Math-Net.Ru

Общероссийский математический портал

С. Ю. Рыбаков, Дзета-функции биэллиптических поверхностей над конечными полями, *Матем. заметки*, 2008, том 83, выпуск 2, 273–285

DOI: <https://doi.org/10.4213/mzm4419>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.95.254.165

26 апреля 2023 г., 17:26:17

УДК 512.754

Дзета-функции биэллиптических поверхностей над конечными полями

С. Ю. Рыбаков

Пусть S – биэллиптическая поверхность над конечным полем, а эллиптическая кривая B – образ отображения Альбанезе $S \rightarrow B$, тогда дзета-функция этой поверхности равна дзета-функции прямого произведения $\mathbb{P}^1 \times B$. В работе также приводится классификация возможных дзета-функций биэллиптических поверхностей.

Библиография: 17 названий.

1. Введение. Многообразие X над конечным полем обладает большим по сравнению с другими полями набором численных инвариантов. Это, например, числа точек многообразия X над конечным расширением поля, которые объединены в дзета-функцию многообразия X . Вопрос о возможных значениях этих инвариантов для поверхностей в зависимости от их геометрии поставлен в статье [1]. В работе [2] изучен случай расслоений на коники и некоторых поверхностей дель-Пеццо. В нашей работе при $\text{char } k \neq 2, 3$ получен полный ответ для биэллиптических поверхностей. Оказывается, что если $S \rightarrow B$ – биэллиптическая поверхность над конечным полем, которая расслаивается над эллиптической кривой B , то дзета-функция этой поверхности равна дзета-функции прямого произведения $\mathbb{P}^1 \times B$.

В этом пункте приводятся уже известные результаты о дзета-функциях эллиптических кривых и вводятся основные обозначения, которые потребуются в дальнейшем. Мы будем работать над конечным полем $k = \mathbb{F}_q$ порядка $q = p^n$ при условии, что характеристика p не равна 2 или 3. Фиксируем также простое число $\ell \neq p$.

ОПРЕДЕЛЕНИЕ 1. Пусть X – многообразие над полем k ; обозначим через $\bar{X} = X \times_k \bar{k}$ – многообразие над алгебраическим замыканием поля k . Пусть N_r – число точек на $\bar{X}$, координаты которых лежат в $\mathbb{F}_{q^r}$. Тогда *дзета-функцией* многообразия X называется степенной ряд с рациональными коэффициентами

$$Z_X(t) = \exp \left(\sum_{r=1}^{\infty} \frac{N_r t^r}{r} \right).$$

Работа выполнена при поддержке Российского фонда фундаментальных исследований (гранты №№ 06-01-72550-НЦНИЛ-а, 06-01-72004-МНТИ-а и 07-01-00051-а).

Для работы с дзета-функциями очень полезны *эталные когомологии* многообразия $\bar{X}$. По определению (см. [3]) это

$$H^i(\bar{X}, \mathbb{Q}_\ell) = \varprojlim_r H^i(\bar{X}_{\text{ét}}, \mathbb{Z}/\ell^r \mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Если многообразие X собственное, то $H^i(\bar{X}, \mathbb{Q}_\ell)$ – это конечномерные пространства над $\mathbb{Q}_\ell$, тривиальные вне интервала $0 \leq i \leq 2 \dim X$. Кроме того, $H^i(\cdot, \mathbb{Q}_\ell)$ – контравариантный функтор.

ОПРЕДЕЛЕНИЕ 2. *Морфизм Фробениуса* схемы X над конечным полем $k = \mathbb{F}_q$ – это отображение $F_X: X \rightarrow X$, которое действует тривиально на точках X , а на функциях действует возведением в q -ю степень.

Существует следующая связь между дзета-функцией и действием, которое индуцирует морфизм Фробениуса на этальных когомологиях $H^i(\bar{X}, \mathbb{Q}_\ell)$ многообразия $\bar{X}$. Изначально этот факт был доказан на семинаре по алгебраической геометрии под руководством Гротендика, более доступно это доказательство изложено в книге [3].

ТЕОРЕМА 1.1. *Пусть X – гладкое собственное многообразие над конечным полем. Тогда имеет место следующее равенство формальных степенных рядов от t с коэффициентами в $\mathbb{Q}_\ell$:*

$$Z_X(t) = \prod_{i=0}^{2 \dim X} \det(1 - tF_X^* | H^i(\bar{X}, \mathbb{Q}_\ell))^{(-1)^{i+1}}.$$

В частности, дзета-функция рациональна, у ряда в правой части рациональные коэффициенты и он не зависит от ℓ .

Пусть A и B – абелевы многообразия, а $\text{Hom}(A, B)$ – группа гомоморфизмов из A в B . Группа $\text{Hom}(A, B)$ – конечнопорожденная группа без кручения. На $\text{End}(A) = \text{Hom}(A, A)$ есть структура кольца с композицией в качестве умножения. Алгебра $\text{End}^\circ(A) = \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ называется *алгеброй эндоморфизмов*.

Пусть A – абелево многообразие над полем k . Для любого натурального m обозначим через A_m ядро умножения на m в группе $A(\bar{k})$. Пусть $A[m]$ – групповая подсхема A , аннулируемая умножением на m . Таким образом, $A_m = A[m](\bar{k})$. Автоморфизм Фробениуса индуцирует на A_m действие, которое продолжается на модуль Тейта $T_\ell(A) = \varprojlim_r A_{\ell^r}$ и на

$$V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \text{Hom}(H^1(\bar{A}, \mathbb{Q}_\ell), \mathbb{Q}_\ell).$$

Если $\dim A = g$, то $T_\ell(A)$ – свободный $\mathbb{Z}_\ell$ -модуль ранга $2g$. Вейлю принадлежит следующая теорема.

ТЕОРЕМА 1.2 [4]. *Автоморфизм Фробениуса индуцирует на $V_\ell(A)$ полупростой линейный оператор $\mathbf{F}$. Его характеристический многочлен равен $f_A(t) = \deg(t - F_A)$, где $\deg$ обозначает степень изогении, а t – целое. Это унитарный многочлен степени $2g$ с целыми коэффициентами, не зависящий от выбора ℓ . Если π – его корень, то $|\pi| = \sqrt{q}$.*

Из этой теоремы следует, что на A ровно $f_A(1)$ точек, определенных над k . Если A – эллиптическая кривая, то по теореме 1.1 можно вычислить дзета-функцию $Z_A(t)$ следующим образом. Пусть

$$P_1(t) = \det(1 - t\mathbf{F}|V_\ell(A)) = t^2 f_A\left(\frac{1}{t}\right),$$

тогда

$$Z_A(t) = \frac{P_1(t)}{(1-t)(1-qt)},$$

так как на $H^0(\bar{A}, \mathbb{Q}_\ell)$ автоморфизм Фробениуса действует тривиально, а на $H^2(\bar{A}, \mathbb{Q}_\ell)$ – умножением на q .

Дзета-функция и класс изогении эллиптической кривой однозначно определяют друг друга, поэтому можно классифицировать эти классы изогении, классифицировав возможные многочлены f_A .

ТЕОРЕМА 1.3 [5]. Пусть B – эллиптическая кривая над полем k , характеристика которого не равна 2 или 3. Тогда характеристический многочлен автоморфизма Фробениуса имеет вид $f_B(t) = t^2 - bt + q$, где b – целое число, для которого $|b| \leq 2\sqrt{q}$ и которое удовлетворяет одному из следующих условий:

- 1) $(p, b) = 1$;
- 2) $b = \pm 2\sqrt{q}$ и p четно;
- 3) $b = \pm\sqrt{q}$, p четно и $p \not\equiv 1 \pmod{3}$;
- 4) $b = 0$ и либо p нечетно, либо p четно и $p \not\equiv 1 \pmod{4}$.

Из теоремы 8 статьи [6] следует, что в случае 2) алгебра эндоморфизмов кривой – центральная простая алгебра порядка 2 над $\mathbb{Q}$, у которой инварианты нетривиальны только в p и в бесконечности. В остальных случаях алгебра эндоморфизмов кривой – минимальное квадратичное расширение поля $\mathbb{Q}$, которое имеет вид $\mathbb{Q}[t]/(f_B(t))$.

В силу замечания, сделанного после теоремы 1.2, группа k -точек эллиптической кривой имеет порядок $f_B(1) = q - b + 1$. Обратно, $b = q - |B(k)| + 1$, поэтому две кривые изогенны тогда и только тогда, когда на них одинаковое количество k -точек. Следующая теорема дает классификацию возможных групп k -точек у кривых в данном классе изогении.

ТЕОРЕМА 1.4 [7]. Пусть характеристика поля k не равна 2 или 3. Рассмотрим все эллиптические кривые в классе изогении с характеристическим многочленом автоморфизма Фробениуса $f(t) = t^2 - bt + q$. Группы k -точек таких кривых G имеют порядок $N = q - b + 1$. Явный вид этих групп таков:

- 1) если $(p, b) = 1$ и $|b| \leq 2\sqrt{q}$, то $G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z}$, где m_2 делит m_1 и $b - 2$; все такие группы реализуются как группы k -точек эллиптической кривой из данного класса изогении;
- 2) если $b = \pm 2\sqrt{q}$, p четно, то $G \cong (\mathbb{Z}/m\mathbb{Z})^2$, где $m = \sqrt{q} \pm 1$;
- 3) если $b = \pm\sqrt{q}$, p четно, $p \not\equiv 1 \pmod{3}$, то $G \cong \mathbb{Z}/N\mathbb{Z}$;
- 4) если $b = 0$ и либо p нечетно и $p \not\equiv 3 \pmod{4}$, либо p четно и $p \not\equiv 1 \pmod{4}$, то $G \cong \mathbb{Z}/N\mathbb{Z}$;
- 5) Если $b = 0$, p нечетно и $p \equiv 3 \pmod{4}$, то либо $G \cong \mathbb{Z}/N\mathbb{Z}$, либо $G \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; оба варианта реализуются.

В частности, во всех классах изогении, кроме 2), существует кривая с циклической группой k -точек.

Эта теорема была позже независимо доказана в работах [8] и [9], которые опираются на [10].

2. Основные теоремы. Бомбьери и Мамфорд доказали классические результаты Энриквеса о классификации алгебраических поверхностей над алгебраически замкнутым полем произвольной характеристики [11]. Нам нужно перенести эти результаты на биэллиптические поверхности над конечным полем.

ОПРЕДЕЛЕНИЕ 3. *Биэллиптической поверхностью* называется минимальная алгебраическая поверхность S размерности Кодаиры нуль с параметрами $h^1(S, \mathcal{O}_S) = 1$ и $h^0(S, \mathcal{O}_S(K_S)) = 0$.

ЛЕММА 2.1. *Пусть гладкая проективная поверхность S минимальна над полем k и размерность Кодаиры $\kappa(S) \geq 0$, тогда $\bar{S}$ минимальна над $\bar{k}$.*

ДОКАЗАТЕЛЬСТВО. Пусть $\bar{S}$ не минимальна. Поскольку $\kappa(\bar{S}) \geq 0$, минимальная модель Y поверхности $\bar{S}$ единственна с точностью до изоморфизма, в частности, любой бирациональный автоморфизм Y будет изоморфизмом [12]. Рассмотрим бирациональное отображение $\bar{S} \rightarrow Y$ в минимальную модель. Тогда двойственный граф исключительных кривых этого морфизма – это одно или несколько деревьев, причем вершины этих деревьев соответствуют кривым с индексом самопересечения -1 . Среди этих деревьев не может быть дерева из двух вершин, так как стягивая кривые, соответствующие этим вершинам, мы получим два разных морфизма в минимальную модель, что дает нетривиальный бирациональный автоморфизм. Отсюда следует, что кривые, соответствующие вершинам дерева, не пересекаются. Поскольку только у таких кривых индекс самопересечения равен -1 , группа Галуа переводит вершины дерева в вершины. Поэтому всю орбиту Галуа можно стянуть над полем k [13; III.4.8], а это противоречит минимальности S .

Из этой леммы и результатов Бомбьери и Мамфорда [11], [12] следует, что биэллиптические поверхности минимальны над $\bar{k}$ и для таких поверхностей $12K_S = 0$, эйлерова характеристика $\chi(S) = \sum (-1)^i b_i$ равна нулю и $b_1 = 2h^1(S, \mathcal{O}_S) = 2$, где $b_i = h^i(\bar{S}, \mathbb{Q}_\ell)$ – числа Бетти.

Для многообразия X над конечным полем можно определить *многообразие Альбанезе* A как абелево многообразие, двойственное к многообразию Пикара $\text{Pic}^0(X)_{\text{red}}$. Тогда, как и в характеристике нуль, существует отображение $a: X \rightarrow A$, обладающее следующим универсальным свойством: для любого отображения $a': X \rightarrow A'$ в абелево многообразие существует такое отображение $h: A \rightarrow A'$, что $a' = h \circ a$. Размерность многообразия Альбанезе равна $h^1(X, \mathcal{O}_X)$ (см. [12]). В частности, многообразие Альбанезе биэллиптической поверхности – эллиптическая кривая.

Нам потребуется следующая конструкция [14].

ТЕОРЕМА 2.2. *Пусть $\mathcal{L}$ – обратимый пучок на поверхности S , обладающий свойством $\mathcal{L}^{\otimes n} \cong \mathcal{O}_S$, где число n должно быть минимальным числом, обладающим этим свойством. Тогда существует связная поверхность A и неразветвленное накрытие $p: A \rightarrow S$ степени n , для которого $p^*\mathcal{L} \cong \mathcal{O}_A$.*

Поверхность A можно определить как относительный спектр над S пучка алгебр $\mathfrak{A} = \bigoplus_{i=0}^{n-1} \mathcal{L}^{-i}$.

Мы будем использовать этот результат, когда $\mathcal{L} = \mathcal{O}_S(K_S)$, а поверхность S – биэллиптическая. В этом случае p называется *каноническим накрытием*. Заметим, что $\mathcal{O}_A(K_A) = p^* \mathcal{O}_S(K_S) \cong \mathcal{O}_A$, поэтому $K_A = 0$. Эйлерова характеристика $\chi(A) = n\chi(S) = 0$, следовательно, $\bar{A}$ – абелева поверхность [12].

Пусть G – конечная групповая схема над k и ее ранг взаимно прост с $\text{char } k$. Тогда G однозначно определяется группой $G(\bar{k})$ и действием автоморфизма Фробениуса F_G на ней. Заметим, что действие Фробениуса действует автоморфизмом группы $G(\bar{k})$. В частности, если $G(\bar{k})$ – линейное пространство над $\mathbb{F}_r$, то действие Фробениуса линейно. Групповую схему, для которой $G(\bar{k}) \cong G(k) \cong \mathbb{Z}/m\mathbb{Z}$, т.е. действие Фробениуса тривиально, будем обозначать просто $\mathbb{Z}/m\mathbb{Z}$. Аналогично, действие групповой схемы G на многообразии X однозначно определено при помощи действия группы $G(\bar{k})$ на многообразии $\bar{X}$, согласованного с действием Фробениуса.

Теперь можно доказать, что теорема классификации биэллиптических поверхностей над произвольным полем, характеристика которого не равна 2 или 3, почти не изменяется по сравнению с алгебраически замкнутым полем. Случай, когда $\text{char } k = 2$ или 3, значительно сложнее и здесь не рассматривается.

ТЕОРЕМА 2.3. Пусть S – биэллиптическая поверхность над конечным полем k , характеристика которого не равна 2 или 3. Тогда $S \cong (B_1 \times B_0)/G$, где B_i – эллиптические кривые, а $G \subset B_1$ – групповая подсхема, которая действует на B_0 без ядра, т.е. морфизм $\varphi: G \rightarrow \text{Aut}(B_0)$ инъективен. Кривая B_1 может быть любой, а для B_0 и G есть список возможных вариантов:

- (a₁) кривая B_0 – любая, а $G(\bar{k}) \cong \mathbb{Z}/2\mathbb{Z} \cong \langle a \rangle_2$, где a действует на B_0 как инволюция $x \mapsto -x$;
- (a₂) кривая B_0 – любая, а $G(\bar{k}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ с образующими a и t_c , где a действует на B_0 как инволюция $x \mapsto -x$, а t_c – сдвиг на точку $c \in B_0[2](\bar{k})$;
- (b₁) кривая B_0 допускает автоморфизм ω порядка 3, сохраняющий нуль, а $G(\bar{k}) \cong \mathbb{Z}/3\mathbb{Z} \cong \langle \omega \rangle_3$; в этом случае $j(\bar{B}_0) = 0$;
- (b₂) кривая B_0 допускает автоморфизм ω порядка 3, сохраняющий нуль, а $G(\bar{k}) \cong (\mathbb{Z}/3\mathbb{Z})^2 \cong \langle \omega \rangle_3 \times \langle t_c \rangle_3$, где t_c – сдвиг на точку $c \in B_0[3](\bar{k})$, для которой $\omega(c) = c$; в этом случае также $j(\bar{B}_0) = 0$;
- (c₁) кривая B_0 допускает автоморфизм i порядка 4, сохраняющий нуль, а $G(\bar{k}) \cong \mathbb{Z}/4\mathbb{Z} \cong \langle i \rangle_4$; в этом случае $j(\bar{B}_0) = 1728$;
- (c₂) кривая B_0 допускает автоморфизм i порядка 4, сохраняющий нуль, а $G(\bar{k}) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle i \rangle_4 \times \langle t_c \rangle_2$, где t_c – сдвиг на точку $c \in B_0[2](\bar{k})$, для которой $i(c) = c$; в этом случае $j(\bar{B}_0) = 1728$;
- (d) кривая B_0 допускает автоморфизм ω порядка 3, сохраняющий нуль, а $G(\bar{k}) \cong \mathbb{Z}/6\mathbb{Z} \cong \langle g \rangle_6$, где $\varphi(g)(x) = -\omega(x)$; в этом случае $j(\bar{B}_0) = 0$.

ДОКАЗАТЕЛЬСТВО. Известно, что эта теорема верна, если поле k алгебраически замкнуто [11], [12]. Пусть $p: A \rightarrow S$ – каноническое накрытие поверхности S . Тогда поверхность A абелева, так как $\bar{A}$ абелева и над конечным полем у абелевых многообразий нет форм без k -точек. Пусть $a: S \rightarrow B$ – отображение Альбанезе, тогда B будет эллиптической кривой по той же причине. Отображение $a \circ p$ будет гомоморфизмом абелевых многообразий с точностью до сдвига, следовательно, имеет смысл говорить о его ядре. Обозначим связную компоненту ядра $a \circ p$ через B_0 . Получаем, что существует изогения $B \times B_0 \rightarrow A$. Обозначим через B_1 образ B при этой

изогении. Тогда изогения $B_1 \times B_0 \rightarrow A$ будет изоморфизмом над $\bar{k}$, так как наша теорема верна над полем $\bar{k}$, т.е. $B_1 \times B_0 \cong A$. Остальное следует из классификации над замкнутым полем.

Из доказательства этой теоремы следует, что отображение Альбанезе устроено следующим образом:

$$S \cong (B_1 \times B_0)/G \rightarrow B_1/G \cong B.$$

ОПРЕДЕЛЕНИЕ 4. Пусть $\{M_n\}$ – проективная система конечных ℓ -примарных абелевых групп с действием конечной группы G . Тогда для векторного пространства $M = (\varprojlim_n M_n) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, на которое действует G , *непрерывные когомологии Галуа* определяются как

$$H_{\text{cont}}^p(G, M) = (\varprojlim_n H^p(G, M_n)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

ЛЕММА 2.4. Пусть конечная группа G , порядок которой взаимно прост с ℓ , действует на проективной системе $\{M_n\}$ ℓ -примарных абелевых групп и, следовательно, на пространстве

$$M = (\varprojlim_n M_n) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Тогда $H_{\text{cont}}^0(G, M) = M^G$, а остальные когомологии тривиальны.

ДОКАЗАТЕЛЬСТВО. Композиция отображений

$$H^r(G, M_n) \xrightarrow{\text{res}} H^r(\{1\}, M_n) \xrightarrow{\text{inf}} H^r(G, M_n)$$

будет умножением на порядок группы G (см. [15; I.2.4]) и, следовательно, изоморфизмом. Заметим, что $H^r(\{1\}, M_n) = 0$ при $r > 0$. При $r = 0$ надо проверить, что функтор проективного предела перестановочен со взятием инвариантов. Это следует из того, что $\varprojlim$ точен на проективных системах конечных групп [16; II.9.1]. Лемма доказана.

ТЕОРЕМА 2.5. Пусть $S \cong (B_1 \times B_0)/G$ – биэллиптическая поверхность над конечным полем k , характеристика которого не равна 2 или 3, тогда имеет место изоморфизм модулей над группой Галуа $\text{Gal}(\bar{k}/k)$:

$$\begin{aligned} H^1(\bar{S}, \mathbb{Q}_\ell) &\cong H^1(\bar{B}_1, \mathbb{Q}_\ell), \\ H^2(\bar{S}, \mathbb{Q}_\ell) &\cong H^2(\bar{B}_1, \mathbb{Q}_\ell) \oplus H^2(\bar{B}_0, \mathbb{Q}_\ell), \\ H^3(\bar{S}, \mathbb{Q}_\ell) &\cong H^1(\bar{B}_1, \mathbb{Q}_\ell) \otimes H^2(\bar{B}_0, \mathbb{Q}_\ell). \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. По теореме 2.3 B_1/G – эллиптическая кривая, изогенная B_1 . Спектральная последовательность Хохшильда–Серра для накрытия $\bar{B}_1 \rightarrow \bar{B}_1/\bar{G}$ имеет вид

$$E_2^{p,q} = H_{\text{cont}}^p(G(\bar{k}), H^q(\bar{B}_1, \mathbb{Q}_\ell)) \Rightarrow H^{p+q}(\bar{B}_1/\bar{G}, \mathbb{Q}_\ell).$$

Если $\ell \neq 2, 3$, то по теореме 2.3 порядок группы $G(\bar{k})$ взаимно прост с ℓ , значит, по предыдущей лемме эта спектральная последовательность вырождается во втором члене, что дает изоморфизмы для $i = 0, 1, 2$:

$$H^i(\bar{B}_1, \mathbb{Q}_\ell)^{G(\bar{k})} \cong H^i(\bar{B}_1/\bar{G}, \mathbb{Q}_\ell).$$

Сравнивая размерности получаем, что действие группы $G(\bar{k})$ на $H^i(\bar{B}_1, \mathbb{Q}_\ell)$ тривиально.

Отображение $\bar{B}_1 \times \bar{B}_0 \rightarrow \bar{S}$ – накрытие Галуа, так как его степень равна порядку группы $G(\bar{k})$ и $G(\bar{k})$ действует без неподвижных точек по теореме 2.3. Поэтому можно снова применить спектральную последовательность Хохшильда–Серра:

$$E_2^{p,q} = H_{\text{cont}}^p(G(\bar{k}), H^q(\bar{B}_1 \times \bar{B}_0, \mathbb{Q}_\ell)) \Rightarrow H^{p+q}(\bar{S}, \mathbb{Q}_\ell).$$

Она тоже вырождается во втором члене, и по формуле Кюннета

$$\begin{aligned} H^0(\bar{S}, \mathbb{Q}_\ell) &\cong (H^0(\bar{B}_1, \mathbb{Q}_\ell) \otimes H^0(\bar{B}_0, \mathbb{Q}_\ell))^{G(\bar{k})}, \\ H^4(\bar{S}, \mathbb{Q}_\ell) &\cong (H^2(\bar{B}_1, \mathbb{Q}_\ell) \otimes H^2(\bar{B}_0, \mathbb{Q}_\ell))^{G(\bar{k})}. \end{aligned}$$

Сравнивая размерности в этих формулах, получаем, что действие группы $G(\bar{k})$ на нулевых и вторых когомологиях кривой B_0 тривиально. Поскольку нулевые когомологии являются тривиальными модулями и над группой Галуа, а действие Фробениуса согласовано с морфизмами в спектральной последовательности Хохшильда–Серра, формула Кюннета дает следующие изоморфизмы модулей над $\text{Gal}(\bar{k}/k)$:

$$\begin{aligned} H^1(\bar{S}, \mathbb{Q}_\ell) &\cong (H^1(\bar{B}_1, \mathbb{Q}_\ell) \oplus H^1(\bar{B}_0, \mathbb{Q}_\ell))^{G(\bar{k})}, \\ H^2(\bar{S}, \mathbb{Q}_\ell) &\cong (H^2(\bar{B}_1, \mathbb{Q}_\ell) \oplus H^1(\bar{B}_1, \mathbb{Q}_\ell) \otimes H^1(\bar{B}_0, \mathbb{Q}_\ell) \oplus H^2(\bar{B}_0, \mathbb{Q}_\ell))^{G(\bar{k})}, \\ H^3(\bar{S}, \mathbb{Q}_\ell) &\cong (H^1(\bar{B}_1, \mathbb{Q}_\ell) \otimes H^2(\bar{B}_0, \mathbb{Q}_\ell) \oplus H^2(\bar{B}_1, \mathbb{Q}_\ell) \otimes H^1(\bar{B}_0, \mathbb{Q}_\ell))^{G(\bar{k})}. \end{aligned}$$

Из того, что $b_1 = h^1(\bar{S}, \mathbb{Q}_\ell) = 2$, и из формулы для $H^1(\bar{S}, \mathbb{Q}_\ell)$ получаем, что

$$H^1(\bar{B}_0, \mathbb{Q}_\ell)^{G(\bar{k})} = 0.$$

Отсюда и из последних формул сразу следует справедливость теоремы.

Напомним, что если характеристический многочлен автоморфизма Фробениуса кривой B_1 равен $f(t)$, то $t^2 f(1/t) = P_1(t) = \det(1 - t\mathbf{F}|H^1(X, \mathbb{Q}_\ell))$. Кроме того (см. [2]),

$$Z_{\mathbb{P}^1 \times B}(t) = Z_B(t)Z_B(qt).$$

Теперь из теоремы 1.1 следует такой результат.

СЛЕДСТВИЕ 2.6. *Если характеристический многочлен автоморфизма Фробениуса кривой B_1 равен $f(t) = t^2 - bt + q$, и $P_1(t) = t^2 f(1/t)$, то дзета-функция поверхности S имеет вид*

$$Z_S(t) = \frac{P_1(t)P_1(qt)}{(1-t)(1-qt)^2(1-q^2t)}. \quad (1)$$

В частности, дзета-функция поверхности S равна дзета-функции прямого произведения $\mathbb{P}^1 \times B$, где кривая $B \cong B_1/G$ – многообразие Альбанезе поверхности S .

ЗАМЕЧАНИЕ 1. На самом деле, мы доказали следующее более общее утверждение. Пусть $S \rightarrow C$ – эллиптическая поверхность над кривой C , которая тривиализуется над этальным накрытием $\tilde{C}$ кривой C , т.е. $S \times_C \tilde{C} \cong \tilde{C} \times B_0$, где B_0 – эллиптическая кривая. Тогда дзета-функция поверхности S равна дзета-функции произведения $C \times \mathbb{P}^1$.

ТАБЛИЦА

	Достаточные условия	Необходимые условия
(a_1)	2 делит $q - b + 1$	2 делит $q - b + 1$
(a_2)	4 делит $1 - b + q$	4 делит $1 - b + q$
$(b_1), p \equiv 1 \pmod{3}$	3 делит $1 - b + q$	3 делит $1 - b + q$
$(b_1), p \equiv 2 \pmod{3}$	3 делит $1 - b + q$	—
$(b_2), p \equiv 1 \pmod{3}$	9 делит $1 - b + q$	9 делит $1 - b + q$
$(b_2), p \equiv 2 \pmod{3}$	9 делит $1 - b + q, n$ четно	—
$(c_1), b \neq \pm 2\sqrt{q},$ $p \equiv 1 \pmod{4}$	4 делит $q - b + 1$	4 делит $q - b + 1$
$(c_1), b \neq \pm 2\sqrt{q},$ $p \equiv 3 \pmod{4}$	4 делит $q - b + 1$ n четно	2 делит $q - b + 1$
$(c_1), b = \pm 2\sqrt{q}$	16 делит $q - b + 1$	4 делит $q - b + 1$
$(c_2), b \neq \pm 2\sqrt{q},$ $p \equiv 1 \pmod{4}$	8 делит $q - b + 1$	8 делит $q - b + 1$
$(c_2), b \neq \pm 2\sqrt{q},$ $p \equiv 3 \pmod{4}$	8 делит $q - b + 1$ n четно	4 делит $q - b + 1$
$(c_2), b = \pm 2\sqrt{q}$	16 делит $q - b + 1$	4 делит $q - b + 1$
$(d), p \equiv 1 \pmod{3}$	6 делит $1 - b + q$	6 делит $1 - b + q$
$(d), p \equiv 2 \pmod{3}$	6 делит $1 - b + q, n$ четно	—

Чтобы классифицировать все возможные дзета-функции биэллиптических поверхностей, осталось выяснить, в каких классах изогении существует кривая B_1 , содержащая одну из групповых схем G , перечисленных в теореме 2.3, и существуют ли кривые B_0 с указанным действием группы G . Сейчас мы сформулируем ответ на этот вопрос, а докажем его в следующем пункте.

ТЕОРЕМА 2.7. Пусть $f(t) = t^2 - bt + q$ — многочлен из теоремы 1.3. Необходимые и достаточные условия того, что существует биэллиптическая поверхность $S = (B_1 \times B_0)/G$ такая, что $f_{B_1} = f$, а G и B_0 такие, как в теореме 2.3, перечислены в таблице.

Эта теорема дает классификацию всех биэллиптических поверхностей типа (a_i) , поверхностей типа (b_i) и (d) при условии $p \equiv 1 \pmod{3}$, и поверхностей типа (c_i) при условии $p \equiv 1 \pmod{4}$. В частности, мы знаем их дзета-функции.

3. Доказательство теоремы 2.7. Схема доказательства такова: сначала мы найдем необходимые и достаточные условия, при которых у кривой B_0 может быть автоморфизм степени 3 или 4 над полем k . Используя эту информацию, уже легко построить биэллиптические поверхности S как фактор $(B_1 \times B_0)/G$.

ЛЕММА 3.1. Пусть эллиптическая кривая B допускает автоморфизм i порядка 4 над k . Тогда характеристический многочлен автоморфизма Фробениуса кривой B равен $f_B(t) = t^2 - 2dt + q$, где d — целое число, для которого выполняется одно из следующих условий:

- 1) $(p, d) = 1$, и $q - d^2$ — полный квадрат; в этом случае $p \equiv 1 \pmod{4}$;

2) $d = 0$ или $d = \pm\sqrt{q}$; в этом случае $p \equiv 3 \pmod{4}$, и n четно.

Обратно, для каждого d , удовлетворяющего одному из условий 1), 2), существует кривая B с характеристическим многочленом автоморфизма Фробениуса $f_B(t) = t^2 - 2dt + q$ и автоморфизмом i порядка 4, который определен над k .

ДОКАЗАТЕЛЬСТВО. Пусть $i \in \text{End}^\circ(B)$. Если алгебра эндоморфизмов кривой B – мнимое квадратичное расширение $\mathbb{Q}$, то автоморфизм Фробениуса имеет вид $d + ai$, где $q = a^2 + d^2$ и $a \neq 0$. Поэтому его след равен $2d$ и, значит, $f_B(t) = t^2 - 2dt + q$. Если $d \neq 0$, то по теореме 1.3 должно быть $(p, d) = 1$, а разложить q в сумму двух квадратов можно, только если $p \equiv 1 \pmod{4}$. Если $d = 0$, то $a = \pm\sqrt{q}$, т.е. n четно, следовательно, $p \equiv 3 \pmod{4}$ по теореме 1.3. Если же алгебра эндоморфизмов некоммутативна, то она единственная кватернионная алгебра над полем $\mathbb{Q}$, у которой инварианты нетривиальны в p и в бесконечности. Она содержит $\mathbb{Q}(i)$, следовательно, ее можно задать образующими i, j, k и соотношениями:

$$i^2 = -1, \quad j^2 = -p, \quad ij = -ji = k,$$

причем $p \equiv 3 \pmod{4}$. По теореме 1.3 получаем, что $d = \pm\sqrt{q}$ и n четно.

Докажем, что кривая с данным характеристическим многочленом автоморфизма Фробениуса существует. Если $(p, d) = 1$, и $q - d^2$ – полный квадрат, то

$$\text{End}^\circ(B) \cong \mathbb{Q}[t]/(t^2 - 2dt + q) \cong \mathbb{Q}(i), \quad \text{где } i = \frac{t - d}{a},$$

а если $d = 0$ и n четно, то

$$\text{End}^\circ(B) \cong \mathbb{Q}[t]/(t^2 + q) \cong \mathbb{Q}(i).$$

Теперь по [5; теорема 3.13] существует кривая B_0 , изогенная B , у которой кольцо эндоморфизмов $\mathbb{Z}[i]$ – кольцо целых $\text{End}^\circ(B)$. Если же $d = \pm\sqrt{q}$, то $\text{End}^\circ(B)$ некоммутативна. Возьмем максимальный порядок, содержащий i , и применим [5; теорема 3.13].

ЛЕММА 3.2. Пусть эллиптическая кривая B допускает автоморфизм ω порядка 3 над k . Тогда характеристический многочлен автоморфизма Фробениуса кривой B имеет вид

- 1) либо $f_B(t) = t^2 - (2a - c)t + q$, где a и c – целые числа, для которых $(p, c) = 1$ и $q = a^2 + c^2 - ac$; в этом случае $p \equiv 1 \pmod{3}$;
- 2) либо $f_B(t) = t^2 \pm \sqrt{q}t + q$ или $f_B(t) = t^2 \pm 2\sqrt{q}t + q$; в этом случае $p \equiv 2 \pmod{3}$ и n четно.

Обратно, для каждого $f_B(t)$, удовлетворяющего одному из условий 1), 2), существует кривая B с таким многочленом автоморфизма Фробениуса и автоморфизмом ω порядка 3, который определен над k .

ДОКАЗАТЕЛЬСТВО. Снова разберем два случая. Если алгебра эндоморфизмов кривой B – мнимое квадратичное расширение поля $\mathbb{Q}$, то автоморфизм Фробениуса имеет вид $a + c\omega$, где $q = a^2 + c^2 - ac$, и $c \neq 0$. Поэтому его след равен $2a - c$ и, значит, $f_B(t) = t^2 - (2a - c)t + q$. Рассмотрим возможные случаи из теоремы 1.3. В случае 1), если $(p, 2a - c) = 1$, то и $(p, c) = (p, a) = 1$, но $4q = (2a - c)^2 + 3c^2$, следовательно, -3 – квадрат по модулю p , а это равносильно тому, что $p \equiv 1 \pmod{3}$. В случае 3),

из того, что $2a - c = \pm\sqrt{q}$, сразу получаем, что $p \equiv 2 \pmod{3}$, и n четно. Наконец, случай 5) невозможен, так как из того, что $2a - c = 0$, следует, что $4q = 3c^2$. Пусть теперь алгебра эндоморфизмов некоммутативна, тогда она – единственная кватернионная алгебра над полем $\mathbb{Q}$, у которой инварианты нетривиальны в p и в бесконечности. Она содержит $\mathbb{Q}(\omega)$, следовательно, ее можно задать образующими I, J, K и соотношениями

$$I^2 = -3, \quad J^2 = -p, \quad IJ = -JI = K,$$

причем $p \equiv 2 \pmod{3}$. По теореме 1.3 получаем, что $f_B(t) = t^2 \pm 2\sqrt{q}t + q$ и n четно.

Докажем, что кривая с данным характеристическим многочленом автоморфизма Фробениуса существует. Если $(p, c) = 1$, и $q = a^2 + c^2 - ac$, то

$$\text{End}^\circ(B) \cong \mathbb{Q}[t]/(t^2 - (2a - c)t + q) \cong \mathbb{Q}(\omega), \quad \text{где } \omega = \frac{t - a}{c},$$

а если $f_B(t) = t^2 \pm \sqrt{q}t + q$, то сразу получаем

$$\text{End}^\circ(B) \cong \mathbb{Q}(\omega), \quad \text{где } \omega = \pm \frac{t}{\sqrt{q}}.$$

По [5; теорема 3.13] существует кривая B_0 , изогенная B , у которой кольцо эндоморфизмов $\mathbb{Z}[\omega]$. Если же $f_B(t) = t^2 \pm 2\sqrt{q}t + q$, то $\text{End}^\circ(B)$ некоммутативна. Возьмем максимальный порядок, содержащий $\omega = -1/2(1 + I)$, и применим [5; теорема 3.13].

ЛЕММА 3.3. *Если эллиптическая кривая B допускает автоморфизм i порядка 4 над $\bar{k}$, который не определен над k , то $p \equiv 3 \pmod{4}$. Если B допускает автоморфизм ω порядка 3 над $\bar{k}$, который не определен над k , то $p \equiv 2 \pmod{3}$.*

ДОКАЗАТЕЛЬСТВО. Если автоморфизм кривой B не определен над k , то он определен над некоторым конечным расширением K степени m . Пусть $\text{End}_K^\circ(B)$ – алгебра эндоморфизмов, определенных над K . Согласно замечанию после теоремы 1.3 размерности алгебр $\text{End}_K^\circ(B)$ и $\text{End}^\circ(B)$ могут равняться 2 или 4. Из того, что $\text{End}(B) \subset \text{End}_K(B)$, следует, что если $\text{End}_K^\circ(B) \neq \text{End}^\circ(B)$, то $\text{End}^\circ(B)$ коммутативна, а $\text{End}_K^\circ(B)$ некоммутативна. В лемме 3.1 мы доказали, что такое возможно только при $p \equiv 3 \pmod{4}$ для автоморфизма порядка 4, а в лемме 3.2 – только при $p \equiv 2 \pmod{3}$ для автоморфизма порядка 3.

Зафиксируем характеристический многочлен $f(t)$ автоморфизма Фробениуса эллиптической кривой B_1 . Обозначим через $G[r]$ ядро умножения на r в групповой схеме G .

ЛЕММА 3.4. *Пусть $r = 2$ или 3, а B_1 и G такие, как в теореме 2.3. Если $p \equiv 1 \pmod{r}$ и $G[r] \cong B_1[r]$, то $G[r] \cong (\mathbb{Z}/r\mathbb{Z})^2$.*

ДОКАЗАТЕЛЬСТВО. По теореме 1.2 на двумерном линейном пространстве $B_1[r](\bar{k})$ над полем $\mathbb{F}_r$ автоморфизм Фробениуса действует линейно с характеристическим многочленом $f(t) \pmod{r}$. Положим

$$g = i^2 = -1, \quad \text{если } r = 2, \quad \text{и} \quad g = \omega, \quad \text{если } r = 3.$$

Из двух предыдущих лемм следует, что групповая подсхема $\langle g \rangle_r \subset G$, порожденная g , изоморфна $\mathbb{Z}/r\mathbb{Z}$, следовательно, одно из собственных значений равно 1. Так как $q \equiv 1 \pmod r$, второе собственное значение этого действия тоже 1. Заметим теперь, что по теореме 2.3 $G[r](\bar{k}) \cong \langle g \rangle_r \oplus \langle t_c \rangle_r$ и оба слагаемых инвариантны относительно действия Фробениуса. Таким образом, действие Фробениуса тривиально на $B_1[r](\bar{k})$.

ЛЕММА 3.5. Пусть $q \equiv 1 \pmod r$, где r – простое число, не равное $\text{char } k$, и B – эллиптическая кривая, у которой алгебра эндоморфизмов коммутативна, а характеристический многочлен автоморфизма Фробениуса равен $f(t) = t^2 - bt + q$. Пусть $m > 1$ – максимально число, для которого r^m делит $1 - b + q$. Тогда существует изогенная B кривая, содержащая r -примарную групповую подсхему $\mathbb{Z}/r^{m-1}\mathbb{Z} \oplus \mathbb{Z}/r\mathbb{Z}$.

ДОКАЗАТЕЛЬСТВО. Заметим, что так как r делит $f(1) = q - b + 1$, то $b = q + 1 - f(1) \equiv 2 \pmod r$, т.е. r делит $b - 2$. Теперь нужную нам кривую в данном классе изогении можно найти по теореме 1.4. Действительно, в случае 1) можно взять $m_2 = r$, а $m_1 = N/r$. Легко проверить, что случаи 3) и 4) невозможны из-за того, что r^2 делит $1 - b + q$. Наконец, в случае 5) получаем, что так как r делит $b - 2$, то $r = 2$, следовательно, искомая кривая существует.

Перейдем к доказательству теоремы 2.7. Вначале докажем достаточные условия.

- (a₁) Выберем B_1 . Так как 2 делит $q - b + 1 = |B_1(k)|$, получаем, что $B_1[2](k)$ содержит некоторую подсхему $G \cong \mathbb{Z}/2\mathbb{Z}$. В качестве B_0 можно взять любую кривую.
- (a₂) Так как 4 делит $q - b + 1$, то по лемме 3.5 и теореме 1.4, 2) существует кривая B_1 , которая содержит подсхему $G \cong (\mathbb{Z}/2\mathbb{Z})^2$. Возьмем теперь $B_0 = B_1$.
- (b₁) Так как 3 делит $q - b + 1$, то на любой кривой B_1 с таким количеством точек существует подсхема $G \cong \mathbb{Z}/3\mathbb{Z}$. Если $p \equiv 1 \pmod 3$, то существуют такие целые a и c , что $q = a^2 + c^2 - ac$ и $(p, c) = 1$. Теперь по лемме 3.2, 1) существует кривая B_0 с автоморфизмом ω порядка 3. Если же $p \equiv 2 \pmod 3$ и n четно, то возьмем любую кривую из случая 2) леммы 3.2.
- (b₂) Так как 9 делит $q - b + 1$, то по лемме 3.5 и теореме 1.4, 2) существует кривая B_1 , которая содержит подсхему $G \cong (\mathbb{Z}/3\mathbb{Z})^2$. Выберем теперь кривую B_0 как и в предыдущем случае. Заметим, что коэффициент при t в каждом из многочленов $f_B(t)$ леммы 3.2 не делится на 3, поэтому можно так выбрать знаки у чисел a , c и $\sqrt{q}$ соответственно, что 3 будет делить $f_B(1)$. Автоморфизм ω индуцирует на $B_0[3](\bar{k})$ линейный оператор с характеристическим многочленом $t^3 - 1 \equiv (t - 1)^3 \pmod 3$. Этот оператор коммутирует с F_{B_0} , поэтому у них есть общий инвариантный вектор.
- (c₁) Если 4 делит $q - b + 1$ и $b \neq \pm 2\sqrt{q}$, то по теореме 1.4 существует кривая B_1 с циклической группой k -точек; эта кривая содержит подсхему $G \cong \mathbb{Z}/4\mathbb{Z}$. Если 16 делит $q - b + 1$ и $b = \pm 2\sqrt{q}$, то любая кривая B_1 из этого класса изогении содержит $\mathbb{Z}/4\mathbb{Z}$. Если $p \equiv 1 \pmod 4$, то существуют такие целые d и a , что $q = d^2 + a^2$ и $(p, d) = 1$. Следовательно, по лемме 3.1, 1) существует кривая B_0 с автоморфизмом порядка 4, для которой $f_{B_0} = t^2 - 2dt + q$. Если $p \equiv 3 \pmod 4$ и n четно, то можно выбрать любую кривую B_0 с автоморфизмом порядка 4 по лемме 3.1, 2).

- (c_2) Так как 8 делит $q-b+1$, то по лемме 3.5 и теореме 1.4, 2) существует кривая B_1 , которая содержит подсхему $G \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Выберем кривую B_0 так же, как и в предыдущем случае, тогда аналогично случаю (b_2) на ней есть точка порядка 2, инвариантная относительно i .
- (d) Из того, что 6 делит $q-b+1$, следует, что на любой кривой B_1 с таким количеством точек существует подсхема $G \cong \mathbb{Z}/6\mathbb{Z}$. Как и раньше кривая B_0 с автоморфизмом порядка 3 существует, если $p \equiv 1 \pmod{3}$.

Теперь определим $S = (B_1 \times B_0)/G$. Докажем, что у каждой точки поверхности $B_1 \times B_0$ существует G -инвариантная окрестность. Пусть $x \in B_1$ и $y \in B_0$, существуют G -инвариантные окрестности этих точек $U \subset B_1$ и $V \subset B_0$ (например, можно взять дополнение к орбите любой точки, не лежащей в орбите x), тогда $U \times V \subset B_1 \times B_0$ — G -инвариантная окрестность точки $(x, y) \in B_1 \times B_0$. Таким образом, фактор существует по теореме [17; 12.1]. Так как над $\bar{k}$ поверхность $S = (B_1 \times B_0)/G$ целая и гладкая, она будет целой и гладкой и над k .

Докажем необходимые условия. В случае (a_1) утверждение очевидно, так как $G \cong \mathbb{Z}/2\mathbb{Z} \subset B_1$, а в случае (a_2) из леммы 3.4 следует, что $(\mathbb{Z}/2\mathbb{Z})^2 \subset B_1$. В случаях (b_1), (b_2) и (d) у кривой B_0 есть автоморфизм ω порядка три, следовательно, по лемме 3.3 при $p \equiv 1 \pmod{3}$ он определен над k . Так как $\omega \in G \subset B_1$, то 3 делит $|B_1(k)| = q-b+1$. По лемме 3.4 в случае (b_2) групповая схема G содержит $(\mathbb{Z}/3\mathbb{Z})^2$, поэтому 9 делит $q-b+1$. Наконец, в случае (d) число 2 также делит $q-b+1$. В случаях (c_i) при $p \equiv 1 \pmod{4}$ автоморфизм i кривой B_0 определен над k лемме 3.3, и из того, что $i \in G \subset B_1$, следует, что 4 делит $q-b+1$. Более того, по лемме 3.4 в случае (c_2) получаем, что G содержит $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, следовательно, 8 делит $q-b+1$. Если $p \equiv 3 \pmod{4}$, то $-1 = i^2$ определен над k , поэтому аналогично предыдущему 2 делит $q-b+1$ в случае (c_1), и 4 делит $q-b+1$ в случае (c_2). Теорема доказана.

Автор благодарит М. А. Цфасмана и Д. Ваклэра за интерес к работе и ценные комментарии. Автор также признателен рецензенту за исправление ряда неточностей и советы по оформлению текста в целом.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] M. A. Tsfasman, "Nombre de points des surfaces sur un corps fini", *Arithmetic, Geometry, and Coding Theory* (Luminy, 1993), Walter de Gruyter, Berlin, 1996, 209–224.
- [2] S. Rybakov, "Zeta functions of conic bundles and Del Pezzo surfaces of degree 4 over finite fields", *Mosc. Math. J.*, **5**:4 (2005), 919–926.
- [3] E. Freitag, R. Kiehl, *Etale cohomology and the Weil conjecture*, With an historical introduction by J. A. Dieudonné, *Ergeb. Math. Grenzgeb.* (3), **13**, Springer-Verlag, Berlin, 1988.
- [4] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann & Cie., Paris, 1948.
- [5] W. Waterhouse, "Abelian varieties over finite fields", *Ann. Sci. École Norm. Sup.* (4), **2** (1969), 521–560.
- [6] W. Waterhouse, J. Milne, "Abelian varieties over finite fields", 1969 *Number Theory Institute* (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, RI, 1971, 53–64.
- [7] M. A. Tsfasman, "Group of points of an elliptic curve over a finite field", *Proc. Ail-Union. Conf. on Number Theory and its Applications*, Tbilisi, 1985, 286–287.
- [8] H.-G. Rück, "A note on elliptic curves over finite fields", *Math. Comp.*, **49**:179 (1987), 301–304.

- [9] J. F. Voloch, “A note on elliptic curves over finite fields”, *Bull. Soc. Math. France*, **116**:4 (1988), 455–458.
- [10] R. Schoof, “Nonsingular plane cubic curves over finite fields”, *J. Combin. Theory. Ser. A*, **46**:2 (1987), 183–211.
- [11] E. Bombieri, D. Mumford, “Enriques’ classification of surfaces in char. p . II”, *Complex analysis and algebraic geometry*, Iwanami Shoten, Tokyo, 1977, 23–42.
- [12] L. Bădescu, *Algebraic Surfaces*, Universitext, Springer-Verlag, New York, 2001.
- [13] Ю. И. Манин, *Кубические формы: алгебра, геометрия, арифметика*, Наука, М., 1972.
- [14] K. Matsuki, *Introduction to the Mori Program*, Universitext, Springer-Verlag, New York, 2002.
- [15] Ж.-П. Серр, *Когомологии Галуа*, Мир, М., 1968.
- [16] Р. Хартсхорн, *Алгебраическая геометрия*, Мир, М., 1981.
- [17] Д. Мамфорд, *Абелевы многообразия*, Мир, М., 1971.

С. Ю. Рыбаков

Независимый московский университет

E-mail: rybakov.sergei@gmail.com

Поступило

03.04.2007