УДК 511.33:512.7:519.61

Н. М. Глазунов (Ин-т кибернетики НАН Украины, Киев)

О ПРОСТРАНСТВАХ МОДУЛЕЙ, РАВНОРАСПРЕДЕЛЕННОСТИ, ОЦЕНКАХ И РАЦИОНАЛЬНЫХ ТОЧКАХ АЛГЕБРАИЧЕСКИХ КРИВЫХ

We consider spaces of moduli of hyperelliptic curves and the Artin – Schreier coverings, and also some families of curves of this sort over fields of a characteristic p. By using the Postnikov method, we obtain expressions for the Kloosterman sums. We perform the computer investigations of the distribution of angles of the Kloosterman sums. For small values of prime p, we study the rational points on curves $y^2 = f(x)$. We consider the problem of accuracy of estimates for the number of rational points of hyperelliptic curves and the existence of rational points of curves of considered form on the spaces of moduli of these curves over a prime finite field.

Розглядаються простори модулів гіпереліптичних кривих та накриттів Артіна – Шраєра, а також деяких сімей таких кривих над полями характеристики p. Методом О. Г. Постнікова отримано вирази для сум Клостермана. Розподіл кутів сум Клостермана досліджено на ЕОМ. Для невеликих простих p досліджено раціональні точки на кривих $y^2 = f(x)$. Розглянуто проблему точності оцінок числа раціональних точок гіпереліптичних кривих та існування раціональних точок кривих вказаного вигляду на просторах модулів цих кривих над простим скінченним полем.

Введение. Пусть $\boldsymbol{B}$ — некоторый класс объектов. В рассматриваемых ниже случаях это будут: i) накрытия Артина – Шрайера

$$y^p - y = cx + \frac{d}{x}, \qquad c, d \in \boldsymbol{Z}, \qquad c, d \not\equiv 0 \pmod p, \tag{1}$$

и соответствующие им суммы Клостермана; ii) алгебраические кривые вида $y^2 = f(x)$ и гиперэллиптические кривые рода g над простыми конечными полями F_p. Пусть S — некоторая схема. Семейством объектов, параметризованных S, называется класс объектов

$$X_s\colon s \in S, \qquad X_s \in \boldsymbol{B},$$

наделенных структурой, совместимой со структурой базы S. Пространства модулей параметризуют, в частности, бирационально изоморфные классы эллиптических кривых [1].

Пусть $E\colon y^2 = x^3 + ax + b$ — эллиптическая кривая без комплексных умножений над $\boldsymbol{Z}$. Вне конечного множества простых, являющихся делителями дискриминанта, E имеет хорошую редукцию в поле F_p. Число точек $\#E_p$ при такой локализации выражается формулой $\#E_p = 1 + p - a_p$. Гипотеза Сато – Тэйта [2] утверждает, что углы φ_p, соответствующие поправочному члену a_p, равнораспределены на интервале $[0, \pi]$ с плотностью $2\pi^{-1}\sin^2 t$. Пусть

$$T_p(c, d) = \sum_{x=1}^{p-1} e^{\frac{2\pi i (cx + d/x)}{p}} \tag{2}$$

(p — простое, $c, d \in \boldsymbol{Z}$, $c, d \not\equiv 0 \pmod p$) — тригонометрическая сумма Клостермана (приложения сумм Клостермана к задачам аналитической теории чисел и библиография приведены, например, в [3 – 5]).

Замечание. Запись суммы Клостермана (2) используется в теоретико-числовых исследованиях (см. [6, 3 – 5]). В исследованиях, связанных с алгебраической геометрией, чаще используются эквивалентные (2), но имеющие на один параметр меньше суммы (см. ниже).

Имеет место представление $T_p = 2\sqrt{p}\cos\theta_p$, где θ_p – аргумент комплексных нулей L-функции, соответствующей сумме (2). Рассматриваются два варианта распределения углов сумм Клостермана:

А) углы суммы

$$T_p(c,d) = \sum_{x=1}^{p-1} e^{2\pi i\frac{(cx+d/x)}{p}},$$

когда c, d независимо пробегают мультипликативную группу F_p^* поля F_p, а p стремится к бесконечности;

Б) углы суммы

$$\sum_{x=1}^{p-1} e^{2\pi i\frac{(cx+d/x)}{p}},$$

когда выражение для суммы фиксировано, а p пробегает простые, не делящее произведение cd.

Н. М. Кац [5] и А. Адольфсон [7] доказали соответственно, что эквивалентные (2) суммы Клостермана $Kl(p,a)$ и $K(q,\lambda)$ распределены на интервале $[0,\pi]$ равномерно с плотностью Сато – Тэйта, когда a, λ пробегают F_p, $a, \lambda \not\equiv 0 \pmod p$, а p стремится к бесконечности. Мы, как и в [5], не даем никакого теоретического обоснования возможного варианта распределения типа Б), однако приводим результаты сопоставления полученных нами экспериментальных данных с доказанным А) и гипотетическим Б) распределением Сато – Тэйта в этих случаях. Краткое резюме об этих вычислениях имеется в [8]. Впервые выражение для значения суммы Клостермана получил А. Вейль. Мы даем элементарное (в смысле [9]) доказательство этого результата, следуя работе А. Г. Постникова [10], исследовавшего другой класс тригонометрических сумм, а вместо оценки А. Вейля используем элементарную оценку [11]. Далее изучаются рациональные точки на кривых вида $y^2 = f(x)$ и гиперэллиптических кривых рода больше единицы над простыми конечными полями, поведение оценок для числа точек на таких кривых на пространствах модулей этих кривых, а также приводится класс кривых, не имеющих рациональных точек над полем определения. Опишем содержание работы. В первом пункте приведены нужные нам сведения о пространствах модулей и определения. Далее сформулированы и доказаны две теоремы о суммах Клостермана, а в следующем пункте приведены результаты компьютерного исследования распределения углов сумм Клостермана и обсуждение этих результатов. В последнем пункте сформулирована и обсуждается задача разделяющих оценок на пространствах модулей и в терминах параметрических пространств исследуются существование рациональных точек на кривых вида $y^2 = f(x)$ и на гиперэллиптических кривых (теорема 3). Для параметризации объектов мы используем элементы алгебраической геометрии, а для исследования оценок и существования точек алгебраических кривых — элементарные методы в смысле [9]. Это дает возможность отделить алгебро-геометрическую и теоретико-числовую части исследуемых задач.

Пространства модулей. Далее используются некоторые определения из теории модулей (см. [1], где приведены и некоторые первоисточники). Однако в отличие от [1], где рассмотрен, в основном, случай нулевой характеристики, мы рассматриваем характеристику $p > 0$ [12, 13]. Алгебраическое многообразие называют пространством модулей данной алгебраической структуры, если точки многообразия параметризуют объекты или классы объектов (по некоторому отношению эквивалентности) этой алгебраической структуры [1].

Напомним, что проблема модулей состоит из двух частей. Во-первых, это выделение класса объектов и описание семейства таких объектов над некоторой схемой S. Во-вторых, выбор отношения эквивалентности. Среди различных пространств модулей в классической алгебраической геометрии различают модули и параметрические (параметризующие) пространства. Точкам параметрического пространства биективно соответствуют объекты параметризуемой алгебраической структуры, в то время как модули параметризуют классы, а каждый класс состоит, например, из бирационально изоморфных объектов. Мы будем использовать вариант этой терминологии, называя пространства модулей с тривиальным отношением эквивалентности *параметрическими пространствами*. Рассматриваются два типа параметрических пространств: квазипроективные многообразия и арифметические поверхности [14]. Для данной проблемы модулей объект, биективно соответствующий точке параметрического пространства, называем *лежащим над этой точкой*. Если для параметрического пространства Π определено понятие гиперплоскости H, то *(гиперплоским) сечением* называем множество нулей $H = 0$ в Π. Множество объектов, лежащих над точками сечения, будем называть *лежащими над сечением*. Соответственно, гиперэллиптическая кривая и накрытие вида (1) над Z определяют арифметическую гиперэллиптическую поверхность H и накрытие V. Конечные точки $\operatorname{Spec} Z$ параметризуют специальные слои A. Если выбросить из $\operatorname{Spec} Z$ множество точек d_1 вырождения гиперэллиптической кривой и множество точек d_2, в которых $c, d \equiv 0 \pmod p$, то $\operatorname{Spec} Z \backslash d_1$ и $\operatorname{Spec} Z \backslash d_2$ параметризуют гиперэллиптические кривые и накрытия специальных слоев H и V соответственно.

Накрытия Артина – Шрайера и сумм Клостермана. Рассмотрим накрытие (1) Артина – Шрайера [15] над полем F_{p^r} — конечным расширением поля F_p. Пусть

$$f(t) = t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n \tag{3}$$

— многочлен из $F_{p^r}[t]$ с $a_n \not\equiv 0 \pmod p$. В некотором конечном расширении k поля F_{p^r} имеет место разложение

$$f(t) = (t-\alpha_1) \ldots (t-\alpha_n).$$

Положим

$$l(f) = c(\alpha_1 + \ldots + \alpha_n) + d(1/\alpha_1 + \ldots + 1/\alpha_n).$$

Для многочленов вида (3) имеет место

$$l(f_1 \cdot f_2) = l(f_1) + l(f_2). \tag{4}$$

Пусть $\operatorname{Tr}\colon F_{p^r} \to F_p$ — отображение следа. Тогда в условиях выполнения (4)

$$\operatorname{Tr}(l(f_1 \cdot f_2)) = \operatorname{Tr}(l(f_1)) + \operatorname{Tr}(l(f_2)).$$

Для заданного многочлена вида (3) определим по аналогии с [10] характер $\chi_\nu(f) = e^{2\pi i \nu \operatorname{Tr}(l(f))/p}$, где ν — одно из чисел множества $0, 1, 2, \ldots, p-1$, $\chi(f) = 0$, если $a_n \equiv 0 \pmod p$. Легко проверить, что $\chi(f_1 \cdot f_2) = \chi(f_1) \cdot \chi(f_2)$.

Для накрытия вида (1) над F_{p^r} L-функцию определяют равенством

$$L(z, \chi) = \prod_{m=1}^{\infty} \prod_{p(t)} \frac{1}{(1 - \chi(p(t)) z^m)}, \tag{5}$$

где внутреннее произведение распространяется на все неприводимые в $F_{p^r}[t]$ многочлены со старшим коэффициентом 1, $\nu \geq 1$. При $\nu = 0$ функция $L(z, \chi_0) = (1 - p^r z)^{-1}$. Положим

$$T_r(\nu; c, d) = \sum_{\xi} e^{2\pi i \nu \frac{\mathrm{Tr}(c\xi + d/\xi)}{p}}, \quad \nu = 1, 2, \ldots, p-1,$$

ξ пробегает элементы мультипликативной группы $F_{p^r}^*$ поля F_{p^r}.

Замечание. $T_1(\nu; c, d) = T_p(c, d)$ при $\nu = 1, 2, \ldots, p-1$.

Теорема 1. *Произведение* (5) *сходится при* $|z| < 1/p^r$. *Функция* (5) *является многочленом второй степени и имеет вид*

$$L(z, \chi_\nu) = 1 + T_r(\nu; c, d)z + p^r z^2. \tag{6}$$

Доказательство проводим по методу А. Г. Постникова [10], который рассмотрел случай рациональных тригонометрических сумм с простым знаменателем.

Лемма 1.

$$\sum_{\xi} e^{2\pi i \nu \frac{\mathrm{Tr}(\xi)}{p}} = \begin{cases} 0, & \nu \neq 0; \\ p^r, & \nu = 0, \end{cases}$$

где ξ *пробегает элементы поля* F_{p^r}.

Лемма 2. *В условиях теоремы произведение в правой части* (5) *сходится и имеет место равенство*

$$\prod_{m-1}^{\infty} \prod_{p(t)} \frac{1}{(1 - \chi(p(t))z^m)} = 1 + \sum_{m=1}^{\infty} \left(\sum \chi(q(t)) \right) z^m,$$

где внутренняя сумма распространяется на все многочлены из $F_{p^r}[t]$ *степени* m *со старшим коэффициентом* 1.

Доказательство вытекает из следующего равенства:

$$\sum_{\deg q(t)=1} \chi(q(t)) = \sum_{\xi} e^{2\pi i \nu \frac{\mathrm{Tr}(c\xi + d/\xi)}{p}},$$

где ξ пробегает мультипликативную группу $F_{p^r}^*$.

Лемма 3. *Функция* (5) *является многочленом второй степени вида* (6), $\nu = 1, 2, \ldots, p-1$.

Доказательство. В силу леммы 2 коэффициент при z^j, $j = 3, 4, \ldots$, имеет вид

$$\sum e^{-2\pi i \nu \frac{\mathrm{Tr}\left(ca_1 a_n + \frac{da_{n-1}}{a_n}\right)}{p}} = \sum_{a_n} \sum_{a_{n-1}} e^{-2\pi i \nu \frac{\mathrm{Tr}\left(\frac{da_{n-1}}{a_n}\right)}{p}} \left(\sum_{a_1} e^{-2\pi i \nu \frac{\mathrm{Tr}(ca_1)}{p}} \right) = 0,$$

где a_n, a_{n-1}, a_1 — коэффициенты многочлена (3), a_n пробегает элементы $F_{p^r}^*$, а a_{n-1}, a_1 пробегают все поле F_{p^r}. Первая сумма распространяется на все многочлены с условием $\deg q(t) = j$. Сумма в скобках равна нулю согласно лемме 1. Коэффициент при z^2 имеет вид

$$\sum e^{-2\pi i\nu\frac{\mathrm{Tr}\left(ca_{n-1}+\frac{da_{n-1}}{a_0}\right)}{p}} = \sum_{a_{n-1}}\sum_{a_0} e^{-2\pi i\nu\frac{\mathrm{Tr}\left(ca_{n-1}+\frac{da_1}{a_{n+1}}\right)}{p}} =$$

$$= p^r - 1 + \sum_{a_{n-1}} e^{-2\pi i\nu\frac{c\mathrm{Tr}(a_1)}{p}} \sum_{a_n} e^{-2\pi i\nu\frac{d\mathrm{Tr}\left(\frac{a_{n-1}}{a_n}\right)}{p}}. \qquad (7)$$

В силу того, что $cd \not\equiv 0 \pmod p$, и цикличности $F_{p^r}^*$ при фиксированном $a_{n-1} \in F_{p^r}^*$ и a_n, пробегающем все элементы группы $F_{p^r}^*$, выражение a_{n-1}/a_n пробегает все элементы группы $F_{p^r}^*$. Согласно лемме 1 $\sum_{a_n} e^{-2\pi i\nu d\,\mathrm{Tr}\left(\frac{a_{n-1}}{a_n}\right)p^{-1}} =$ $= -1$, и двойная сумма в крайнем справа выражении в (7) равна 1. Теорема доказана.

Положим $L_p = 1 + T_1(\nu; c, d)z + pz^2$, $L_{p^r} = 1 + T_r(\nu; c, d)z + p^r z^r$,

$$W_p(z) = \prod_{\nu=1}^{p-1} L_p, \qquad W_{p^r}(z) = \prod_{\nu=1}^{p-1} L_{p^r}. \qquad (8)$$

Используя элементарную оценку [11] для числа точек $\#X(F_{p^r})$ кривой (1) в поле F_{p^r}

$$\left|\#X(F_{p^r}) - p^r\right| < 2(p-1)p^{r/2}, \qquad (9)$$

оценим по модулю корни произведения (8) и выразим через значения этих корней суммы Клостермана.

Теорема 2. *Корни произведения* (8) *по модулю равны* $1/\sqrt{p}$.

Доказательство. Разложим L_p в поле комплексных чисел C:

$$L_p = (1-\omega_1 z)(1-\omega_2 z).$$

Тогда аналогично [10] доказывается, что если

$$W_p(z) = \prod_{\tau=1}^{2(p-1)} (1-\omega_\tau z),$$

то

$$W_{p^r}(z) = \prod_{\tau=1}^{2(p-1)} (1-\omega_\tau^r z).$$

Обозначим через $\#T(F_{p^r})$ число решений уравнения $\mathrm{Tr}(c\zeta + d/\zeta) = 0$ относительно ζ в поле F_{p^r}. Имеет место равенство

$$\left|\sum_{\tau=1}^{2(p-1)} \omega_\tau^r\right| = \left|p\#T(F_{p^r}) - p^r - 1\right|. \qquad (10)$$

Для его доказательства достаточно сравнить в тождестве

$$\prod_{\tau=1}^{2(p-1)} (1-\omega_\tau^r z) = \prod_{\nu=1}^{p-1} L_{p^r}$$

коэффициенты при z в первой степени и показать, что

$$\left|\sum_{\tau=1}^{2(p-1)}\omega_\tau^r\right| = \left|\sum_{\nu=1}^{p-1}\sum_{\xi} e^{2\pi i\nu\frac{\mathrm{Tr}(c\xi+d/\xi)}{p}}\right| =$$

$$= \left|\sum_{\nu=0}^{p-1}\sum_{\xi} e^{2\pi i\nu\frac{\mathrm{Tr}(c\xi+d/\xi)}{p}} - p^r - 1\right| = \left|p\#T(F_{p^r}) - p^r - 1\right|,$$

ξ пробегает $F_{p^r}^*$. Из леммы 8 [10] следует, что

$$\#X(F_{p^r}) = p\#T(F_{p^r}). \tag{11}$$

Теперь разлагая $\ln W_p(z)$ в ряд Тэйлора и учитывая (10), (11) и (9), получаем

$$\ln W_p(z) = -\sum_{\tau=1}^{2(p-1)} \ln\frac{1}{1-\omega_\tau z} = -\sum_{m=1}^{\infty}\frac{1}{m}\left(\sum_{\tau=1}^{2(p-1)}\omega_\tau^m\right)z^m.$$

Однако

$$\left|\sum_{m=1}^{\infty}\frac{1}{m}\left(\sum_{\tau=1}^{2(p-1)}\omega_\tau^m\right)z^m\right| \le \sum_{m=1}^{\infty}\frac{1}{m}\left|p\#T(F_{p^r}) - p^m\right||z^m| \le 2(p-1)\sum_{m=1}^{\infty}\left(\frac{1}{m}p^{m/2}\right)|z^m|.$$

Следовательно, ряд $\ln W_p(z)$ сходится при $|z| < 1/\sqrt{p}$. Применяя теорему о круге сходимости степенного ряда к $\ln W_p(z)$ и учитывая, что $\prod_{\tau=1}^{2(p-1)}|\omega_\tau| = p^{p-1}$, получаем $|\omega_\tau| = \sqrt{p}$, $\tau = 1, 2, \ldots, 2(p-1)$.

Следствие. $T_p = 2\sqrt{p}\cos\theta_p(c, d)$.

Результаты компьютерных исследований. Здесь изложены результаты вычисления углов θ_p сумм Клостермана на интервале $[0, \pi]$ в следующих двух случаях:

А) доказанный Н. М. Кацем [5] и А. Адольфсоном [7] случай распределения углов сумм

$$T_p(c, d) = \sum_{x=1}^{p-1} e^{2\pi i\frac{(cx+d/x)}{p}},$$

когда $c, d, cd \not\equiv 0 \pmod p$, независимо пробегают F_p, а p стремится к бесконечности;

Б) проверка гипотезы для суммы $\sum_{x=1}^{p-1} e^{2\pi i(cx+d/x)/p}$, $c = d = 1$, на выборке из 1600 последовательных простых чисел, когда сумма фиксирована. Проведено сопоставление доказанного случая А) с результатами вычислений случая Б).

Методика вычислений и их обработка. Интервал $[0, \pi]$ разбиваем на 20 подынтервалов $U_i = [(i-1)\pi/20, i\pi/20]$, $i = 1, 2, \ldots, 20$, i — номер интервала U_i, $\nu(U_i)$ — количество углов θ_j (где j, $1 \le j \le n$, — номер последовательного простого числа), попавших в интервал U_i, $h(U_i)$ — гипотетическое количество углов θ_j, содержащихся в интервале U_i, для данной выборки при $\sin^2 t$-распределении, $p_i = (2/\pi)\int_{U_i}\sin^2 dt$, $h(U_i) = \|np_i\|$, где $\|\alpha\|$ — ближайшее целое к α, n — число элементов в выборке.

Случай А. Вычисления и теория показывают, что распределения значений углов $\theta_p(c, d)$ сумм $T_p(c, d) = \sum_{x=1}^{p-1} e^{2\pi i(cx+d/x)/p}$ по интервалам $U_i = [(i-1)\pi/20, i\pi/20]$, $i = 1, 2, \ldots, 20$, при $c = \mathrm{const}$, $1 \le d \le p-1$ одинаково при различных $1 \le c \le p-1$. Вследствие этого далее приводятся экспериментальные

данные распределения углов сумм $T_p(c, d)$ при $c = \text{const}$, $1 \le d \le p-1$. Например, при $p = 1597$, $c = 890$, $1 \le d \le p-1$ распределения углов $\theta_p(c, d)$ приведены в табл. 1.

Таблица 1

i	$\nu(U_i)$	$h(U_i)$	i	$\nu(U_i)$	$h(U_i)$
1	0	1	11	154	158
2	6	9	12	158	151
3	29	24	13	141	136
4	51	44	14	109	116
5	65	67	15	99	92
6	90	92	16	70	67
7	111	116	17	44	44
8	134	136	18	18	24
9	154	151	19	7	9
10	153	153	20	3	1

Подсчитаем теперь по χ^2-критерию Пирсона [16] вероятность отвергнуть гипотезу о $\sin^2 t$-распределении, используя данные таблицы. Поскольку в каждый интервал должно попадать не менее 10 значений, объединяем интервалы U_1 и U_2 и интервалы U_{19} и U_{20}.

Утверждение 1. *В случае* А *для таблицы* 1 *с* 16 *степенями свободы* $\chi^2 = 7{,}52$.

Случай Б. Данные распределения углов θ_p на выборке из 1600 последовательных простых чисел от 2 до 13499 приведены в табл. 2.

Таблица 2

i	$\nu(U_i)$	$h(U_i)$	i	$\nu(U_i)$	$h(U_i)$
1	0	1	11	164	159
2	7	9	12	141	151
3	25	24	13	150	136
4	41	44	14	128	116
5	66	68	15	106	92
6	98	92	16	67	68
7	99	116	17	40	44
8	132	136	18	25	24
9	152	151	19	2	9
10	156	159	20	1	1

Обработка результатов вычислений по χ^2-критерию Пирсона аналогична случаю А). Из таблиц [16] следует, что с вероятностью 0,95 величина χ^2 должна лежать в интервале $[0; 26{,}296]$ в случае А) и в интервале $[0; 24{,}996]$ в случае Б).

Утверждение 2. *В случае* Б) *с* 15 *степенями свободы* $\chi^2 = 10{,}43$.

С 5% уровнем значимости по χ^2-критерию Пирсона гипотеза о равнораспределенности углов θ_p на интервале $[0, \pi]$ с функцией плотности $(2/\pi)\sin^2 t$ верна.

Параметрические пространства, разделяющие оценки и рациональные точки на кривых вида $y^2 = f(x)$ над простым конечным полем. Пусть $n \ge 3$ — нечетное число, $p > 2$ — простое число, $f(x)$ — унитарный многочлен степени n, $f(x) \in F_p[x]$. Рассмотрим кривую

$$y^2 = f(x). \tag{12}$$

Кривые вида (12) параметризуются точками афинного пространства $A^n(F_p)$ размерности n над полем F_p. Назовем параметрическое пространство над полем k *факторизующим*, если любая кривая, лежащая над этим пространством, имеет точку в поле k. В противном случае пространство называем *нефакторизующим*.

Если зафиксировать степень n многочлена f, из известных оценок Хассе и А.Вейля для числа решений (12) вытекает следующее утверждение.

Предложение 1. *При достаточно большом $p \geq p_0$ (граница p_0 зависит от n) пространство $A^n(F_p)$ является факторизующим для кривых* (12).

Рассмотрим случай малых n. При $n = 3$ кривая (12) всегда имеет решение при $p > 3$, т. е. параметрическое пространство кубических кривых вида (12) является факторизующим при $p > 3$. В случае $n \geq 5$ из работы [17] следует, что при $p > (n+1)^2/2 - 2$ (оценка Д. А. Митькина) пространства $A^n(F_p)$ являются факторизующими для кривых (12). Если оценка Д. А. Митькина не выполнена, то пространство может не быть факторизующим. Кривая $y^2 = x^5 + x^4 + 7x^3 + 8x^2 + 3x + 8$ лежит над точкой $(1, 7, 8, 3, 8) \in A^5(F_{11})$ и не имеет решений в F_p. В то же время оценка Д. А. Митькина, как и оценки Хассе и Вейля, не является необходимой. Вычисления [18] показали, что пространство $A^5(F_{13})$ является факторизующим для кривых (12), хотя в этом случае $p < (n+1)^2/2 - 2$. Аналогичные результаты верны и для оценок Серра [19, 20]. Рассмотрим гиперэллиптическую кривую C_g рода $g \geq 2$ над F_p. Для проективного замыкания C_g квазипроективное пространство

$$H_{g,p} = \left(P^{2g+1}(F_p) \setminus (\mathrm{Disk}(C_g) = 0)\right),$$

где $\mathrm{Disk}(C_g)$ — дискриминант кривой C_g, параметризует все гиперэллиптические кривые рода g над F_p. Согласно приведенной оценке, при $p \geq 17$ любая гиперэллиптическая кривая рода 2 имеет точки в F_p для таких простых p. Аналогично, для $g = 3$ любая гиперэллиптическая кривая рода 3 имеет точки в F_p для $p \geq 37$. Для $p = 3, 5, 7, 11$ имеются примеры кривых, которые не имеют точек в F_p. Согласно вычислениям [18], любая кривая рода 2 над F_{13} имеет точки в этом поле. Из тех же вычислений видно, что для $p = 3, 5, 7, 11, 13, 17$ существуют примеры кривых, которые не имеют точек в F_p.

Сформулируем результаты в виде отдельного утверждения.

Предложение 2. *Оценки Хассе, Вейля, Митькина, Серра в афинном и проективном вариантах являются достаточными для того, чтобы пространства соответственно $A^n(F_p)$ и $H_{g,p}$ были факторизующими, но не являются необходимыми.*

Приведенные выше рассмотрения приводят к следующей задаче, которую будем называть задачей А. Г. Постникова. Для ее формулировки введем необходимые понятия и определения.

Пусть $\{\Im_{g,p}\}$ — семейство параметрических пространств с параметрами g и p, $c \in \Im_{g,p}$ — некоторый элемент, $\#c$ — его некоторая числовая характеристика, $b(g, p, \#c)$ — некоторая оценка, выполняющаяся для всех элементов $c \in \Im_{g,p}$. Пусть $\Re(c, b(g, p, \#c))$ — некоторый предикат на элементах $\Im_{g,p}$. Будем говорить, что оценка $b(g, p, \#c)$ *разделяет* (*точно разделяет*) семейство $\{\Im_{g,p}\}$, если для данного $g = \mathrm{const}$ существует $p = p_0(g)$ такое, что для

любого $p \geq p_0(g)$ и для всех $c \in \mathfrak{I}_{g,p}$ предикат $\Re(c, b) = \text{TRUE}$, и для $p \leq p_0(g)$ (для каждого g и для каждого $p \leq p_0(g)$) существуют $c \in \mathfrak{I}_{g,p}$ с $\Re(c, b) = \text{FALSE}$. Точно разделяющую оценку будем называть *точной оценкой*.

Пусть $\mathfrak{I}_{g,p} := H_{g,p}$ — параметрическое пространство гиперэллиптических кривых рода g, $C_g \in H_{g,p}$, $\#C_g$ — число точек кривой C_g в F_p, т. е. в предыдущих обозначениях $c = C_g$.

Задача Постникова (проблема точной оценки). Существует ли для семейства $\{H_{g,p}\}$ пространств гиперэллиптических кривых точная оценка, разделяющая это семейство на факторизующие и нефакторизующие пространства? Если такая оценка существует, то какой ее вид?

В настоящее время автору неизвестно решение этой задачи.

Исследование арифметических свойств объектов, параметризуемых подпространствами пространства модулей, в настоящее время активно развивается [1]. Поставим вопрос о существовании таких параметрических пространств, у которых существуют сечения, над которыми лежат кривые, не имеющие рациональных точек в F_p.

Теорема 3. *Пусть* $A^{(p-1)/2}(F_p)$ — *параметрическое пространство кривых вида* (12), *а простое* $p \equiv 3 \pmod 4$. *Тогда при* $p \geq 11$ *над его сечением* $(a_1, \ldots, a_{(p-3)/2}) = (0, \ldots, 0)$ *существуют кривые с* $a_{(p-1)/2} \neq 0$, *не имеющие решений над* F_p.

Доказательство проводим по схеме А. Г. Постникова [18]. При $p = 11$ такой кривой является $y^2 = x^5 + 7$. Пусть $p > 11$, y^2 принимает квадратичные вычеты и значение 0; $x^{(p-1)/2}$ принимает три значения: -1, 0, 1. Если в ряду $0, 1, 2, \ldots, p-1$ встречается комбинация „невычет, невычет, невычет", то взяв за точку сечения среднее из этих чисел, получим требуемую кривую. Пусть $\left(\frac{a}{p}\right)$ — символ Лежандра. Количество комбинаций „невычет, невычет, невычет" задается формулой

$$T = \frac{1}{8}\sum_{x=2}^{p-2}\left(1-\left(\frac{x-1}{p}\right)\right)\left(1-\left(\frac{x}{p}\right)\right)\left(1-\left(\frac{x+1}{p}\right)\right) =$$

$$= \frac{1}{8}\sum_{x=0}^{p-1}\left(1-\left(\frac{x-1}{p}\right)\right)\left(1-\left(\frac{x}{p}\right)\right)\left(1-\left(\frac{x+1}{p}\right)\right) + \frac{\theta}{2}, \quad |\theta| \leq 1.$$

Далее,

$$T = \frac{1}{8}\left[p + \sum_0^{p-1}\left(\frac{(x-1)x}{p}\right) + \sum_0^{p-1}\left(\frac{(x-1)(x+1)}{p}\right) + \sum_0^{p-1}\left(\frac{x(x-1)}{p}\right) - \sum_0^{p-1}\left(\frac{(x-1)x(x+1)}{p}\right)\right] +$$

$$+ \frac{\theta}{2} = \frac{1}{8}\left[p - 3 + \sum_0^{p-1}\left(\frac{(x-1)x(x+1)}{p}\right)\right] + \frac{\theta}{2} > \frac{1}{8}\left(p - 3 - 2\sqrt{p}\right) - \frac{1}{2}.$$

Чтобы T было больше нуля, достаточно выполнения неравенства $p - 3 - 2\sqrt{p} - 4 > 0$, что имеет место при $p \geq 19$. Теорема доказана.

В настоящее время активно исследуются задачи существования и точных значений числа рациональных точек кривых рода больше единицы над полями F_p [19, 20]. Теорема 3 дает возможность указать класс кривых рода больше единицы, не имеющих решений в F_p. Пусть $\text{Disc}(f)$ обозначает дискриминант многочлена f из теоремы 3 и $p = 4m + 3$.

Следствие. *В условиях теоремы* 3 *над сечением* $(a_1, \ldots, a_{(p-1)/3}) = (0, \ldots, 0)$

параметрического пространства гиперэллиптических кривых над F_p *при* $p > 11$ *лежат гиперэллиптические кривые рода* $(p-3)/4$, *не имеющие решений над* F_p.

Доказательство. В этом случае параметрическое пространство имеет вид $A^{(p-1)/2}(F_p) \setminus (\mathrm{Disc}(f) = 0)$. Дискриминант правой части уравнения $y^2 = x^{(p-1)/2} + a_{(p-1)/2}$, существующего при $p \geq 11$ согласно теореме 3, равен

$$\left(\frac{p-1}{2}\right)^{(p-1)/2} a_{(p-1)/2} \neq 0.$$

Следствие доказано.

1. *Harris J.,Morrison J.* Moduli of curves. – Berlin; New York: Springer, 1998. – 366 p.
2. *Серр Ж.-П.* Абелевы 1-адические представления и эллиптические кривые. – М.: Мир, 1973. – 191 с.
3. *Duke W.,Friedlander J., Iwaniec H.* Bilinear forms with Kloosterman fractions // Invent. math. – 1997. – **128**. – P. 23 – 43.
4. *Livne R.* The average distribution of cubic exponential sums // J. reine und angew. Math. – 1987. – **375/6**. – S. 362 – 379.
5. *Katz N. M.* Gauss sums, Kloosterman sums, and monodromy groups. – Princeton: Princeton Univ. Press, 1988. – 186 p.
6. *Линник Ю. В.* Эргодические свойства алгебраических полей. – Л.: Изд-во Ленингр. ун-та, 1967. – 208 с.
7. *Adolphson A.* On the distribution of angles of Kloosterman sums // J. reine und angew. Math. – 1989. – **395**. – S. 214 – 220.
8. *Glazunov N. M.* On distribution and values of of Kloosterman sums $Tp(c,d)$ for primes ≤ 13499 // Represantation Theory and Computer Algebra. – Kiev: Math. Inst. NASU Ukraine, 1997. – P. 51.
9. *Гельфонд А. О., Линник Ю. В.* Элементарные методы в аналитической теории чисел. – М.: Физматгиз, 1962. – 272 с.
10. *Постников А. Г.* Эргодические вопросы теории сравнений и теории диофантовых приближений. – М.: Наука, 1966. – 112 с.
11. *Степанов С. А.* Конструктивный метод в теории уравнений над конечными полями // Тр. Мат. ин-та АН СССР. – 1973. – **132**. – С. 237 – 246.
12. *Glazunov N. M.* Moduli, periods, modular symbols and how to compute them // Braket. – Stockholm Univ., 1998. – P. 3.
13. *Glazunov N. M.* On two moduli problems concerning number of points and equidistribution over prime finite fields // Proc. Int. Conf. Discrete Methods in Control Systems. – Krasnovidovo-Moscow: Moscow State Univ., 1998. – P. 23 – 25.
14. *Silverman J. H.* Advanced topics in the arithmetic of elliptic curves. – Berlin; New York: Springer, 1994. – 430 p.
15. *Серр Ж.-П.* Алгебраические группы и поля классов. – М.: Мир, 1975. – 475 с.
16. *Крамер Г.* Математические методы статистики. – М.: Мир, 1975. – 475 с.
17. *Митькин Д. А.* Существование рациональных точек на гиперэллиптической кривой над простым конечным полем // Вест. Моск. ун-та. Математика и механика. – 1975. – № 6. – С. 86 – 90.
18. *Глазунов Н. М., Постников А. Г.* О существовании рациональных точек на кривой над простым конечным полем // Исследования по теории чисел. – Саратов: Саратов. ун-т, 1988. – С. 4 – 8.
19. *Lauter K.* Non-existence of a curve over F_3 of genus 5 with 14 rational points. – Bonn, 1998. – 6 p. – (Preprint / Max-Planck Institut).
20. *Serre J.-P.* Lectures on the Mordell – Weil theorem. – Braunschweig: Vieweg, 1990. – 218 p.

Получено 14.03.2000,
после доработки — 15.08.2000