Math-Net.Ru

Общероссийский математический портал

И. Р. Шафаревич, О некоторых семействах абелевых поверхностей, *Изв. РАН. Сер. матем.*, 1996, том 60, выпуск 5, 213–223

DOI: <https://doi.org/10.4213/im92>

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: 35.174.16.151

26 апреля 2023 г., 17:09:08

УДК 513.6

И. Р. Шафаревич

О некоторых семействах абелевых поверхностей

Доказывается, что для всех алгебраических кривых Γ , являющихся накрытиями заданной степени n заданной кривой Γ_0 и всех непостоянных семейств “ложных эллиптических кривых” над Γ , их общие слои принадлежат лишь к конечному числу типов с точностью до изоморфизма над алгебраическим замыканием поля рациональных функций на Γ . Указаны приложения к теории поверхностей типа КЗ.

Библиография: 9 наименований.

Напомним, что *ложной эллиптической кривой* называется двумерное абелево многообразие, кольцо эндоморфизмов которого изоморфно порядку неопределенной кватернионной алгебры над полем $\mathbb{Q}$.

В работе [1] рассматривались абелевы поверхности и поверхности типа КЗ над полями алгебраических чисел. Рассматривались сингулярные поверхности, т.е. имеющие максимальное значение числа Пикара: $\rho = 4$ для абелевых поверхностей и $\rho = 20$ для поверхностей типа КЗ. Там доказано, что среди таких поверхностей, определенных над расширением заданной степени поля $\mathbb{Q}$, имеется лишь конечное число неизоморфных над алгебраическим замыканием этого поля. В этой работе рассматривается “функциональный аналог” того же вопроса, т.е. мы рассматриваем поверхности, определенные над полем рациональных функций на алгебраической кривой. В случае абелевых поверхностей мы изучаем следующий по трудности случай $\rho = 3$ и, в частности, ложные эллиптические кривые. Будет доказана

ТЕОРЕМА. Пусть $K = \mathbb{C}(\Gamma)$, где Γ – алгебраическая кривая. Существует лишь конечное число определенных над полем K непостоянных ложных эллиптических кривых с точностью до изоморфизма над алгебраическим замыканием поля K .

Утверждение теоремы остается верным, если рассматривать такие же поверхности, определенные не над фиксированным полем K , а над всеми полями K , имеющими заданную степень над чисто трансцендентным подполем $\mathbb{C}(T)$.

В конце работы указаны применения к случаю поверхностей типа КЗ.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Абелево многообразие A над полем $K = \mathbb{C}(\Gamma)$ определяет семейство $\mathcal{A} \rightarrow \Gamma$, общий слой которого – ложная эллиптическая кривая. Согласно работам Г. Шимуры (например, [2]) для таких кривых существует конечное число универсальных семейств $\mathcal{A}_i \rightarrow S$, так что семейство $\mathcal{A}$ определяет морфизм $f: \Gamma \rightarrow S$, и общий слой семейства $\mathcal{A}$ изоморфен общему слою одного из семейств $\mathcal{A}_i$ над некоторым накрытием базы. Так как семейство $\mathcal{A}$ непостоянно, то морфизм f эпиморфен. Согласно работам Г. Шимуры база S универсальных семейств строится следующим образом. По определению кольцо эндоморфизмов

общего слоя семейства является некоторым порядком $\mathcal{O}$ неопределенной кватернионной алгебры B над полем рациональных чисел. Пусть $\mathcal{O}^1$ – группа элементов порядка $\mathcal{O}$ с приведенной нормой, равной 1, и $\mathcal{O}^1 \rightarrow \mathrm{SL}(2, \mathbb{R})$ – вложение. Тогда $S = H/\mathcal{O}^1$, где H – верхняя полуплоскость. Кривая S определена над некоторым полем алгебраических чисел $\mathbb{k}$, которое является композитом квадратичных расширений поля рациональных чисел (см., например, [3, §9, с. 247, 248]).

Так как поле $\mathbb{C}(\Gamma)$ имеет по условию фиксированную степень n над полем $\mathbb{C}(T)$, то существует морфизм $\Gamma \rightarrow \mathbb{P}^1$, определенный функцией $u \in \mathbb{C}(\Gamma)$. Тогда функция $v = f_*(u) = N(f)$ определяет морфизм $S \rightarrow \mathbb{P}^1$, имеющий степень $\leq n$, если он не постоянен. Действительно, $(u) = (u)_0 - (u)_\infty$, где $\deg(u)_0 = \deg(u)_\infty = n$. Тогда $(v) = f_*(u)_0 - f_*(u)_\infty$ и $\deg f_*(u)_0 = \deg f_*(u)_\infty = n$. Если морфизм v постоянен, то мы можем заменить функцию u на $u - c$, где c – любая константа. Функция $N(u - c)$ (N обозначет норму в поле $\mathbb{C}(\Gamma)$ над полем $\mathbb{C}(S)$) постоянна для всех c , только если постоянна u . Таким образом, мы можем предполагать, что кривая S обладает непостоянным морфизмом $S \rightarrow \mathbb{P}^1$ ограниченной степени n , и нам достаточно доказать, что существует лишь конечное число порядков $\mathcal{O}$ с таким свойством. При $n = 2$ кривая S гиперэллиптическая. Этот случай уже рассматривался (например, см. работу [4]), правда, лишь для некоторых специальных порядков (так называемых порядков Эйхлера). При этих ограничениях удалось не только доказать конечность числа таких порядков, но и найти их полный список. Мы покажем, что основная идея работы [4] может быть применена и в нашей, более общей, ситуации.

Первая трудность, с которой мы сталкиваемся, заключается в том, что морфизм $S \rightarrow \mathbb{P}^1$ может быть определен не над тем полем, над которым была определена кривая S . Нам достаточно более слабого свойства.

ЛЕММА 1. Пусть кривая S определена над совершенным полем $\mathbb{k}$, $S \rightarrow \mathbb{P}^1$ – морфизм степени $\leq n$. Тогда существуют кривая C , определенная над полем $\mathbb{k}$, рода $\leq (n - 1)^2$ и морфизм $S \rightarrow C$ степени $\leq n$, определенный над $\mathbb{k}$.

Мы можем считать, что морфизм $\varphi: S \rightarrow \mathbb{P}^1$ определен над полем $\mathbb{k}$, которое является расширением Галуа поля $\mathbb{k}$ с группой Галуа G порядка d . Рассмотрим морфизм $\psi = \prod_{\sigma \in G} \varphi^\sigma: S \rightarrow (\mathbb{P}^1)^d$. Образ его обозначим через C . Очевидно, что кривая C определена над $\mathbb{k}$, $C \subset (\mathbb{P}^1)^d$ и степени проекций $C \rightarrow \mathbb{P}^1$ (мы пишем $(\mathbb{P}^1)^d$ в виде $\mathbb{P}^1 \times \cdots \times \mathbb{P}^1$) не превосходят n . Нам достаточно доказать, что род кривой C не превосходит $(n - 1)^2$. Доказательство проводится индукцией по d . Очевидно, что интересен лишь случай $d \geq 2$. При $d = 2$ утверждение содержится в виде упражнения в книге [5, с. 366]. Там утверждается (в обозначениях, более близких к нашим), что если $C \subset C_1 \times C_2$, степени проекций $C \rightarrow C_i$ не превосходят n_i , а кривые C , C_1 и C_2 имеют роды g , g_1 и g_2 , то

$$g \leq (n_1 - 1)(n_2 - 1) + n_1 g_2 + n_2 g_1 \quad (1)$$

(в нашем случае $g_1 = g_2 = 0$).

Для удобства читателя приведем доказательство этого упражнения. Пусть C_1^ν и C_2^ν – нормализации кривых C_1 и C_2 , а $\bar{C}$ – образ кривой C^ν при отображении $\varphi_1 \times \varphi_2$, где $\varphi_i: C^\nu \rightarrow C_i^\nu$ – естественные морфизмы нормализаций. В группе Севери поверхности $C_1^\nu \times C_2^\nu$ содержится подгруппа, порожденная кривыми $C_1 \times p_2$,

$p_1 \times C_2$. Мы будем обозначать их просто C_i . Поэтому цикл C представляется в виде $\overline{C} = \alpha_1 C_1 + \alpha_2 C_2 + X$, где X принадлежит ортогональному дополнению к этой подгруппе. Согласно неравенству Ходжа $(X^2) < 0$. Как легко видеть, $\overline{C} = n_1 C_1 + n_2 C_2 + X$, $(\overline{C}^2) = 2n_1 n_2 + X^2 \leq 2n_1 n_2$. С другой стороны, для канонического класса поверхности $C_1' \times C_2'$ мы имеем $K = (2g_1 - 2)C_2' + (2g_2 - 2)C_1'$. Так как $g < \frac{1}{2}(\overline{C}^2 + \overline{C}K)$, то отсюда легко следует

$$g \leq n_1 n_2 + (g_2 - 1)n_1 + (g_1 - 1)n_2 + 1 = (n_1 - 1)(n_2 - 1) + g_1 n_2 + g_2 n_1.$$

В общем случае (при $d > 2$) положим $(\mathbb{P}^1)^d = (\mathbb{P}^1)^{d-1} \times \mathbb{P}^1$. Пусть ψ – проекция $C \rightarrow \mathbb{P}_2 \times \dots \times \mathbb{P}_d = (\mathbb{P}^1)^{d-1}$ и $\deg(C \rightarrow \psi(C)) = \nu$. Тогда $\deg(\psi(C) \rightarrow \mathbb{P}^1) \leq n/\nu$. По индуктивному предположению $g(\psi(C)) < (n/\nu - 1)^2$. Очевидно, $\overline{C} \subset \psi(C) \times \mathbb{P}^1$, причем степени проекций C на $\psi(C)$ и $\mathbb{P}^1$ равны n/ν и n . Согласно формуле (1)

$$g(C) \leq (n - 1)(\nu - 1) + \nu(n/\nu - 1)^2.$$

Как легко видеть,

$$(n - 1)^2 - (n - 1)(\nu - 1) - \nu(n/\nu - 1)^2 = (n - 1)(n/\nu)(\nu - 1) \geq 0,$$

что и доказывает лемму.

Теперь, следуя идее работы [4], воспользуемся теорией конгруэнц-соотношений Ихары для кривых Шимур. Мы будем пользоваться следующими результатами (см. [6]). Пусть l – простое число, не делящее дискриминант порядка $\mathcal{O}$, $\mathfrak{l}$ – его простой делитель в поле определения кривой S и $\mathcal{O}_{\mathfrak{l}}$ – соответствующее локальное кольцо. Так как поле определения кривой S есть композит квадратичных расширений поля $\mathbb{Q}$, то степень поля $\mathcal{O}_{\mathfrak{l}}/\mathfrak{l}$ над $\mathbb{F}_l$ не больше двух и число $q = \#\mathcal{O}_{\mathfrak{l}}/\mathfrak{l}$ делит l^2 . Кривая S имеет хорошую редукцию $S/\mathfrak{l}$ по модулю $\mathfrak{l}$, и на кривой $S/\mathfrak{l}$ имеется не менее H точек, определенных над $\mathbb{F}_{q^2}$,

$$H = 1 + g_0 - 2g. \quad (2)$$

Здесь g – род кривой S , а g_0 – род кривой Шимур S , соответствующей порядку $\mathcal{O}_0$, который получается из $\mathcal{O}$ наложением в точке l условия

$$\mathcal{O}_0 \otimes \mathbb{Z}_l = (\mathcal{O} \cap w^{-1}\mathcal{O}w) \otimes \mathbb{Z}_l,$$

где $w = \begin{pmatrix} 0 & 1 \\ l & 0 \end{pmatrix}$. Доказательство соотношения (2), как показано в работе [6], основывается на следующем. Существует такая схема X над $\mathcal{O}/\mathfrak{l}$, что $X \otimes \mathbb{Q}_l = S \otimes \mathbb{Q}_l$. В схеме $X \times X$ существует такая подсхема T (она и является “конгруэнц-соотношением”), что кривая $T \otimes \mathbb{Q}_l$ имеет род g_0 , а $T \otimes \mathbb{F}_l = \Pi \cup \Pi^t$, где Π и Π^t являются графиками отображений $x \rightarrow x^q$ схем $S/\mathfrak{l} \rightarrow S/\mathfrak{l}$ и $S/\mathfrak{l} \leftarrow S/\mathfrak{l}$ в $S/\mathfrak{l} \times S/\mathfrak{l}$. При нормализации ровно H точек, определенных над $\mathbb{F}_{q^2}$, не “разводятся” в пары точек. Так как арифметический род не меняется при специализации, то $1 - g_0 = 2(1 - g) - H$, что и дает (2).

Согласно лемме 1 кривая S обладает сюръективным морфизмом степени $\leq n$ на кривую C рода $\leq (n - 1)^2$, причем и кривая C , и морфизм определены над полем $\mathbb{k}$.

Таким же морфизмом обладает и кривая S/l на C/l (или ее компонента, если она приводима). Согласно оценке Вейля число точек на кривой C/l над полем $\mathbb{F}_{q^2}$ не превосходит $\bar{c}(n)q^2$, где $\bar{c}(n)$ – константа, зависящая только от n (например, $\bar{c}(n) < 2(n-1)^2 + 1$). Тогда число точек на кривой S/l над полем $\mathbb{F}_{q^2}$ не превосходит $c(n)q^2$, где $c(n) = \bar{c}(n)n$. Формула (2) дает тогда

$$1 + g_0 - 2g < c(n)q^2 < c(n)l^4. \quad (3)$$

Доказательство теоремы основано на оценке левой части этого неравенства снизу. Для случая “порядков Эйхлера” существуют явные формулы для g и g_0 , которыми здесь можно воспользоваться (см., например, [7]). В общем случае мне такие формулы не известны и вместо них приходится довольствоваться некоторыми оценками.

Прежде всего напомним, что, выбирая надлежащий фундаментальный многоугольник группы Γ , действующей на верхней полуплоскости $\mathbb{H}$ с компактным фактором $\mathbb{H}/\Gamma$, мы можем объединить вершины многоугольника в эквивалентные относительно Γ циклы. Сумма углов в вершинах цикла имеет вид $2\pi/q$, где $q > 1$ целое. Если число циклов с заданным значением q равно e_q , то простые соображения геометрии Лобачевского дают для рода поверхности $\mathbb{H}/\Gamma$ формулу

$$g = \frac{S}{4\pi} - \sum \frac{e_q(q-1)}{2q} + 1,$$

где S – площадь фундаментального многоугольника (см. [7, с. 119]). Циклы соответствуют неподвижным точкам периодических элементов в Γ , а e_q равно числу классов сопряженных элементов периода q . Для кривой Шимур S $\Gamma = \mathcal{O}^1$ – группе элементов редуцированной нормы 1 в порядке $\mathcal{O}$ кватернионной алгебры. Поэтому q может принимать только значения 2 и 3, так что в этом случае $g = S/4\pi - e_2/4 - e_3/3 + 1$.

Для площади P максимального порядка M Эйхлер показал, что

$$\frac{P}{4\pi} = \frac{1}{12} \prod_{p|D} (p-1), \quad (4)$$

где D – дискриминант алгебры. Это следует из того, что для максимального порядка число классов идеалов равно 1; P играет роль регулятора поля алгебраических чисел, и соотношение (4) получается из обычного выражения числа классов через вычет ζ -функции. Другой вариант доказательства см. в [7]. Для произвольного порядка $S = P(M^1 : \mathcal{O}^1)$ и оценка этой величины сводится к оценке $(M^1 : \mathcal{O}^1)$.

Докажем, что

$$(M^1 : \mathcal{O}^1) = \prod_p (M_p^1 : \mathcal{O}_p^1). \quad (5)$$

Иначе говоря, естественное отображение $\mathcal{O}^1 \backslash M^1 \rightarrow \prod_p \mathcal{O}_p^1 \backslash M_p^1$ является биекцией. Инъективность отображения очевидна. Сюръективность следует из того, что если для $\eta \in \prod_p M_p^1$ $\eta \equiv 1(p^{n_p})$ при достаточно больших n_p , то $\eta \in \prod_p \mathcal{O}_p^1$

ввиду того, что индекс $(M_p^1 : Q_p^1)$ конечен. Согласно сильной теореме аппроксимации [7, с. 81] любой элемент $\xi \in \prod_p M_p^1$ представляется в виде $\xi = \eta x$, где η удовлетворяет указанным выше сравнениям и, значит, принадлежит $\prod_p \mathcal{O}_p^1$, а $x \in M$. Но тогда $x \in \prod_p M_p^1$ и, значит, $x \in M^1$.

В частности, отсюда следует, что $(M^1 : \mathcal{O}_0^1) = (M^1 : \mathcal{O}^1)(\mathcal{O}^1 : \mathcal{O}_0^1)$. Очевидно, $\mathcal{O}_l = M_l = M_2(\mathbb{Z}_l)$, а $\mathcal{O}_{0,l}$ состоит из матриц вида $\begin{pmatrix} a & b \\ lc & d \end{pmatrix}$. Отображение $M^1 \rightarrow \mathrm{SL}(2, \mathbb{F}_l)$ является эпиморфизмом, а ядро его содержится в $\mathcal{O}_{0,l}^1$. Поэтому $(\mathcal{O}_l^1 : \mathcal{O}_{0,l}^1) = (\mathrm{SL}(2, \mathbb{F}_l) : B)$, где B – подгруппа Бореля, т.е. $(M^1 : \mathcal{O}_0^1) = (M^1 : \mathcal{O}^1)(l + 1)$ и

$$g_0 - 2g = (1/12) \prod_p (p-1)(M^1 : \mathcal{O}^1)(l-1) - E_0 + 2E,$$

где $E = e_2/4 + e_3/3$, e_2 и e_3 имеют указанный выше смысл для порядка $\mathcal{O}$, а E_0 – тот же инвариант для $\mathcal{O}_0$. Таким образом,

$$g_0 - 2g \geq (1/12) \prod_p (p-1)(M^1 : \mathcal{O}^1)(l-1) - E_0,$$

и оценка снизу этого выражения сводится к:

- а) оценке сверху для E_0 ;
- б) оценке снизу для $\prod_p (p-1)(M^1 : \mathcal{O}^1)(l-1)$.

а) *Оценка сверху для E_0* . Докажем, что

$$E_0 < c_1 2^t, \quad (6)$$

где t – число простых делителей дискриминанта порядка $\mathcal{O}$, а c_1 – некоторая абсолютная константа.

Обозначим через $\mathcal{O}_p$ локальный порядок $\mathcal{O} \otimes \mathbb{Z}_p$, а через $e_{2,p}$ и $e_{3,p}$ – выражения, определенные для $\mathcal{O}_p$ так же, как e_2 и e_3 определялись для $\mathcal{O}$.

Докажем, что

$$e_i \leq 2 \prod_p e_{i,p}. \quad (7)$$

Мы рассмотрим только выражение для e_2 ; e_3 рассматривается так же. По определению e_2 равно числу классов элементов $x \in \mathcal{O}$, $x^2 = -1$, с точностью до сопряженности элементами $y \in \mathcal{O}^1$. Все такие элементы сопряжены с фиксированным i , $i^2 = -1$, в $B^\times$, и централизатор элемента i совпадает с $\mathbb{Q}(i)$. Поэтому

$$e_2 = \#(\mathcal{O}^1 \backslash T/\mathbb{Q}(i)^\times), \quad T = \{t \in B^\times, t^{-1}it \in \mathcal{O}\},$$

$$e \leq 2\#\mathcal{O}^\times \backslash T/\mathbb{Q}(i)^\times.$$

Естественное отображение

$$\mathcal{O}^\times \backslash T/\mathbb{Q}(i)^\times \rightarrow \mathcal{O}_{\mathbb{A}}^\times \backslash T_{\mathbb{A}}/\mathbb{Q}(i)^\times,$$

где индекс $\mathbb{A}$ обозначает аделизацию, является вложением. Действительно, если $t_2 = \omega t_1 l$, $\omega \in \mathbb{Q}_{\mathbb{A}}^\times$, $l \in \mathbb{Q}(i)^\times$, $t_1, t_2 \in T$, то $\omega \in \mathcal{O}^\times$ и, значит,

$$e \leq 2\#\{\mathcal{O}_{\mathbb{A}}^\times \backslash T_{\mathbb{A}}/\mathbb{Q}(i)^\times\}.$$

С другой стороны,

$$\mathcal{O}_{\mathbb{A}}^{\times} \backslash T_{\mathbb{A}} / \mathbb{Q}(i)^{\times} = \mathcal{O}_{\mathbb{A}}^{\times} \backslash T_{\mathbb{A}} / \mathbb{Q}(i)_{\mathbb{A}}^{\times}.$$

Действительно, $\mathbb{Q}(i)_{\mathbb{A}}^{\times} = \mathbb{Q}(i)^{\times} U$, где U – обратимые иделы. Поэтому элемент двойного класса смежности $\omega t \lambda$, где $\omega \in \mathcal{O}_{\mathbb{A}}^{\times}$, $t \in T$, $\lambda \in \mathbb{Q}(i)_{\mathbb{A}}^{\times}$, представляется в виде tul , где $l \in \mathbb{Q}(i)^{\times}$, $u \in U$, так как $\lambda = ul$. Это равно $\omega t u t^{-1} t l$, т.е. $(\omega \omega_1) t l$, где $\omega_1 = t u t^{-1}$. Так как

$$\mathcal{O}_{\mathbb{A}}^{\times} \backslash T_{\mathbb{A}} / \mathbb{Q}(i)_{\mathbb{A}}^{\times} = \prod_p \mathcal{O}_p^{\times} \backslash T_{\mathbb{A}} / \mathbb{Q}(i)_p^{\times},$$

то это и доказывает (7).

Таким образом, задача свелась к локальным задачам, и неравенство (6) будет вытекать из следующего утверждения.

ЛЕММА 2. *Для $i = 2, 3$ $e_{i,p} = 1$, если p не делит дискриминант порядка $\mathcal{O}$, и $e_{i,p} \leq 2$ в остальных случаях, кроме $p = 2$, когда $e_{i,2}$ ограничено абсолютной константой (не зависящей от порядка $\mathcal{O}$).*

Рассмотрим e_2 . Пусть p не делит дискриминант порядка $\mathcal{O}$. Тогда $\mathcal{O}_p = M_2(\mathbb{Z}_p) = \text{End } A$, $A = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Из того что $x^2 = -1$, $n(x) = 1$, легко следует, что x не является умножением на скаляр в A/p . Поэтому существует такой вектор $e \in A/p$, что e и $x e$ образуют базис в A/p , а значит, и в A . В этом базисе x имеет матрицу $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, т.е. сопряжен такому элементу из $M_2(\mathbb{Z}_p)$. Поэтому $e_{i,p} = 1$.

Пусть $p \neq 2$, $i \in \mathcal{O}_p$, $i^2 = -1$. Если $p \equiv 1 \pmod{4}$, то $\mathcal{O}_p$ является порядком Эйхлера [7, с. 39] и $e_p = 2$ [7, с. 43]. Пусть $p \equiv 3 \pmod{4}$. Тогда любой порядок $\mathcal{O}_p$, содержащий i , имеет вид $\mathbb{Z}_p[i] + u\mathbb{Z}_p[i]$, где $u \in \mathbb{Z}_p$, $iu = -ui$. Это следует из того, что $\mathcal{O}_p = A + B$, $A = \{x, xi = ix\}$, $B = \{x, xi = -ix\}$, $A \ni i$, значит, $A = \mathbb{Z}_p[i]$, а B является свободным модулем ранга 1 над A .

Поэтому $B = jp^k \mathbb{Z}_p[i]$ при некотором k , $j^2 = p^{\varepsilon}$, $\varepsilon = 1$ или $\varepsilon = 0$ (в зависимости от того, является алгебра B_p телом или нет). Пусть $x = \alpha + jp^m \beta$. Условие $x^2 = -1$ дает $\beta(\alpha + \bar{\alpha}) = 0$. Тогда или $\beta = 0$, $x = \pm i$, или $\bar{\alpha} = -\alpha$, $x = iu$, $u \in \mathbb{Z}$. Кроме того,

$$u^2 - 1 = p^{2m+\varepsilon} \beta \bar{\beta}_{2m+\varepsilon}, \quad (8)$$

$u = \sqrt{1 + p^{2m+\varepsilon} \beta \bar{\beta}}$. Пусть $u = 1 + (1/2)p\beta \bar{\beta} + \dots$. Покажем, что x сопряжено с i в $\mathcal{O}^{\times}$. Найдем такой элемент $1 + jp^m \xi$, $\xi \in \mathbb{Z}_p[i]$, что

$$(1 + p^m j \xi) i = (iu + p^m j \beta)(1 + p^m j \xi). \quad (9)$$

Мы получаем для ξ равенство $i = iu + p^{2m+\varepsilon} \beta \bar{\beta}$, откуда

$$\xi = \frac{i(1-u)}{p^{2m+\varepsilon} \bar{\beta}}.$$

Ввиду (8) $\xi \in \mathbb{Z}_p[i]$. Сравнение коэффициентов при j в (9) дает, как легко видеть, ввиду (8) то же выражение для ξ .

Пусть теперь $p = 2$. Рассуждение здесь аналогично предыдущему, но несколько сложнее. Чтобы его немного упростить, мы будем пользоваться следующим соображением. Пусть $\mathcal{O} \supset \mathcal{O}_1$ – два порядка в 2-адической кватернионной алгебре B и индекс $(\mathcal{O} : \mathcal{O}_1)$ является абсолютной константой. Тогда из справедливости утверждения леммы для $\mathcal{O}$ вытекает его справедливость для $\mathcal{O}_1$. Это сразу следует из того, что в нашем случае индекс $(\mathcal{O}^\times : \mathcal{O}_1^\times)$ тоже ограничен абсолютной константой: если $(\mathcal{O} : \mathcal{O}_1) = n$, то $\mathcal{O}_1 \supset n\mathcal{O}$, $(\mathcal{O}^\times : \mathcal{O}_1^\times) < (\mathcal{O}^\times : (1 + n\mathcal{O}))$, а $(\mathcal{O}^\times : (1 + n\mathcal{O})) \leq (\mathcal{O} : n\mathcal{O}) = n^4$.

Рассмотрим сначала случай, когда алгебра B является алгеброй с делением с обычными кватернионными единицами $1, i, j, k = ij$. Легко видеть, что если $x \in B$, $x^2 = -1$, $n(x) = 1$, то $x \in \mathbb{Z}_2 1 + \mathbb{Z}_2 i + \mathbb{Z}_2 j + \mathbb{Z}_2 k$. Порядок $\mathcal{O}$ можно записать в виде $\mathbb{Z}_2[i] + j\alpha\mathbb{Z}_2[i]$. Мы можем умножить α на любой элемент из $(\mathbb{Z}_2[i])^\times$. В результате можно ограничиться случаем $\alpha = 2^k$ или $\alpha = 2^k(1 + i)$, а ввиду сделанного выше замечания – первым случаем, т.е. положить $\mathcal{O} = \mathcal{O}_k = \mathbb{Z}_2[i] + j2^k\mathbb{Z}_2[i]$. В этой ситуации полностью применимо рассуждение, использованное при $p \neq 2$ – надо лишь взять трансформирующий элемент в (9) в виде $1 + 2^{k-1}j\beta$. Мы получим, что элемент x сопряжен с i при помощи элемента не из $\mathcal{O}_k^\times$, а из $\mathcal{O}_{k-1}^\times$. Но этого достаточно для нашего утверждения, так как индекс $(\mathcal{O}_k^\times : \mathcal{O}_{k-1}^\times)$ абсолютно ограничен.

Пусть теперь $B = M_2(\mathbb{Q}_2)$. Зададим элемент i в виде матрицы:

$$i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Тогда совершенно так же, как выше, проверяется, что любой порядок, содержащий i , содержится в порядке $\mathbb{Z}_2[i] + 2^k M_2(\mathbb{Z}_2)$ с индексом, который ограничен абсолютной константой. В свою очередь, такой порядок содержится в порядке вида $\mathbb{Z}_2[i] + 2^k j\mathbb{Z}_2[i]$ – можно взять за j матрицу

$$j = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Наконец, для такого порядка дословно сохраняются вычисления, справедливые для порядка в алгебре с делением.

Выражение $e_{3,p}$ рассматривается совершенно аналогично. В некоторых случаях рассуждения сохраняются дословно, а именно если p не делит дискриминант порядка $\mathcal{O}$ и если $p \equiv 1 \pmod{3}$. Если $p \equiv 2 \pmod{3}$, $p \neq 2$, или $p = 3$, нужно только заметить, что классы сопряженности элементов ρ , $\rho^2 + \rho + 1 = 0$, совпадают с классами сопряженности элементов y , $y^2 + 3 = 0$. Поэтому сохраняются те же формулы, что для e_2 с заменой -1 на -3 . В оставшемся случае $p = 2$ легко убедиться, что максимальный порядок можно записать в виде $\mathbb{Z}_2[\rho] + j\mathbb{Z}_2[\rho]$, где $j\alpha j^{-1} = \bar{\alpha}$ для $\alpha \in \mathbb{Z}_2[\rho]$ и $j^2 = 2^\varepsilon$, а $\varepsilon = 0, 1$, как в случае e_2 при $p = 2$. Тогда любой порядок можно записать в виде $\mathbb{Z}_2[\rho] + 2^k j\mathbb{Z}_2[\rho]$. Если

$$x = \alpha + 2^k j\beta, \quad x^2 + x + 1 = 0, \quad \alpha, \beta \in \mathbb{Z}_2[\rho],$$

то $\text{Sp } x = -1$, $n(x) = 1$. Отсюда $\alpha\bar{\alpha} - 2^{2k+\varepsilon}\beta\bar{\beta} = 1$, т.е.

$$2^{2k+\varepsilon}\beta\bar{\beta} = -1 + \alpha\bar{\alpha} = (\rho - \alpha)(\rho - \bar{\alpha}).$$

Так как $\rho - \alpha$ и $\rho - \bar{\alpha}$ не могут одновременно делиться на 2, то одно из них делится на $2^{2k+\varepsilon}$. Пусть это будет $\rho - \alpha$. Докажем, что тогда x сопряжено с ρ . Трансформирующий элемент надо взять в виде $1 + j^{2k}\xi$, и тогда то же самое вычисление дает нужный результат. Это заканчивает доказательство леммы 2.

б) *Оценка снизу для $\prod_{p|D}(p-1)(M^1 : \mathcal{O}^1)(l-1)$.* Отбросив множитель $l-1$, мы докажем неравенство

$$\prod_{p|D}(p-1)(M^1 : \mathcal{O}^1) \geq c \prod_p (p-1), \quad (10)$$

где произведение справа распространено на все простые числа p , для которых $\mathcal{O}_p \neq M_2(\mathbb{Z}_p)$, или, что то же самое, $p \nmid D(\mathcal{O})$.

Поскольку $(M^1 : \mathcal{O}^1) = \prod_p (M_p^1 : \mathcal{O}_p^1)$, нам достаточно доказать соответствующее неравенство для каждого p и соответствующих ему множителей в отдельности. Для p , делящих дискриминант алгебры, мы уже имеем множитель $p-1$ в левой части неравенства. Для остальных p алгебра $B \otimes \mathbb{Q}_p$ изоморфна $M_2(\mathbb{Q}_p)$. Мы будем дальше обозначать через M ее максимальный порядок, а через $\mathcal{O}$ – некоторый порядок, $\mathcal{O} \subset M$, $\mathcal{O} \neq M$.

Так как $(M^1 : \mathcal{O}^1) \geq ((M/p)^1 : (\mathcal{O}/p)^1)$, то нам достаточно доказать, что $((M/p)^1 : (\mathcal{O}/p)^1) \geq p-1$. Очевидно, $(M/p)^1 = \mathrm{SL}(2, \mathbb{F}_p)$. Положим $\mathcal{O}/p = R$. Нам надо доказать, что $(\mathrm{SL}(2, \mathbb{F}_p) : R^1) \geq p-1$, если $R \neq M_2(\mathbb{F}_p)$. Легко перебрать все подкольца $R \subsetneq M_2(\mathbb{F}_p)$. Если R содержит хотя бы одну матрицу с различными собственными значениями, принадлежащими $\mathbb{F}_p$, то R содержит кольцо

$$\begin{pmatrix} \mathbb{F}_p & 0 \\ 0 & \mathbb{F}_p \end{pmatrix}.$$

Если же в R содержится еще хотя бы одна матрица, то R сопряжено с кольцом

$$\begin{pmatrix} \mathbb{F}_p & \mathbb{F}_p \\ 0 & \mathbb{F}_p \end{pmatrix}.$$

Если у всех матриц из R все собственные значения принадлежат $\mathbb{F}_p$ и являются кратными, то R совпадает с $\mathbb{F}_p E$ или сопряжено с $\mathbb{F}_p E + \mathbb{F}_p J$, где

$$J = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Наконец, если в R содержится матрица, собственные значения которой не принадлежат $\mathbb{F}_p$, то $R = \mathbb{F}_{p^2}$. Во всех случаях легко найти порядок группы R^1 и проверить, что $(\mathrm{SL}(2, \mathbb{F}_p) : R^1) > p-1$.

Так как $p-1 \geq 4$, если $p > 3$, то мы получаем оценку $H > c_1 4^t - c_2 2^t$. Вместе с (3) это дает неравенство

$$c_1 4^t - c_2 2^t < c(n)l, \quad (11)$$

где t – число простых делителей дискриминанта p порядка $\mathcal{O}$, а l – простое число, отличное от этих простых делителей. Если $p_1, p_2, \dots, p_t$ – это все первые t простых чисел, то за l можно взять $p_{t+1} - (t+1)$ -е простое число, а если одно из первых t простых чисел среди $p_1, p_2, \dots, p_t$ отсутствует, то мы можем взять его за l , и тогда

$l < p_{t+1}$. Так как $p_t \sim t \log t$ (8), то всегда можно выбрать $l < ct \log t$ с некоторой константой c . В результате мы получаем неравенство

$$c_1 4^t - c_2 2^t \leq c_3(n)(t \log t),$$

которому, очевидно, удовлетворяет только конечное множество чисел t . Мы можем дальше рассматривать каждое из этих значений в отдельности и, значит, считать t фиксированным. Пользуясь более сильным неравенством

$$c \prod (p-1) - c_2 2^t < c_3(n)(t \log t),$$

мы видим, что ограничены и сами p . Поэтому мы можем считать их фиксированными. Таким образом, могут считаться фиксированной и кватернионная алгебра B и простые делители дискриминанта ее порядка $\mathcal{O}$. Наконец, воспользовавшись еще более сильной оценкой

$$c(M^1 : \mathcal{O}^1) - c_2 2^t < c_3(n)(t \log t),$$

мы видим, что ограничен индекс $(M^1 : \mathcal{O}^1)$. Остается доказать, что в максимальном порядке M содержится лишь конечное число порядков $\mathcal{O}$ с заданным значением индекса $(M^1 : \mathcal{O}^1)$. Так как $(M^1 : \mathcal{O}^1) = \prod (M_p^1 : \mathcal{O}_p^1)$, то ограничены все локальные индексы $(M_p^1 : \mathcal{O}_p^1)$, а поскольку порядок определяется своими локализациями, то достаточно доказать, что в кватернионной алгебре над полем $\mathbb{Q}_p$ с максимальным порядком M содержится лишь конечное число порядков $\mathcal{O}$ с заданным индексом $(M^1 : \mathcal{O}^1)$. Это вытекает из следующего утверждения.

ЛЕММА 3. Пусть M – максимальный порядок в кватернионной алгебре B над $\mathbb{Q}_p$, $\mathcal{O}$ – содержащийся в нем порядок, $(M^1 : \mathcal{O}^1) = \nu$ и ν делится точно на p^k .

Тогда $\mathcal{O} \supset p^k M$, где $t = k + 1$ при $p = 2$ и $t = k + 3$ при $p \neq 2$.

Очевидно, $\mathcal{O}^1 \supset (M^1)^\nu$. Докажем, что кольцо U , порожденное $(M^1)^\nu$, содержит $p^m M$.

Рассмотрим сначала случай, когда $B = M_2(\mathbb{Q}_p)$, $M = M_2(\mathbb{Z}_p)$. Очевидно,

$$(M^1)^\nu \supset V, \quad V = \begin{pmatrix} 0 & p^k \alpha \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 0 \\ p^k \beta & 0 \end{pmatrix}.$$

Нам остается рассмотреть диагональные матрицы. Обозначим через (a, b) матрицу с a и b по диагонали. Если $p \neq 2$, то $(1 + py)^{p^k} = 1 + p^{k+1}z$, $z \not\equiv 0 \pmod{p}$. Поэтому среди элементов $(x, x^{-1})^\nu$, $x = 1 + py$, содержится элемент вида $(1 + p^{k+1}z, (1 + p^{k+1}z)^{-1})$ с $z \not\equiv 0 \pmod{p}$. Тогда $U \ni (x, x^{-1})^\nu - (1 + p^{k+1}z)E = (0, p^{k+1}y)$. Так как

$$(1 + p^{k+1}z) - (1 + p^{k+1}z)^{-1} = (1 + p^{k+1}z)^{-1}(1 - (1 + p^{k+1}z)^2),$$

то $y = -(1 + p^{k+1}z)^{-1}z(2 + p^{k+1}z)$, $y \not\equiv 0 \pmod{p}$. Поэтому $U \supset (0, p^{k+1}\mathbb{Z}_p)$, и аналогично $U \supset (p^{k+1}\mathbb{Z}_p, 0)$. Если $p = 2$, то $U \supset (1 + 2^{k+2}z, (1 + 2^{k+2}z)^{-1})$ с нечетным z . Аналогично предыдущему

$$(1 + 2^{k+2}z) - (1 + 2^{k+2}z)^{-1} = -2^{k+3}z(1 + 2^{k+2}z),$$

откуда $U \supset (0, 2^m \mathbb{Z}_2)$, $U \supset (2^m \mathbb{Z}_2, 0)$.

Пусть теперь $\mathbb{B} \otimes \mathbb{Q}_p$ является алгеброй с делением. Она порождается неразветвленным квадратичным расширением $\mathbb{Q}_p(\alpha)$ и простым элементом π с $\pi^2 = p$, где $\pi^{-1}\alpha\pi = \bar{\alpha}$ – сопряжение. Можно выбрать α так, что $\mathbb{Z}_p[\alpha]$ будет кольцом целых в $\mathbb{Q}_p(\alpha)$. Тогда $\mathbb{Z}_p[\alpha] + \pi\mathbb{Z}_p[\alpha]$ является максимальным порядком.

Сначала докажем утверждения леммы для элементов из $\mathbb{Z}_p[\alpha]$.

При $p \neq 2$ $(\mathbb{Z}_p[\alpha])^\times \supset 1 + p\mathbb{Z}_p[\alpha]$. Поэтому $U \supset (1 + p^{k+1}\beta)(1 + p^{k+1}\bar{\beta})^{-1} = 1 + p^{k+1}(\beta - \bar{\beta}) + p^{k+2}y$. Тогда $U \ni p^{k+1}\gamma$, где $\gamma \notin \mathbb{Z}_p \bmod p$. Значит, $U \supset p^m \mathbb{Z}_p[\alpha]$.

При $p = 2$ возьмем в $\mathbb{Z}_2[\alpha]$ элемент λ , с $\lambda + \bar{\lambda} = 1$. Тогда $(1 + 2^{k+2}\lambda) \times (1 + 2^{k+2}\bar{\lambda})^{-1} = 1 - 2^{k+2} + 2^{k+3} + 2^{2k+4}y$ и $U \supset 2^{2k+3}z$, $z \notin \mathbb{Z}_2 \bmod 2$, а значит, $U \supset 2^{2k+3}\mathbb{Z}_2[\alpha]$.

Очевидно, что U инвариантно относительно трансформирования любыми элементами алгебры.

При $p \neq 2$

$$p^m(1 + \pi)\alpha(1 + \pi)^{-1} = p^m(1 - p)^{-1}\alpha + p^m(1 - p)^{-1} \cdot (\alpha - \bar{\alpha})\pi + (1 - p)^{-1}p\bar{\alpha},$$

откуда мы видим, что $U \supset p^m \mathbb{Z}_p[\alpha]\pi$ и, значит, $U \supset p^m M$.

При $p = 2$ мы опять берем $1 + 2^{k+2}\lambda$, $\lambda \in \mathbb{Z}_2[\alpha]$, с $\lambda + \bar{\lambda} = 1$ и рассматриваем элемент $2^{k+3}(1 + \pi)\lambda(1 + \pi)^{-1}$, принадлежащий U . Как и раньше, мы находим в U элемент $2^{k+3}\lambda\pi$ с $\lambda \notin \mathbb{Z}_2 \bmod 2$. Отсюда

$$U \supset 2^{k+3}\pi\mathbb{Z}_2[\alpha] \quad \text{и} \quad U \supset 2^m M.$$

Доказательство леммы закончено, а значит, доказана и теорема.

ЗАМЕЧАНИЕ 1. Из теоремы, очевидно, следует геометрический аналог гипотезы Coleman'a (см. [1]) для ложных эллиптических кривых.

ЗАМЕЧАНИЕ 2. Пусть X – поверхность типа КЗ с числами Пикара $\rho = 19$. Как известно [9], для такой поверхности существует двулистное накрытие $Y \rightarrow X$, где Y – куммерова поверхность абелевой поверхности A с числом Пикара $\rho = 3$. Для A существуют две возможности: A является ложной эллиптической кривой или A изогенна квадрату эллиптической кривой без комплексного умножения. Соответственно X мы будем называть *поверхностью типа КЗ I* или *II* типа. Из доказанной теоремы вытекает аналогичное утверждение для поверхностей типа КЗ I типа.

Редукция утверждения от X к Y , а от Y к A дословно совпадает с той, которая изложена в работе [1] для случая сингулярных поверхностей ($\rho = 20$). Тем самым для поверхностей типа КЗ I типа доказан функциональный аналог гипотезы, сформулированной в работе [1].

Автор рад выразить глубокую благодарность профессору И. Ихара за разъяснения, касающиеся кривых Шимуры и связанных с ними конгруэнц-соотношений.

Список литературы

1. *Shafarevich I.* On the arithmetic of singular K3-surfaces // Proceedings of N.G. Chebotarev Centennial Conference. Kazan, Russia, 5–11 June 1994 /Eds. M.M. Arslanov, A.N. Parshin, I.R. Shafarevich. Berlin: Verlag Walter de Gruyter, 1996.
2. *Shimura G.* On the theory of automorphic functions // Ann. of Math. 1959. V. 70. № 1.
3. *Shimura G.* Introduction to the Arithmetic Theory of Automorphic Functions. Princeton University Press, 1971.
4. *Ogg A.* Real points on Shimura curves // Arithmetic and Geometry. V. 1. P. 277–308. Birkhauser, 1983.
5. *Arbarello E., Cornalba M., Griffiths P.A., Harris J.* Geometry of Algebraic Curves. V. 1. Springer-Verlag, 1985.
6. *Ihara Y.* Congruence Relations and Shimura Curves. Proceedings of Symposia in Pure Mathematics. 1979. V. 33. Part 2. P. 291–311.
7. *Vigneras M.-F.* Arithmetique des Algebres de Quaternions. Lecture Notes in Mathematics. V. 800. Springer-Verlag, 1980.
8. *Ичгам А.Е.* Распределение простых чисел. М.: ОНТИ, 1936.
9. *Nikulin V.V.* On Rational Maps Between K3 Surfaces. Constantin Carathéodory: An International Tribute. Th. M. Rassias World Science Publ, 1991. P. 964–995.

Математический ин-т им. В.А. Стеклова

Поступило в редакцию
11.I.1996