Отчет о научной деятельности

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

1. Результаты, полученные в этом году

В работе я рассматриваю абсолютно неприводимые, проективные, гладкие кривые $C/\mathbb{F}_q$ рода 3 над конечными полями $\mathbb{F}_q$ с дискриминантами $d(\mathbb{F}_q) \in \{-19, -43, -67, -163\}$, которые являются оптимальными кривыми, т.е. число их точек удовлетворяет границе Хассе-Вейля-Серре:

$$|C(\mathbb{F}_q)| = q + 1 \pm \lfloor 2\sqrt{q} \rfloor g.$$

Мною был реализован метод построения явных уравнений оптимальных кривых рода 3 над конечными полями с рассматриваемыми дискриминантами с помощью заданной группы автоморфизмов. Для этого были сформулированы и доказаны следующие предложения:

1. Оптимальная кривая $C/\mathbb{F}_q$ рода 3 является двойным накрытием оптимальной эллиптической кривой.
2. Оптимальная кривая $C/\mathbb{F}_q$ рода 3 не является гиперэллиптической.
3. Над полем $\mathbb{F}_q$ одновременно не могут существовать максимальная и минимальная кривые рода 3.
4. $\mathrm{Aut}_{\mathbb{F}_q}(C) \cong D_3$, где D_3 - группа Диэдра порядка 6.

Результатом работы является следующая теорема:

Теорема 1.1. *Если оптимальная кривая C рода три определена над конечным полем $\mathbb{F}_q$ с дискриминантом $d \in \{-19, -43, -67, -163\}$, то ее уравнение имеет следующий вид:*

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

для некоторых констант a, b, c, $d \in \mathbb{F}_q$.

Явные уравнения оптимальных кривых могут быть получены с помощью следующего алгоритма:

Алгоритм 1.2.

Require: $p = \mathrm{char}(\mathbb{F}_p)$, α, β, *где* $E(d) : y^2+y = x^3-\alpha x+\beta$- *кривая Гросса,* $\chi(d)$- *зигелева модулярная форма;*
Ensure: a, b, c- *коэффициенты оптимальной кривой* $C(\mathbb{F}_p)$;

$n := \#E(d)(\mathbb{F}_q)$;
$jInvariant := \frac{(48\alpha)^3}{16\alpha^3-27(1+4\beta)^2}$;
if $n = p + 1 + \lfloor 2\sqrt{p} \rfloor$ ***then***
  $type := max$;
else
  $type := min$;
if $\left(\left(\frac{\chi}{p}\right) = 1 \ and \ type = max\right) \ or \ \left(\left(\frac{\chi}{p}\right) = -1 \ and \ type = min\right)$ ***then***
  $NumberOfPoints := p + 1 + 3\lfloor 2\sqrt{p} \rfloor$;
if $\left(\left(\frac{\chi}{p}\right) = 1 \ and \ type = min\right) \ or \ \left(\left(\frac{\chi}{p}\right) = -1 \ and \ type = max\right)$ ***then***
  $NumberOfPoints := p + 1 - 3\lfloor 2\sqrt{p} \rfloor$;
for $a = 1, \ldots, p-1$ ***do***
  for $b = 1, \ldots, p-1$ ***do***
    for $c = 1, \ldots, p-1$ ***do***
      $A := \frac{20}{3}b + \frac{32}{3}a + \frac{128}{3}ac + \frac{56}{3}bc + \frac{8}{3}c^2 + \frac{256}{3}ac^2 + \frac{16}{3}bc^2 - \frac{160}{3}a^2 - \frac{176}{3}ab - \frac{256}{3}abc + 64a^2b + 128ab^2 - \frac{70}{3}b^2 - 96a^2b^2 - 80ab^3 + 128ab^2c + 256a^3b - \frac{88}{3}b^2c^2 + 40b^3c + \frac{64}{3}abc^2 - 128a^2bc - \frac{32}{3}bc^3 - \frac{512}{3}a^2c - \frac{640}{3}a^2c^2 + 256a^4 + 28b^3 - \frac{176}{3}b^2c - 11b^4 - \frac{16}{3}c^4 - \frac{1}{3} + \frac{256}{3}ac^3 \bmod p$;
      $B := \frac{20}{9}b + \frac{32}{9}a + \frac{128}{9}ac + \frac{56}{9}bc + \frac{8}{9}c^2 + \frac{128}{9}ac^2 - \frac{64}{9}bc^2 - \frac{416}{9}a^2 - \frac{496}{9}ab + \frac{3584}{27}a^3 - \frac{2432}{9}abc + \frac{2048}{9}a^2b + \frac{1664}{9}ab^2 - \frac{170}{9}b^2 - 128a^2b^2 - \frac{992}{3}ab^3 + \frac{20}{9}b + \frac{32}{9}a - \frac{3904}{27}b^3c^3 - \frac{8192}{9}a^2c^3 + \frac{14336}{9}a^3c^2 + \frac{26624}{27}a^3c^3 - \frac{4096}{3}a^5c + \frac{2240}{3}ab^2c + 512a^3b - 128b^2c^2 + \frac{1040}{9}b^3c - 384abc^2 + \frac{3584}{3}a^2bc + \frac{128}{9}bc^5 - \frac{256}{9}bc^3 - \frac{8192}{3}a^4b - \frac{4096}{3}a^3b^2 - 1024a^3b^3 + \frac{1664}{3}a^2b^3 + \frac{2464}{3}ab^4 - 624ab^5 + \frac{1280}{9}ac^5 - \frac{736}{9}b^2c^4 - \frac{2560}{9}a^2c - 640a^2c^2 + \frac{1024}{3}a^4 - \frac{64}{9}bc^4 - \frac{2}{27} + \frac{1352}{27}b^3 - \frac{736}{9}b^2c + \frac{128}{27}c^6 - \frac{4096}{3}a^5 - 122b^4 - \frac{248}{3}b^4c^2 - 1632a^2b^4 + \frac{3392}{9}ab^2c^3 + \frac{4352}{3}a^3b^2c - 1152a^2b^2c^2 + \frac{3136}{3}ab^4c - \frac{7168}{9}a^2c^4 - 70b^6 + \frac{2048}{3}a^4c^2 + \frac{476}{3}b^5 - \frac{32}{9}c^4 - \frac{1088}{9}b^2c^3 + \frac{1280}{9}ac^4 - \frac{800}{3}b^4c - \frac{352}{9}b^3c^2 + \frac{680}{3}b^5c + \frac{8960}{9}a^3c + \frac{320}{9}ac^3 + \frac{2816}{3}a^2bc^2 - \frac{512}{3}a^3bc - 1280a^2b^2c + \frac{2816}{3}a^2b^3c - \frac{2048}{3}a^4bc + \frac{512}{3}ab^3c^2 - \frac{7168}{9}a^2bc^3 - 512ab^3c + \frac{2816}{3}ab^2c^2 - \frac{640}{9}abc^3 + \frac{4096}{3}a^3bc^2 + \frac{1024}{9}abc^4 \bmod p$;

$\delta := -16(4A^3 + 27B^2)$;
$j := -1728 \cdot \frac{(4A)^3}{\delta}$;
if $j = jInvariant$ *and* $\#C(\mathbb{F}_p) = NumberOfPoints$ ***then***
return a, b, c;

С помощью описанного метода для соответствующих дискриминантов были получены кривые (я привожу лишь по паре для каждого дискриминанта):

Пример 1.3. *Оптимальные кривые над конечными полями с дискриминантом* $d(\mathbb{F}_q) = -19$*:*

q	Максимальная кривая	Минимальная кривая
	$[a, b, c, d]$	$[a, b, c, d]$
47	$[13, 25, 15, 1]$	-
997	-	$[1, 277, 888, 1]$

Пример 1.4. *Оптимальные кривые над конечными полями с дискриминантом* $d(\mathbb{F}_q) = -43$*:*

q	Максимальная кривая	Минимальная кривая
	$[a, b, c, d]$	$[a, b, c, d]$
167	-	$[9, 143, 133, 1]$
941	$[1, 551, 836, 1]$	-

Пример 1.5. *Оптимальные кривые над конечными полями с дискриминантом* $d(\mathbb{F}_q) = -67$*:*

q	Максимальная кривая	Минимальная кривая
	$[a, b, c, d]$	$[a, b, c, d]$
359	-	$[2, 198, 1, 1]$
947	$[8, 90, 612, 1]$	-

Пример 1.6. *Оптимальные кривые над конечными полями с дискриминантом* $d(\mathbb{F}_q) = -163$*:*

q	Максимальная кривая	Минимальная кривая
	$[a, b, c, d]$	$[a, b, c, d]$
1847	-	$[1, 702, 964, 1]$
1933	$[1, 1478, 42, 1]$	-

2. Опубликованные и поданные в печать работы

Опубликованных работ за этот год не имею.

По результатам проделанной работы готова статья, которую планирую подать в Tohoku Mathematical Journal.

3. Участие в конференциях и школах

1. Вторая международная конференция "Арифметические дни". Выступала с докладом. Место проведения: Россия, г. Санкт-Петербург. Сроки: 20-23 мая 2013 г.

2. AGCT-14 (14-ая международная конференция по арифметике, геометрии, криптографии и теории кодирования). Выступала с докладом. Место проведения: Франция, Люмини. Сроки: 3-7 июня 2013 г.

4. Работа в научных центрах и международных группах

–

5. 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";
- "Теория псевдослучайных генераторов";
- "Быстрые мультипликаторы";
- "Теоретико-числовые методы в криптографии";
- "Введение в алгебраическую теорию чисел и криптографию в квадратичных полях";

- "Методы вычисления дискретного логарифма".