УДК 512.772.7 DOI 10.17223/2226308X/12/3

ВЫЧИСЛЕНИЕ ИДЕАЛА 3-КРУЧЕНИЯ ДЛЯ НЕКОТОРОГО КЛАССА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

Е. С. Малыгина

Рассмотрены гиперэллиптические кривые рода 2, определяемые многочленом Диксона. Для таких кривых представлено вычисление идеала 3-кручения, в частности получены его четыре образующие с использованием представления Мамфорда — Кантора для дивизора 3-кручения и теории θ- и $\wp$-функций.

Ключевые слова: *гиперэллиптическая кривая, многочлен Диксона, идеал l-кручения, дивизор l-кручения, модулярное уравнение.*

Введение

Модулярные уравнения, связывающие инварианты l-изогенных эллиптических кривых, являются фундаментальным инструментом в арифметической геометрии. Одним из важных приложений модулярных уравнений является вычисление порядка точек эллиптической кривой над конечным полем. Наилучшим методом является алгоритм Шуфа — Элкиса — Аткина [1], в котором широко используются точки l-кручения. На сегодняшний день такие уравнения могут быть эффективно вычислены даже для больших значений l.

Однако для кривых рода $g \geqslant 2$ информации о вычислении модулярных уравнений крайне мало. Будем рассматривать гиперэллиптические кривые рода 2, определяемые многочленом Диксона [2], и для них представим формулы для вычисления идеала l-кручения в случае $l = 3$. Следует отметить, что идеал l-кручения является главной составляющей при вычислении модулярного уравнения.

В свою очередь, модулярное уравнение можно использовать для исследования изогений абелевых многообразий, что является важным инструментом не только для изучения абелевых многообразий, но и для криптографических приложений, основанных на изогениях.

Использование специального класса гиперэллиптических кривых на основе многочленов Диксона обусловлено рядом причин. Во-первых, якобиан кривой с уравнением $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ допускает разложение [3]

$$\mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C) \sim \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C_1) \times \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C_2)$$

в случае, если $g(C)$ нечётно, и

$$\mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C) \sim \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(\mathbb{F}_q[\sqrt[g]{b}]) \times \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(\tilde{C}_3),$$

если $g(C)$ чётно. При этом кривые $C_1, C_2, C_3, \tilde{C}_3$ определены многочленами Диксона $D_g(x, \alpha)$. Во-вторых, в [4] мы получили явные формулы для многочленов деления и, как следствие, представление Мамфорда — Кантора для дивизоров 3-кручения. Вычисление точек в якобиане исходной кривой C, таким образом, может быть сведено к более лёгкой задаче, а именно к вычислению числа точек в якобианах соответствующих кривых C_1, C_2 и $C_3, \tilde{C}_3$.

1. Модулярное уравнение

Пусть гиперэллиптическая кривая $C/\mathbb{F}_q$ рода $g(C) = 2$ определена уравнением

$$C : Y^2 = f(X) = \sum_{i=0}^{2g+1} f_i X^i = X^5 + f_4 X^4 + f_3 X^3 + f_2 X^2 + f_1 X + f_0.$$

Обозначим $\mathrm{Jac}_{\mathbb{F}_q}(C)[l]$ подгруппу l-кручения элементов якобиана $\mathrm{Jac}_{\mathbb{F}_q}(C)$ кривой C, где l — простое число и $l \neq \mathrm{char}(\mathbb{F}_q)$.

Далее пусть $l = 3$ и $D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3]$ — дивизор 3-кручения веса 2, то есть

$$D = [3](P_1 - \infty) + [3](P_2 - \infty),$$

где $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ — точки кривой C. Данный дивизор можно записать с помощью представления Мамфорда — Кантора, вычислив прежде многочлены деления:

$$D = (u(X), v(X)) = (X^2 + u_1 X + u_0, v_1 X + v_0).$$

Тогда существует радикальный идеал $I_3 \subset \mathbb{F}_p[x_1, x_2, y_1, y_2]$, такой, что

$$D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3] \Leftrightarrow f(x_1, x_2, y_1, y_2) = 0,\ \forall f \in I_3.$$

По аналогии с эллиптическими многочленами деления идеал I_3 называется 3-идеалом деления или идеалом 3-кручения. Согласно гипотезе Манина — Мамфорда [5], все ненулевые дивизоры 3-кручения имеют вес 2, следовательно, степень идеала I_3 равна $3^4 - 1$.

Определим $t_3(D) = u_1(D)$, где $u_1(D)$ соответствует коэффициенту u_1 в представлении Мамфорда — Кантора дивизора D. Необходимо вычислить значение $t_3(D)$ по модулю I_3. Положим $h_{1,3} \in \mathbb{F}_p[x_1, x_2, y_1, y_2]$ — многочлен, принимающий значение $u_1(D)$ на дивизоре 3-кручения D. Чтобы получить $h_{1,3}$, необходимо вычислить координаты Мамфорда — Кантора для дивизора $(P_1 - \infty) + (P_2 - \infty)$. Тогда $\chi_3 = \prod_{D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3] \setminus \{0\}} (T - t_3(D))$ является характеристическим многочленом $h_{1,3} \bmod I_3$. Зная χ_3, можно вывести модулярное уравнение Φ_3, где $\chi_3 = \Phi_3^2$ и $\deg \Phi_3 = (3^4 - 1)/2$.

2. Идеал 3-кручения

Напомним, что

$$\forall f \in I_3\ \big([3](P_1 - \infty) = -[3](P_2 - \infty) \Leftrightarrow D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[3] \Leftrightarrow f(x_1, x_2, y_1, y_2) = 0\big)$$

и

$$D = (u(X), v(X)) = (X^2 + u_1 X + u_0, v_1 X + v_0).$$

Идеал 3-кручения I_3 является идеалом в кольце $\mathbb{F}_q[x_1, x_2, y_1, y_2]$ с алгебраическим множеством $V(I_3) = (\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta)[3] = (\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta) \cap \mathrm{Jac}_{\mathbb{F}_q}(C)[3]$. Здесь Θ является дополнением к образу $\sigma(Z)$ в $\mathrm{Jac}_{\mathbb{F}_q}(C)$ при отображении $\sigma : C^2 \to \mathrm{Jac}_{\mathbb{F}_q}(C)$ и $Z \subset C^2$, то есть $\Theta = \{[P - \infty]\}$, где P — точка кривой C.

Согласно [6], идеал 3-кручения определён следующим образом:

$$I_3 = (F_1(\wp(z), \wp'(z), \wp''(z), \wp'''(z)), F_2(\wp(z), \wp'(z), \wp''(z), \wp'''(z)), F_3(\wp(z), \wp'(z), \wp''(z), \wp'''(z)),$$
$$F_4(\wp(z), \wp'(z), \wp''(z), \wp'''(z))).$$

Здесь $\wp$ является $\wp$-функцией Вейерштрасса для гиперэллиптического случая, то есть

$$\wp(z) = -4D_\infty^2(\log\theta[\delta](z)),$$

где $\delta = \begin{bmatrix} a \\ b \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^2$ и

$$\theta[\delta](z) = \theta[\delta](z, \tau) = \sum_{m \in \mathbb{Z}^2} \exp(\pi i (m + a)^t \tau (m + a) + 2\pi i (m + a)^t (z + b))$$

является классической θ-функцией с характеристикой δ. Для вычисления идеала I_3 нам понадобится следующая

Теорема 1 [6]. Морфизм

$$\varphi : \begin{cases} \mathrm{Jac}_k(C) - \Theta \to \mathbb{C}^{2g}, \\ z \mapsto (\wp(z), \wp'(z), \ldots, \wp^{(2g-1)}(z)) \end{cases}$$

есть вложение, такое, что $\wp^{(i)}(z)$ для $i \in \{0, \ldots, 2g-1\}$ порождают аффинное кольцо в $\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta$. С помощью уравнения кривой $C : Y^2 = f(X)$ величины $\wp^{(i)}(z)$ выражаются через универсальный многочлен с коэффициентами, зависящими от $u(t), v(t), w(t)$ модели

$$\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta = \{(u(t), v(t), w(t)) : f(t) - v^2(t) = u(t)w(t), \deg u = g, \deg v \leqslant g-1, \deg w = g+1\}.$$

Коэффициенты многочленов $u(t), v(t), w(t)$ выражаются также с помощью универсального многочлена от переменных $\wp^{(i)}(z)$.

Принимая во внимание, что мы работаем с дивизором 3-кручения, являющимся представителем класса $[D] \in (\mathrm{Jac}_{\mathbb{F}_q}(C) - \Theta)[3]$, и что представление Мамфорда — Кантора для дивизоров $[3](P_1 - \infty)$ и $[3](P_1 - \infty)$, сумма которых есть дивизор $D = (X^2 + u_1 X + u_0, v_1 X + v_0)$, задано явно в [4], введём следующие обозначения:

$$X_1 = -u_1(x_1, x_2, y_1, y_2) + \frac{1}{2} f_1, \quad X_2 = -v_1(x_1, x_2, y_1, y_2),$$
$$X_3 = -\frac{1}{2} f_2 + f_1 \cdot u_1(x_1, x_2, y_1, y_2) - \frac{3}{2} u_1^2(x_1, x_2, y_1, y_2),$$
$$X_4 = f_1 \cdot v_1(x_1, x_2, y_1, y_2) - 3v_1(x_1, x_2, y_1, y_2) u_1(x_1, x_2, y_1, y_2).$$

Для гиперэллиптической кривой $C/\mathbb{F}_p$ рода $g = 2$ с уравнением

$$Y^2 = (X-2)(D_4(X) + c) = X^5 - 2X^4 - 4\alpha X^3 + 8\alpha X^2 + (2\alpha^2 + c)X - 4\alpha^2 - 2c,$$

где $D_4(X) = X^4 - 4\alpha X^2 + 2\alpha^2$ — многочлен Диксона, положим $\alpha = 1$, тогда окончательно уравнение кривой примет вид

$$Y^2 = X^5 - 2X^4 - 4X^3 + 8X^2 + (c+2)X + (-2c-4).$$

Формулы для первых двух образующих F_1 и F_2 идеала 3-кручения:

$$F_1(X_1, X_2, X_3, X_4) = -2 - c + 8u_1 + 4u_1^2 + 8v_1^2 - 2u_1^3 - u_1^4 + 11v_1^2 \cdot u_1,$$

$$F_2(X_1, X_2, X_3, X_4) := 2c - \frac{6488065}{294912} u_1 - \frac{25362425}{1179648} u_1^2 + 20v_1^2 + \frac{32440325}{589824} u_1^3 + 44v_1^2 \cdot u_1 + \\ + \frac{23789569}{393216} u_1^4 + 33v_1^2 \cdot u_1^2 + 15u_1^5 - \frac{589825}{294912}.$$

Формула для F_3 слишком объёмная и связана с вычислением θ-констант, поэтому упростим её представление следующим образом:

$$F_3(X_1, X_2, X_3, X_4) = \frac{1}{d}(3X_2^3 + X_3X_4 - X_2X_5)((X_1 - \tilde{F}_1)^3 + 2(X_2^2 - \tilde{F}_2{}^2) + 2(\tilde{F}_1 - X_1)(\tilde{F}_3 + X_3)),$$

где

$$X_5 = -8 + 22u_1^2(x_1, x_2, y_1, y_2) + 10u_1^3(x_1, x_2, y_1, y_2) + \frac{5}{2} v_1^2(x_1, x_2, y_1, y_2);$$

$$\tilde{F}_1 = d\,\frac{-27X_2^4X_3^2+27X_2^5X_4+18X_2X_3^3X_4-9X_2^2X_3X_4^2-X_4^4-18X_2^2X_3^2X_5-3X_2^3X_4X_5+}{+2X_3X_4^2X_5-2X_2X_4X_5^2}{(3X_2^3+X_3X_4-X_2X_5)^2};$$

$$\tilde{F}_2 = -\frac{1}{2}\,\frac{4X_2X_3X_4X_5^3-60X_2^3X_3X_4X_5^2+45X_2^2X_3^2X_4^2X_5+54X_2^2X_3^2X_4X_5+243X_2^5X_3X_4X_5+}{+36X_2X_3^4X_4X_5+324X_2^6X_3^3-81X_2^8X_5+54X_2^6X_5^2-18X_3^5X_4^2+27X_2^5X_4^3-3X_2^4X_5^3-}$$
$$\underline{-2X_2^2X_5^4+54X_2^3X_3^4X_4-54X_2^4X_3^3X_5-243X_2^7X_3X_4-27X_2^4X_3^2X_4^2-162X_2^4X_3^2X_4-}$$
$$\underline{-54X_2X_3^3X_4^2-18X_2^2X_3^3X_5^2+18X_2X_3^3X_4^3+9X_2^2X_3X_4^4-3X_2^3X_4^3X_5+2X_3X_4^4X_5-}$$
$$\underline{-2X_2X_4^3X_5^2-2X_3^2X_4^2X_5^2-486dX_2^6X_3^3+54dX_2^5X_4^3-2dX_4^6-216dX_2^4X_3^2X_4^2+}$$
$$\underline{+486dX_2^7X_3X_4+324dX_2^3X_3^4X_4+36dX_2X_3^3X_4^3-36dX_2^2X_3X_4^4-324dX_2^4X_3^3X_5-}$$
$$\underline{-6dX_2^3X_4^3X_5+4dX_3X_4^4X_5-4dX_2X_4^3X_5^2-54dX_2^5X_3X_4X_5-36dX_2^3X_3X_4X_5^2}{(3X_2^3+X_3X_4-X_2X_5)^3};$$

$$\tilde{F}_3 = -\frac{1}{4}\,\frac{972X_2^{10}X_3X_5-2754X_2^6X_3^3X_4^2-1512X_2^3X_4^3X_4^3+8X_2X_4^5X_5^2-1944X_2^7X_3^2X_5^2+}{+1620X_2^8X_4^2X_5-801X_2^6X_4^2X_5^2+2916X_2^9X_3^2X_5+972X_2^4X_3^4X_5^2+27X_2^4X_3^2X_4^4-}$$
$$\underline{-648X_2^4X_3^3X_4X_5^2+180X_2X_3^4X_4^3X_5+1512X_2^5X_3^2X_4X_5^2+648X_2^4X_3^3X_4^2X_5-}$$
$$\underline{-6156X_2^7X_3^2X_4X_5-1944X_2^3X_3^5X_4X_5+1944X_2^6X_3^3X_4X_5+324X_2^3X_3^4X_4^2X_5+}$$
$$\underline{+5832X_2^9X_3^2X_4+324X_2^5X_3^2X_5^3-486X_2^5X_3X_4^3X_5+972X_2^2X_3^6X_4^2-8748X_2^8X_3^4-}$$
$$\underline{-729X_2^{10}X_4^2+18X_3^5X_4^4-54X_3^5X_4^3-108X_2^5X_4^5+6dX_4^8+144dX_2^2X_3X_4^6+}$$
$$\underline{+162X_2^8X_3X_5^2-657X_2^6X_3X_5^3+5346X_2^6X_3^3X_4+1620X_2^3X_3^4X_4^2-972X_2^7X_3X_4^2+}$$
$$\underline{+108X_2X_3^3X_4^4-486X_2^7X_3^2X_5+324X_2^5X_3^2X_5^2-54X_2^3X_3^2X_5^3-18X_2X_3^3X_4^5+}$$
$$\underline{+78X_2^4X_4^2X_5^3+168X_2^4X_3X_5^4+12X_3^2X_4^4X_5^2+12X_2^2X_4^2X_5^4-X_3^3X_4^2X_5^3-X_2^2X_3X_5^5-}$$
$$\underline{-36X_2^2X_3X_4^6+12X_2^3X_4^5X_5-252X_2^2X_3^3X_4^2X_5^2-1944X_2^4X_3^3X_4X_5+54X_2X_3^4X_4^2X_5+}$$
$$\underline{+54X_2^2X_3^3X_4X_5^2+648X_2^5X_3X_4^2X_5-108X_2^3X_3X_4^2X_5^2-114X_2^3X_3^2X_4X_5^3-}$$
$$\underline{-270X_2^2X_3^2X_4^4X_5+210X_2^3X_3X_4^3X_5^2-24X_2X_3X_4^3X_5^3+2X_2X_3^2X_4X_5^4+7776dX_2^6X_3^3X_4^2-}$$
$$\underline{-1944dX_2^3X_3^4X_4^3+16dX_2X_4^5X_5^2-2916dX_2^7X_3X_4^3+1350dX_2^4X_3^2X_4^4-11664dX_2^9X_3^2X_4-}$$
$$\underline{-7776dX_2^5X_3^5X_4+7776dX_2^6X_3^4X_5-144dX_2X_3^3X_4^5-8X_3X_4^6X_5+1080dX_2^5X_3^2X_4X_5^2+}$$

$$\underline{+10206dX_2^8X_3^4 - 216dX_2^5X_4^5 + 864dX_2^4X_3^3X_4^2X_5 - 648dX_2^7X_3^2X_4X_5 + 540dX_2^5X_3X_4^3X_5+}$$

$$\underline{+24dX_2^3X_4^5X_5 - 16dX_3X_4^6X_5 - 324dX_2^8X_4^2X_5 - 198dX_2^6X_4^2X_5^2 + 648dX_2^4X_3^4X_5^2+}$$

$$\underline{+648dX_2^2X_3^6X_4^2 + 24dX_2^4X_4^2X_5^3 + 8dX_3^2X_4^4X_5^2 + 8dX_2^2X_4^2X_5^4 - 72dX_2^2X_3^2X_4^4X_5+}$$

$$\underline{+192dX_2^3X_3X_4^3X_5^2 + 144dX_2X_3^4X_4^3X_5 + 1458dX_2^{10}X_4^2 - 1296dX_2^3X_3^5X_4X_5-}$$

$$\underline{-288dX_2^2X_3^3X_4^2X_5^2 + 144dX_2^3X_3^2X_4X_5^3 - 16dX_2X_3X_4^3X_5^3}$$
$$(3X_2^3 + X_3 * X_4 - X_2 * X_5)^4$$

и константа d сопряжена с вычислением θ-констант:

$$\theta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} (0), \quad \theta \begin{bmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \end{bmatrix} (0).$$

Четвёртая образующая F_4 идеала 3-кручения имеет следующий вид:

$$F_4(X_1, X_2, X_3, X_4) = \frac{1}{2} \underline{-27dX_2^4X_3^2 + 27dX_2^5X_4 + 18dX_2X_3^3X_4 - 9dX_2^2X_3X_4^2 - dX_4^4-}$$
$$\underline{-18dX_2^2X_3^2X_5 - 3dX_2^3X_4X_5 + 2dX_3X_4^2X_5 - 2dX_2X_4^2X_5^2 + 9X_1X_2^6+}$$
$$\underline{+6X_1X_2^3X_3X_4 - 6X_1X_2^4X_5 + X_1X_3^2X_4^2 - 2X_1X_2X_3X_4X_5 + X_1X_2^2X_5^2}$$
$$(3X_2^3 + X_3X_4 - X_2X_5)^2 + \tilde{F}_4,$$

где выражение $\tilde{F}_4$ сопряжено с вычислением $\wp$- и θ-функций.

ЛИТЕРАТУРА

1. *Cohen H. and Frey G.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2005.
2. *Lidl R., Mullen G. L., and Turnwald G.* Dickson Polynomials. Chapman and Hall/CRC, 1993.
3. *Novoselov S. A.* Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$. arXiv: 1902.05992. 2019.
4. *Malygina E. S. and Novoselov S. A.* Division polynomials for hyperelliptic curves defined by Dickson polynomials // Proc. 8th Workshop on Current Trends in Cryptology. Svetlogorsk, Kaliningrad region, June 4–7, 2019. `https://ctcrypt.ru/ematerials2019`.
5. *Hindry M. and Silverman J.* Diophantine Geometry. An Introduction. Graduate Texts in Mathematics. V. 201. Springer Verlag, 2000.
6. *Kampkötter W.* Explizite Gleichungen für Jacobische Varietätenhyperelliptisher Rurven.Ph. D. Thesis, Universität Gesamthochschule Essen, 1991.