УДК 512.772.7

А. В. Лежнин

О ГЕНЕРАЦИИ КРИВЫХ *P*-РАНГА 1 РОДА 2 НАД КОНЕЧНЫМИ ПОЛЯМИ

Даются явные методы генерации кривых рода 2 p-ранга 1 над различными конечными полями.

Explicit methods of generations of curves of genus 2 of p-rank 1 over finite fields are produced.

Ключевые слова: кривая над полем, конечное поле.

Key words: curve over field, finite field.

1. Пусть k — поле конечной характеристики p, C — проективная гладкая кривая рода $g > 0$, определенная над k, $k(C)$ — поле рациональных функций C над k. Пусть на C существует такая совокупность различных рациональных точек $P_1, \ldots, P_g$, что дивизор $\sum_{i=1}^{g} P_i$ неспециален. Выберем для каждой P_i локальный $t_i \in k(C)$ и определим адель r_i поля k в смысле Шевалле, положив $(r_i)_P = \frac{1}{t_i}$, если $P = P_i$, и $(r_i)_P = 0$ иначе.

Пусть $\mathcal{A}(D)$ — пространство аделей, кратных дивизору D. Тогда адели $r_1, \ldots, r_g$, $g > 0$, образют базис k-векторного пространства $\mathcal{A}/(\mathcal{A}(0) + k(C))$, так как дивизор $\sum_{i=1}^{g} P_i$ неспециальный. В частности, $r_i^p \equiv \sum_{j=1}^{g} a_{ij} r_j \bmod(\mathcal{A}(0) + k(C))$, где $A = (a_{ij})$ — матрица g × g, называемая *матрицей Хассе — Витта.*

Эта матрица имеет два основных свойства.

1. При замене неспециальной системы точек (P_i) другой и системы (t_i) другой матрица A преобразуется по закону $A \to S^{-1} A S^{(p)}$, где S — невырожденная (g, g)-матрица с элементами из k, а $S^{(p)}$ — матрица с элементами — p-ми степенями соответствующих элементов S.

2. Если k алгебраически замкнуто, то циклические неразветвленные расширения $k(C)$ степени p — во взаимно однозначном соответствии с элементами базиса линейного пространства над простым полем из c, $\bar{c}^{(p)} A = \bar{c}$. Размерность этого линейного пространства r равна рангу $AA^{(p)} \ldots A^{(p^{g-1})}$. Число классов дивизоров порядка p поля $k(C)$ равно p^r.

Теорема 1. *Пусть кривая C рода g определена над полем k характеристики $p > 0$ из $q = p^n$ элементов и на ней есть неспециальная система g рациональных точек. По свойству 1 матрица A Хассе — Витта кривой C определена с точностью до преобразований $S^{-1} A S^{(p)}$, где S — невырожденная матрица*

с элементами из k, а характеристический многочлен $|A_\pi - \lambda E|$ *матрицы* $A_\pi = AA^{(p)}\ldots A^{(p^{g-1})}$ *– абсолютный инвариант С. Верно* $\bar{\pi}(\lambda) = (-1)^g \lambda^g |A_\pi - \lambda E|$, *где* $\bar{\pi}(\lambda)$ *– редуцированный по модулю p характеристический многочлен эндоморфизма* $\pi : (x) \to (x^q)$ *якобиева многообразия J кривой С.*

2. Пусть k — алгебраически замкнутое поле характеристики $p > 0$ и $t \in k(C)$ — функция с $dt = 0$. Каждую f можно записать единственным образом: $f = f_0^p + f_1^p t + \ldots + f_{p-1}^p t^{p-1}$, $f_i \in k(C)$. Очевидно, что $f_{p-1}^p = -d^{p-1} f / dt^{p-1}$.

Пусть $\omega = fdt$ дифференциал. Обозначим через $\mathfrak{C}(\omega) := f_{p-1} dt$.

Определение. p^{-1}-линейное отображение $\mathfrak{C}$ — *оператор Картье – (Тэйта).*

Можно доказать, что: 1) $\mathfrak{C}$ не зависит от выбора t; 2) $\mathfrak{C}$ действует на регулярных дифференциалах.

Предложение 2. *Оператор Картье имеет следующие свойства:* 1) $\mathfrak{C}(\omega_1 + \omega_2) = \mathfrak{C}(\omega_1) + \mathfrak{C}(\omega_2)$; 2) $\mathfrak{C}(f^p \omega) = f\mathfrak{C}(\omega)$; 3) $\mathfrak{C}(df) = 0$; 4) $\mathfrak{C}(f^{p-1} df) = df$.

Регулярные дифференциалы *df — точные дифференциалы*. При этом дифференциал ω точный тогда и только тогда, когда $\mathfrak{C}(\omega) = 0$. .

Регулярные дифференциалы *df/f— логарифмические дифференциалы*, причем $\mathfrak{C}(df / f) = \mathfrak{C}(f^{p-1} df / f^p) = \mathfrak{C}(f^{p-1} df) / f = df / f$. По теореме Якобсона дифференциал ω логарифмический, если и только если $\mathfrak{C}(\omega) = \omega$.

Оператор Картье дает информацию по части *p*-кручений якобиана.

Предложение 3. *Jac(X)[p](k) канонически изоморфен аддитивной группе регулярных логарифмических дифференциалов. В частности, эта группа является конечной группой порядка* p^r.

Теорема 4. *Пусть С (соответственно А) — кривая рода g (абелево многообразие размерности g), определенная над* $k_0 = \mathbb{F}_{p^n}$. *Инвариант Хассе – Витта С (А) есть сумма кратностей ненулевых корней редуцированного по модулю p многочлена Фробениуса С (А) над k.*

Определение. *p-ранг абелева многообразия А* над полем *k* характеристики p — целое $r = r(A)$ такое, что группа $A[p](\bar{k})$ точек *p*-кручения над алгебраическим замыканием $\bar{k}$ поля *k* имеет порядок p^r. При этом под *p-рангом кривой С* подразумевается *p*-ранг его якобиана J_C.

3. Пусть k — конечное поле из $q = p^n$ элементов и π — q-число Вейля. Для любого вложения поля $K = \mathbb{Q}(\pi)$ в $\mathbb{C}$ $\pi \to q/\pi$ — комплексное сопряжение на *K*. Так как этот автоморфизм *K* не зависит от выбора вложения, обозначим его $x \to \bar{x}$ и назовем *комплексным сопряжением*. Если обозначить K_0 фиксированное поле комплексного сопряжения, то K_0 действительно и *K* либо равно K_0, либо СМ-поле, то есть мнимое квадратичное расширение действительного числового поля.

Лемма 5. *Простое абелево многообразие А над k из* $q = p^n$ *элементов имеет размерность 2 и p-ранг 1, если и только если три условия верны для его эндоморфизма Фробениуса* π:

1) поле есть СМ-поле степени 4;

2) простое p разлагается на множители в K как $p\mathcal{O}_K = \mathfrak{p}_1 \overline{\mathfrak{p}_1} \mathfrak{p}_2^e$, *где e = {1, 2};*

3) выполняется $\pi\mathcal{O}_K = \mathfrak{p}_1^n \mathfrak{p}_2^{en/2}$ *с е таким же, как в (2).*

Заметим, что условие (3) означает, что *en* четное.

Следствие 6. *Простая абелева поверхность A/K p-ранга 1 абсолютно простая, то есть простая над* $\overline{k}$, *и она изогенна якобиану кривой C над k.*

Замечание. Условия (1)—(3) леммы эквивалентны тому, что характеристический многочлен $f = X^4 - a_1X^3 + (a_2 + 2q)X^2 - qa_1X + q^2$ для π удовлетворяет условиям: 1) f неприводим; 2) $ord_P(a_1) = 0$; 3) $ord_P(a_2), \geqslant n/2$; 4) $(a_2 + 4q)^2 - 4qa_1^2$ не является квадратом в кольце p-адических целых $\mathbb{Z}_p$.

4. Примеры кривых, имеющих род 2 и p-ранг 1 над конечным полем.

$\mathbb{F}_q$	Уравнение	L-многочлен
$\mathbb{F}_9$	$x^6 + x^4z^2 + xz^5 + y^2z^4 = 0$	$81t^4 + 72t^3 + 30t^2 + 8t + 1$
	$x^6 + x^5z + x^4z^2 + y^2z^4 + z^6 = 0$	$81t^4 + 18t^3 + 3t^2 + 2t + 1$
	$x^6 + x^4z^2 + xz^5 + y^2z^4 = 0$	$81t^4 + 72t^3 + 30t^2 + 8t + 1$
$\mathbb{F}_8$	$x^5 + x^4z + x^2yz^2 + xz^4 + y^2z^3 = 0$	$64t^4 - 56t^3 + 24t^2 - 7t + 1$
	$x^6 + x^5z + x^3z^3 + xyz^4 + xz^5 + y^2z^4 = 0$	$64t^4 + 56t^3 + 24t^2 + 7t + 1$
	$x^6 + x^5z + xyz^4 + y^2z^4 + z^6 = 0$	$64t^4 - 8t^3 - 4t^2 - t + 1$
$\mathbb{F}_{25}$	$x^6 + x^5z + x^4z^2 + x^3z^3 + xz^5 + y^2z^4 = 0$	$625t^4 - 25t^3 - 40t^2 - t + 1$
	$x^6 + x^4z^2 + xz^5 + y^2z^4 = 0$	$625t^4 + 300t^3 + 86t^2 + 12t + 1$
	$x^6 + x^3z^3 + x^2z^4 + xz^5 + y^2z^4 = 0$	$625t^4 + 100t^3 + 54t^2 + 4t + 1$

Список литературы

1. *O'Connor L. H., McGuire G., Naehrig M. et al.* A CM construction for curves of genus 2 with p-rank 1 // Journal of Number Theory (special edition on Elliptic Curve Cryptography). 2011. Vol. 131. P. 920—935.

2. *Serre J. P.* Sur la topologie des variete algebraiques en characteristic p // Sympos. Internac. Topologia algebraica, Mexico, 1956

3. *Манин Ю. И.* О матрице Хассе — Витта алгебраической кривой // Изв. АН СССР. Сер. матем. 1961. 25:1. С. 153—172.

4. *Hasse H., Witt E.* Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p // Monatshefte f. Math. und Phys. 1936. 43. P. 477—492.

5. *Deuring M.* Die Typen der Multiplikatorenringe elliptischer Funktionenkrper // Abh. Math. Sem. Univ. Hamburg, 1941. 14. P. 197—272.

6. *Norman H.* Many rational points: coding theory and algebraic geometry // Kluwer Academic Publishers, 2003. P. 47—55.

Об авторе

Александр Валерьевич Лежнин — ассист., Балтийский федеральный университет им. И. Канта, Калининград.

E-mail: alezhnin@ya.ru

About the author

Alexandr Lezhnin — Ass., I. Kant Baltic Federal University, Kaliningrad.

E-mail: alezhnin@ya.ru