version of the paper is HP Labs Technical Report, HPL-1999-70.)

[7] S. D. Galbraith, F. Hess, N. P. Smart. Extending the GHS Weil descent attack. Advances in Cryptology (EUROCRYPT 2002),// Springer-Verlag, LNCS,2002,v.2332,p.29-44.

[8] A. Menezes, Qu M. Analysis of the Weil descent attack of Gaudry, Hess and Smart.// Topics in Cryptology - CT-RSA 2001, Springer-Verlag LNCS, 2020, 308-318, 2001.

[9] N.Koblitz Algebraic Aspects of Cryptography.Springer-Verlag,1998,-109p.

[10] Шевалле К. Введение в теорию алгебраических функций от одной переменной.-М.:Физматгиз,1959,-336с.

[11] Ленг С. Алгебраические числа.-М.:Мир.,1966,-221с.

[12] Stichtenoth H. Algebraic function fields and codes.Springer,1998,-262c.

[13] Karabina K., Menezes A., Pomerance C., Shparlinski I.E. On the asymptotic effectiveness of Weil descent attacks.// J. of math. Cryptology, v.4, Iss.2 (Jan 2010),p.175-191.

[14] Galbraith S.D. Weil descent of jacobians. February 1, 2011 https://www.math.auckland.ac.nz/ sgal018/dec.pdf