Отчет о научной деятельности за 2015 г.

Алексеенко Екатерины Сергеевны, старшего преподавателя кафедры «Компьютерной безопасности» Института Прикладной математики и информационных технологий Балтийского Федерального университета им. И.Канта.

1. Результаты, полученные за весь период

В течение всего периода получения стипендии удалось получить все заявленные ранее результаты. А именно, найти явный вид кривых рода три над конечными полями с большим числом рациональных точек. Подход строится на эквивалентности категорий обычных абелевых многообразий и эрмитовых модулей, построенной Серром и Делинем в общем случае обычных многообразий. Используя данную эквивалентность категорий и классификацию эрмитовых модулей над квадратичными полями с числом классов, равным единице, удалось описать свойства якобианов искомых кривых явным образом, при условии их существования.

Одним из подходов является нахождение степени накрытия оптимальной эллиптической кривой искомой кривой и вычисление явным образом базиса пространства Римана-Роха, что дает возможность записать уравнение кривой в явном виде.

Второй метод заключается в построении канонического подъема якобиана кривой с комплексным умножением рода три до якобиана римановой поверхности с заданной группой автоморфизмов. После классификации римановых поверхностей по их полной группе автоморфизмов сделана редукция и проверка полученной кривой на оптимальность.

Более подробно наши методы могут быть описаны следующим образом. Пусть C – неприводимая гладкая алгебраическая кривая рода g. Если число рациональных точек кривой C удовлетворяет границе Хассе-Вейля-Серра:

$$|\#C(\mathbb{F}_q) - q - 1| \leq g[2\sqrt{q}],$$

то кривая называется оптимальной над $\mathbb{F}_q$ (минимальной или максимальной).

Пусть C – оптимальная кривая рода g над $\mathbb{F}_q$. Тогда относительный автоморфизм Фробениуса индуцирует гомоморфизм

$$\mathrm{F} : \mathrm{T}_l\mathrm{Jac}(C) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{T}_l\mathrm{Jac}(C) \otimes_{\mathbb{Z}} \mathbb{Q},$$

где $\mathrm{T}_l\mathrm{Jac}(C)$ – проективный предел системы $\varprojlim \mathrm{Jac}(C)[l^n]$. Более того, если характеристический многочлен $\mathrm{Jac}(C)$ разложить на линейные множители

$$\mathrm{P}_{\mathrm{Jac}(C)}(T) = \prod_{i=1}^{2g}(T - \alpha_i),$$

то число рациональных точек на C равно

$$\#C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{g}\alpha_i = q + 1 - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha}_i),$$

где $\alpha_{i+g} = \overline{\alpha}_i$. Собственные значения эндоморфизма Фробениуса F обладают следующим свойством: $\alpha_i + \bar{\alpha}_i = -[2\sqrt{q}]$, когда C максимальная, и $\alpha_i + \bar{\alpha}_i = [2\sqrt{q}]$, когда C минимальная. Поэтому, если кривая оптимальна, то ее L-многочлен определяется следующим образом:

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t) = \prod_{i=1}^{g}(1 \mp [2\sqrt{q}]t + qt^2)$$

для минимальной (максимальной) кривой. Теория Хонды-Тэйта показывает, что якобиан $\mathrm{Jac}(C)$ максимальной (минимальной) кривой C изогенен произведению копий одной максимальной (минимальной) эллиптической кривой, то есть $\mathrm{Jac}(C) \sim E^g$, где E – оптимальная эллиптическая кривая над конечным полем $\mathbb{F}_q$. Класс изогении E над конечным полем $\mathbb{F}_q$ характеризуется характеристическим многочленом эндоморфизма Фробениуса на E.

Рассмотрим эквивалентность категорий обычных абелевых многообразий вида $\mathbb{F}_q$, которые изогенны E^g (и, следовательно, E – обычная эллиптическая кривая), и категорию R-модулей, где R – кольцо, определяемое Фробениусом эллиптической кривой E. Относительно вводимых ограничений на поле $\mathbb{F}_q$ мы имеем $R = \mathcal{O}_K$, где $K = \mathbb{Q}(\sqrt{-d})$ – некоторое мнимое квадратичное числовое поле. Пусть $\mathrm{Jac}(C)$ – главно поляризованный якобиан кривой C с тэта-дивизором θ. Тогда по теореме Торелли кривая C полностью определяется $(\mathrm{Jac}(C), \theta)$ с точностью до изоморфизма над алгебраическим замыканием $\bar{\mathbb{F}}_q$. Рассмотрим эрмитов модуль $(\mathcal{O}_K^g; h)$, где $\mathcal{O}_K^g$ – это $\mathcal{O}_K$-модуль, и $h : \mathcal{O}_K^g \times \mathcal{O}_K^g \to \mathcal{O}_K$ – эрмитова форма. Эквивалентность категорий определяет функтор $\mathcal{F} : \mathrm{Jac}(C) \longrightarrow \mathrm{Hom}(E, \mathrm{Jac}(C))$ и его обратный функтор $\mathcal{V} : \mathcal{O}_K^g \longrightarrow \mathcal{O}_K^g \otimes_{\mathcal{O}_K} E$. Относительно этой эквивалентности поляризация якобиана $\mathrm{Jac}(C)$

соответствует эрмитовой $\mathcal{O}_K$-форме h. Поэтому мы можем использовать классификацию эрмитовых форм и свойства этих классов для описания и построения оптимальных кривых.

Рассмотрим оптимальную кривую C рода $g(C) = 3$ над конечным полем $\mathbb{F}_q$ с дискриминантом $d(\mathbb{F}_q) \in \{-19, -43, -67, -163\}$. С помощью классификации эрмитовых модулей с такими дискриминантами доказано, что оптимальную кривую можно рассматривать как двойное накрытие эллиптической оптимальной кривой.

Кроме того, были доказаны следующие результаты:

(1) Оптимальная кривая $C/\mathbb{F}_q$ не является гиперэллиптической.
(2) Над полем $\mathbb{F}_q$ одновременно не может существовать минимальной и максимальной кривых рода три.
(3) $\mathrm{Aut}_{\mathbb{F}_q}(C) \cong D_3$, где D_3 – диэдральная группа порядка 6.

Используя доказанные свойства и теорию функциональных полей, был описан первый метод получения явных уравнений оптимальной кривой. А именно, были построены явные базисы пространств Римана-Роха, ассоциированных с дивизором, кратным бесконечно удаленной точке, относительно фиксированного морфизма в $\mathbb{P}^1$. Используя данные базисы, были найдены соотношения, которые в дальнейшем позволили найти явные уравнения кривых.

Теорема 1.1. *Оптимальная кривая C задается следующими уравнениями:*

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, a, b$ - коэффициенты из $\mathbb{F}_q$. Эллиптическая кривая E задана уравнением $y^2 = x^3 + ax + b$.

Используя инвариантность пространства Римана-Роха, которое строится, было найдено явное представление группы автоморфизмов относительно базисов этого пространства, ассоциированного с дивизором с носителем в бесконечно удаленной точке. Используя данное представление были найдены зависимости между параметрами уравнения кривой.

Теорема 1.2. *Если $\mathbb{F}_q$ – конечное поле с дискриминантом $d \in \{-19, -43, -67, -163\}$, то существует оптимальная кривая*

С рода три со следующим уравнением:

$$a(X^4+Y^4+Z^4)+b(X^3Y+XY^3+X^3Z-Y^3Z+XZ^3-YZ^3)+$$
$$+c(X^2Y^2+X^2Z^2+Y^2Z^2)+(XYZ^2+XY^2Z-X^2YZ)=0$$

для $a, b, c \in \mathbb{F}_q$.

Также мною был изложен метод нахождения уравнения кривой рода четыре над полем $\mathbb{F}_{5^7}$ с дискриминантом -19, основанный на идее Э. Хау. Кривая строится с помощью двойных накрытий рода два эллиптической кривой, определенной над $\mathbb{F}_5$.

Итогом работы прошедших лет явилась кандидатская диссертация на тему «Явные конструкции оптимальных кривых рода три», защита которой назначена на 19 января 2016 года в ИППИ РАН им. А.А. Харкевича.

2. Результаты, полученные в этом году

За прошедший год я занималась вопросом приложений гипербентных функций к кривым над конечными полями. К сожалению, полученный мною результат и подход (как выяснилось позже), касающийся переформулирования критерия Чарпина-Гонга в терминах числа $\mathbb{F}_{2^n}$-рациональных точек, совпал с результатами польских математиков. Поэтому в этом направлении новых результатов нет.

В настоящее время я занимаюсь исследованием оболочки Галуа некоторой башни функциональных полей над конечными полями. Другими словами, я исследую башню $\tilde{\mathcal{T}} = \{\tilde{T_1}, \tilde{T_2}, \tilde{T_3}, \tilde{T_4}, \ldots\}$, где $\tilde{T_i}$ – оболочка Галуа расширения T_i/T_1 для $i \geq 2$ и $\mathcal{T} = \{T_1, T_2, T_3, T_4, \ldots\}$ – вторая башня Штихтинота-Гарсиа. На данный момент найдены три минимальных многочлена, порождающих $\tilde{T_4}$ над $\tilde{T_3}$, группа Галуа и ее действия на порождающие элементы явно. Кроме того, думаю, что в ближайшее время удастся определить, является ли $\mathbb{F}_{p^2}$ полным полем констант функционального поля $\tilde{T_4}$, число точек $N(\tilde{T_4})$, род $g(\tilde{T_4})$, исследовать вопрос оптимальности башни $\tilde{\mathcal{T}}$. По итогам исследовательской работы планируется публикация статьи.

3. Опубликованные и поданные в печать работы

1. E. Alekseenko, A. Zaytsev. «Explicit equations of optimal curves of genus 3 over certain finite fields with three parameters». Contemporary Mathematics, in Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 637: 245 – 251, 2015.

4. Участие в конференциях и школах

1. Конференция фонда «Династия» Д.Зимина «Встреча поколений». Место проведения: Россия, г. Москва, НМУ, июнь 2015 г. Выступление с докладом по тематике диссертации.

2. Летняя школа-семинар «Алгебраические многообразия и коды, исправляющие ошибки». Место проведения: Россия, г. Калининград, БФУ им. И.Канта, июль 2015 г. Выступление с докладом по тематике диссертации.

5. Работа в научных центрах и международных группах

Являюсь младшим научным сотрудником лаборатории “Математические методы защиты и обработки информации” в инновационном парке БФУ им. И. Канта.

6. Педагогическая деятельность (включая научное руководство)

1. Являюсь участником семинара "Алгебраическая геометрия и ее приложения"на базе лаборатории "Математические методы защиты и обработки информации".

2. Преподаю на кафедре "Компьютерной безопасности"следующие дисциплины:

- "Прикладная алгебра";
- "Теоретико-числовые методы в криптографии";
- "Быстрые мультипликаторы";
- "Введение в алгебраическую теорию чисел и криптографию в квадратичных полях";
- "Методы вычисления дискретного логарифма";
- "Методы и алгоритмы генерации эллиптических кривых для криптографии".