16. *Barbour A. D., Holst L., and Janson S.* Poisson Approximation. Oxford: Oxford Univ. Press, 1992. 277 p.
17. *Михайлов В. Г., Шойтов А. М.* О длинных повторениях цепочек в цепи Маркова // Дискрет. матем. 2014. Т. 26. № 3. С. 79–89.
18. *Minakov A. A.* Poisson approximation for the number of non-decreasing runs in Markov chains // Матем. вопр. криптогр. 2018. Т. 9. № 2. С. 103–116.

УДК 512.772 DOI 10.17223/2226308X/12/5

ХАРАКТЕРИСТИЧЕСКИЕ МНОГОЧЛЕНЫ НЕКОТОРЫХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ РОДОВ 2,3 И p-РАНГА 1[1]

Е. М. Мельничук, С. А. Новоселов

Исследуются характеристические многочлены некоторых классов гиперэллиптических кривых рода $2, 3$ p-ранга 1 над конечным полем. p-Ранг является важным инвариантом кривой, который накладывает ограничения на характеристический многочлен кривой и, следовательно, на число точек в её якобиане. Получены сравнения (по модулю характеристики) и ограничения на коэффициенты для характеристических многочленов кривых p-ранга 1 с автоморфизмами.

Ключевые слова: *гиперэллиптические кривые, p-ранг, характеристические многочлены, группа автоморфизмов.*

Введение

Гиперэллиптическая кривая C рода g над конечным полем $\mathbb{F}_q$ задаётся уравнением

$$y^2 + h(x)y = f(x),$$

где $h(x), f(x) \in \mathbb{F}_q[x]$ и $\deg h(x) \leqslant g+1$, $\deg f(x) = 2g+1$ или $\deg f(x) = 2g+2$ и многочлен $f(x)$ является унитарным.

В настоящее время гиперэллиптические кривые изучаются как альтернатива эллиптическим кривым. Гиперэллиптические кривые требуют меньший размер ключа при сравнимом уровне безопасности. Одними из перспективных направлений в криптографии на (гипер)эллиптических кривых являются классическая криптография на дискретном логарифме, криптография на билинейных спариваниях, постквантовая криптография на изогениях.

Для криптографии на дискретном логарифме необходимы кривые рода 2 и 3 с большим простым числом точек в якобиане. Для кривых больших родов имеются атаки методом исчисления индексов. Для криптографии на билинейных спариваниях, помимо требований для стойкости дискретного логарифма, необходимы кривые с малой степенью вложения. Ярким примером применения криптосистем на билинейных спариваниях является механизм Zk-Snark, применяемый в криптовалюте Zcash. В основе Zk-Snark лежит редуцированное эйт-спаривание. Криптография на изогениях гиперэллиптических кривых в настоящее время только начинает развиваться. Основной проблемой является отсутствие эффективных формул для вычисления изогений.

Множество точек гиперэллиптических кривых рода 2 и 3 не образует группу, в отличие от эллиптических кривых, поэтому для использования таких кривых в криптографии строится ассоциированная с кривой группа — якобиан кривой.

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-31-00244.

Определение 1. Якобианом гиперэллитической кривой C называется факторгруппа

$$J_C = Div^0(C)/Pr(C),$$

где $Div^0(C)$ — множество дивизоров степени 0; $Pr(C)$ — множество главных дивизоров кривой C.

Важным инвариантом гиперэллиптической кривой является p-ранг.

Определение 2. Пусть C — гиперэллиптическая кривая. Тогда $J_C[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^r$ для $0 \leqslant r \leqslant g$ и $e \geqslant 1$. Число r называется p-рангом кривой C.

Хорошо исследованы кривые с p-рангом 0, которые имеют маленькую степень вложения, и p-рангом 2, подавляющее большинство которых имеют большую степень вложения. Для суперсингулярных абелевых многообразий (p-ранг равен 0) известны [1] полные списки возможных характеристических многочленов. Соответственно задача подсчёта точек на суперсингулярных кривых может быть решена простым перебором возможных вариантов. Для кривых p ранга 1 подобных списков в настоящее время не составлено.

В данной работе исследуются характеристические многочлены для кривых p-ранга 1. В силу того, что данные кривые являются промежуточным случаем, мы предполагаем возможность существования как классов кривых с маленькой степенью вложения, так и кривых с большой степенью вложения.

Будем рассматривать классы кривых рода 2, чей p-ранг не превосходит 2, и кривые рода 3, чей p-ранг меньше или равен 3. Среди них выделим кривые p-ранга 1.

1. Характеристический многочлен и p-ранг

L-многочлен кривой связан с p-рангом посредством следующей теоремы.

Теорема 1 (Штихтенот). Пусть $L(T) = a_0 + a_1T + a_2T^2 + \ldots + a_{2g}T^{2g}$, тогда p-ранг кривой C равен

$$\max\{i : a_i \not\equiv 0 \pmod{p}\}.$$

Если кривая имеет автоморфизмы, определённые над некоторым расширением конечного поля, то, в силу следующей теоремы, это накладывает дополнительные ограничения на характеристический многочлен данной кривой.

Теорема 2 [4]. Пусть k — поле, K — расширение поля k, A — абелево многообразие над полем k и $\tau \in \mathrm{End}_K^0(A_K)$, такой, что

1) действие группы $\mathrm{Gal}(K|k)$ на $\mathrm{End}_K^0(A_K)$ отображает подпространство $\mathbb{Q}[\tau] \subset \subset \mathrm{End}_K^0(A_K)$ в себя;
2) τ не определено ни над одним промежуточным полем μ расширения $K|k$, где $\mu \subsetneq K$;
3) $\mathbb{Q}[\tau]$ — поле.

Тогда характеристический многочлен эндоморфизма Фробениуса абелева многообразия A имеет вид $f(T^{[K:k]})$ для некоторого многочлена $f(T) \in \mathbb{Z}[T]$ степени $2\dim(A)/[K:k]$.

Так как якобиан гиперэллиптической кривой является абелевым многообразием, то теорема 2 применима и к гиперэллиптическим кривым. Это позволяет получить следующий результат.

Теорема 3. Пусть дана гиперэллиптическая кривая C рода g, такая, что выполняются условия теоремы 2. Тогда $r_C \geqslant [K:k]$.

Кроме того, имеет место следствие для кривых рода g и p-ранга 1.

Следствие 1. Кривая C рода g может иметь p-ранг 1 только при условии $[K:k]=1$.

Заметим, что следствие не гарантирует наличия p-ранга 1 у кривой C, однако это необходимое условие в контексте теоремы 2. Применим эти результаты к некоторым классам гиперэллиптических кривых.

2. Кривые p-ранга 1 и их характеристические многочлены

Для кривых рода 3 с нетривиальной группой автоморфизмов p-ранг может быть определён с помощью результатов из [3], что позволяет выделить кривые p-ранга 1.

Теорема 4. Пусть гиперэллиптическая кривая $C/\mathbb{F}_p$ рода 3 имеет группу автоморфизмов C_{14}. Тогда уравнение кривой имеет вид $y^2=x^7+1$. Положим

$$v=\binom{(p-1)/2}{5(p-1)/14}+\binom{(p-1)/2}{3(p-1)/14}+\binom{(p-1)/2}{(p-1)/14},\ w=\binom{(p-1)/2}{5(p-1)/14}\binom{(p-1)/2}{3(p-1)/14}+$$
$$+\binom{(p-1)/2}{5(p-1)/14}\binom{(p-1)/2}{(p-1)/14}+\binom{(p-1)/2}{3(p-1)/14}\binom{(p-1)/2}{(p-1)/14}.$$

Тогда кривая C имеет p-ранг 1, если $p\equiv 1 \pmod 7$, $v\not\equiv 0 \pmod p$ и $w\equiv 0 \pmod p$. Кроме того, характеристический многочлен эндоморфизма Фробениуса имеет следующий вид:

$$\chi(\lambda)\equiv\lambda^{2g}+v\lambda^{2g-1} \pmod p.$$

Теорема 5. Пусть группа автоморфизмов G кривой C равна D_{12}. Тогда кривая имеет модель $y^2=x(x^6+\alpha x^3+1)$, где $\alpha\in K$. Обозначим $c=P_{(p-1)/2}(\rho)$, $d=P_{(p-1)/6}(\rho)$, $e=P_{(p-5)/6}(\rho)$, где $\rho=-\alpha/2$ и P_n — многочлены Лежандра. Тогда если $\alpha\neq 0$, то

1) p-ранг кривой равен 1 при $p\equiv 1 \pmod 3$, $c+2d\not\equiv 0 \pmod p$ и $c^2+2cd\equiv\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda)\equiv\lambda^{2g}+(c+2d)\lambda^{2g-1} \pmod p;$$

2) p-ранг равен 1 при $p\equiv 2 \pmod 3$, $c\not\equiv 0 \pmod p$ и $e\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda)\equiv\lambda^{2g}+c\lambda^{2g-1} \pmod p.$$

Теорема 6. Пусть группа автоморфизмов G кривой C равна V_8. Тогда данная кривая имеет вид $y^2=x^8-1$. Пусть

$$s=\binom{(p-1)/2}{3(p-1)/8}+\binom{(p-1)/2}{(p-1)/4}+\binom{(p-1)/2}{(p-1)/8},$$
$$t=\binom{(p-1)/2}{3(p-1)/8}\binom{(p-1)/2}{(p-1)/4}+\binom{(p-1)/2}{3(p-1)/8}\binom{(p-1)/2}{(p-1)/8}+\binom{(p-1)/2}{(p-1)/4}\binom{(p-1)/2}{(p-1)/8}.$$

Тогда

1) если $p\equiv 1 \pmod 8$, то при $s\not\equiv 0, t\equiv 0 \pmod p$ кривая имеет p-ранг 1. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda)\equiv\lambda^{2g}+w\lambda^{2g-1} \pmod p;$$

2) если $p \equiv 5 \pmod 8$ и $r = \binom{(p-1)/2}{(p-1)/4}$, то при $r \not\equiv 0 \pmod p$ кривая имеет p-ранг 1. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda) \equiv \lambda^{2g} + r\lambda^{2g-1} \pmod p.$$

Теорема 7. Пусть группа автоморфизмов G кривой C равна $D_8 \times C_2$. Тогда кривая имеет модель $y^2 = x^8 + \alpha x^4 + 1$, где $\alpha \in K$. Пусть $a = P_{(p-1)/4}(\rho)$, $b = P_{(p-3)/4}(\rho)$, $c = P_{(p-1)/2}(\rho)$, где $\rho = -\alpha/2$. Тогда

1) если $p \equiv 1 \pmod 4$, то p-ранг кривой равен 1 при $a \equiv 0$, $c \not\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda) \equiv \lambda^{2g} + c\lambda^{2g-1} \pmod p;$$

2) если $p \equiv 3 \pmod 4$, то p-ранг кривой равен 1 при $b \equiv 0$, $c \not\equiv 0 \pmod p$. В этом случае многочлен Фробениуса по модулю p равен

$$\chi(\lambda) \equiv \lambda^{2g} + c\lambda^{2g-1} \pmod p.$$

Заключение

В работе получены характеристические многочлены $\pmod p$ гиперэллиптических кривых рода $2, 3$ и p-ранга 1 для кривых с автоморфизмами.

В дальнейшем на основе полученных результатов планируется построить алгоритм подсчёта числа точек на кривых, изоморфных кривым с автоморфизмами над расширением конечного поля, по аналогии с работой [5] и исследовать их степени вложения с целью анализа возможности применения таких кривых как в классических криптосистемах, так и в криптосистемах на основе билинейных спариваний и изогений.

ЛИТЕРАТУРА

1. *Singh V., Zatysev A., and McGuire G.* On the Characteristic Polynomial of Frobenius of Supersingular Abelian Varieties of Dimension up to 7 over Finite Fields. arXiv preprint arXiv:1011.2257. 2010.
2. *Novoselov S. A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials // Прикладная дискретная математика. 2017. № 37. С. 20–31.
3. *Мельничук Е. М., Новоселов С. А.* p-Ранги гиперэллиптических кривых рода 3 с нетривиальной группой автоморфизмов // Труды математического центра имени Н. И. Лобачевского. 2018. Т. 56. С. 188–192.
4. *Bouw I. I., Diem C., and Scholten J.* Ordinary elliptic curves of high rank over with constant j-invariant // Manuscripta Mathematica. 2004. V. 114. No. 4. P. 487–501.
5. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$. `https://arxiv.org/abs/1902.05992`. 2019.

УДК 519.7 DOI 10.17223/2226308X/12/6

ВАРИАЦИИ ОРТОМОРФИЗМОВ И ПСЕВДОАДАМАРОВЫХ ПРЕОБРАЗОВАНИЙ НА НЕАБЕЛЕВОЙ ГРУППЕ

Б. А. Погорелов, М. А. Пудовкина

В криптографии ортоморфизмы на абелевой группе используются как S-боксы в схемах Лея — Месси, квази-Фейстеля, в блочной шифрсистеме FOX, в режиме