УДК 512.77

С. И. Алешников, С. Н. Ткаченко
С. В. Столярчук, А. А. Шпилевой

АНАЛИЗ АЛГОРИТМОВ ВЫЧИСЛЕНИЙ В ЯКОБИАНЕ КРИВОЙ ПИКАРА

Рассматривается представление элементов якобиана кривой Пикара, которое позволяет построить алгоритм для редукции дивизоров со сложностью $O(deg(D))$. Сложение дивизоров можно осуществить, используя алгоритм редукции.

In this article a representation of the elements of the Jacobian of a Picard curve is considered, which allows us to construct an algorithm for the reduction of divisors with complexity $O(deg(D))$. Addition of divisors can be performed using the reduction algorithm.

Ключевые слова: дивизор, якобиан кривой, кривая Пикара, редукция дивизоров.

Keywords: divisor, Jacobian of a curve, Picard curve, reduction of a divisor.

Введение

В настоящее время все более широкое применение находят системы защиты данных на основе эллиптических и гиперэллиптических кривых. Однако эти два класса кривых уже весьма хорошо изучены, и для алгоритмов на их основе предлагаются эффективные методы взлома. В связи с этим активно исследуются иные виды кривых.

Приложения кривых рода 3 к проблемам защиты информации и соответствующие методы вычислений начали изучаться фактически с начала 2000-х гг. Сюда можно отнести работы [1—4]. В [5] рассматриваются, среди прочих, гиперэллиптические кривые рода 3. В последние годы наблюдается возврат к указанной проблематике — например, в [6; 7].

В данной работе будут рассматриваться кривые Пикара (имеющие род 3). Мы опишем редукцию и сложение дивизоров в якобиане такой кривой, а также представление дивизоров в виде многочленов, которое затем используется для построения алгоритма редукции дивизора.

1. Основные понятия

Пусть k — поле; $\overline{k}$ — его алгебраическое замыкание. Для алгебраической кривой C будем обозначать $C(\overline{k})$ — множество ее точек с координатами в поле $\overline{k}$; $C(k)$ — множество ее k-рациональных точек, то есть

Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2019. № 4. С. 5 – 12.

точек с координатами в поле k; $k(C)$ — множество рациональных функций на C с коэффициентами в k. Будем обозначать далее Div_C — группу дивизоров на кривой C; Div_C^0 — подгруппу дивизоров степени 0 в Div_C; $Princ_C$ — подгруппу главных дивизоров группы Div_C^0.

Определение 1.1. Факторгруппа $J_C = \mathrm{Div}_C^0 / \mathrm{Princ}_C$ называется *якобианом* кривой C. Элементы из J_C, то есть классы эквивалентности по модулю $Princ_C$, называются *точками* якобиана.

Определение 1.2. Дивизор D на кривой C называется *k-рациональным*, если он инвариантен относительно действия абсолютной группы Галуа $G_k = Gal(\overline{k} / k)$. Класс эквивалентности k-рационального дивизора $D \in J_C$ называется *k-рациональной точкой* якобиана.

Множество k-рациональных точек якобиана образует подгруппу $J_C(k)$ группы J_C, называемую *k-рациональным якобианом* кривой C.

Определение 1.3. *Кривой Пикара* называется плоская проективная кривая C рода 3 с уравнением

$$ZY^3 - Z^4 p_4\left(\frac{X}{Z}\right) = 0,$$

где $p_4(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ — многочлен из $k[x]$.

В случае $\mathrm{char}(k) = 0$ или $\mathrm{char}(k) > 0$ кривая C не имеет особых точек тогда и только тогда, когда дискриминант многочлена $p_4(x)$ отличен от 0. Без ограничения общности можно считать, что $a_3 = 0$.

Если поле k алгебраически замкнуто, то есть $k = \overline{k}$, то всякая кривая Пикара имеет 5 вполне разветвляющихся точек $R_1,\ldots, R_5$ по отношению к морфизму $\pi_x : \mathrm{C(k)} \to \mathbf{P}^1_k$, $(x : y : z) \mapsto x$, а именно: $R_i = (r_i : 0 : 0)$, $i = 1,\ldots, 4$, где r_i — корни многочлена $p_4(x)$ и $R_5 = (0 : 1 : 0)$. Пусть ξ — примитивный корень степени 3 из единицы. Тогда отображение

$$\sigma\colon C(k) \to C(k),\ (x : y : z) \mapsto (x : \xi y : z)$$

является автоморфизмом C, удовлетворяющим равенствам

$$\pi_x \circ \sigma = \mathrm{id}_{\mathbf{P}^1_k} \qquad \text{и} \qquad \sigma^3 = \mathrm{id}_{C(k)}.$$

Определение 1.4. Две точки P_1, $P_2 \in C(k)$ называются *сопряженными*, если $P_1 = \sigma(P_2)$ или $P_2 = \sigma(P_1)$. Далее будем писать σP вместо $\sigma(P)$.

Как известно, в J_C существует только один класс эквивалентности канонических дивизоров, называемый *каноническим классом*.

Лемма 1.5. Пусть C — кривая Пикара без особых точек. Тогда положительными дивизорами канонического класса K кривой C являются пересечения прямых с кривой C.

2. Представление дивизоров

Определение 2.1. Аффинный положительный дивизор D, то есть такой дивизор, что $P_\infty \notin \mathrm{supp}(D)$, называется *полуредуцированным*, если не существует точки P_1, такой, что $D \geq P_1 + \sigma P_1 + \sigma^2 P_1$. Определим множества

$$\mathrm{Div}_C^{+,\,i} := \left\{ D \in \mathrm{Div}_C \,\middle|\, \begin{matrix} \text{D есть k-рациональный полуре-} \\ \text{дуцированный дивизор степени i} \end{matrix} \right\},\ i \geq 0,$$

$$\mathcal{D}(r,s) = \bigcup_{i=r}^{s} \mathrm{Div}_C^{+,\,i},\ 0 \leq r < s.$$

Порядком многочлена $f(x, y) \in k[x, y]$ в точке P_∞ называется число

$$\mathrm{ord}_{P_\infty}(f(x,y)) = -\nu_{P_\infty}(f(x,y)),$$

где ν_{P_∞} — нормирование поля $k(C)$ в точке P_∞. *Старший одночлен* многочлена $f(x, y)$ есть одночлен $a_{i_1 j_1} x^{i_1} y^{j_1}$, удовлетворяющий равенству

$$\nu_{P_\infty}(f(x,y)) = \min_{i,j} \nu_{P_\infty}(a_{ij} x^i y^j) = \nu_{P_\infty}(a_{i_1 j_1} x^{i_1} y^{j_1}).$$

Пусть $D \in \mathcal{D}(2,4)$. Определим для дивизора D коническое сечение

$$v_D(x, y) = a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00}$$

наименьшего порядка в P_∞, удовлетворяющее условию $(v_D(x, y)) \geq D$ и такое, что старший одночлен $v_D(x, y)$ приведен. Заметим, что в некоторых случаях коническое сечение может сводиться к прямой или нулевому многочлену и $v_D(x, y)$ удовлетворяет неравенству

$$\mathrm{ord}_{P_\infty}(v_D(x,y)) \leq 8 - (5 - \deg(D)). \qquad (1)$$

$v_D(x, y)$ называется *интерполирующим коническим сечением дивизора* D.

Лемма 2.2. Для $v_D(x, y)$ выполняются следующие равенства.

1. $\mathrm{ord}_{P_\infty}(v_D(x,y)) = 7 \Leftrightarrow a_{02} = 0$ и $a_{11} \neq 0$.
2. $\mathrm{ord}_{P_\infty}(v_D(x,y)) = 6 \Leftrightarrow a_{02} = 0$ и $a_{11} = 0$ и $a_{20} \neq 0$.
3. $\mathrm{ord}_{P_\infty}(v_D(x,y)) = 4 \Leftrightarrow a_{02} = 0, a_{11} = 0, a_{20} = 0$ и $a_{01} \neq 0$.

Определение 2.3. Дивизор D, $\deg(D) \geq 3$, называется *коллинеарным*, если найдутся точки $P_1, P_2, P_3 \in \mathrm{supp}(D)$ и прямая r_0, такие, что

$$(r_0)_0 \geq P_1 + P_2 + P_3.$$

В противном случае D называется *обычным*.

Лемма 2.4. Пусть $D \in \mathcal{D}(3, 4)$. Тогда справедливы следующие утверждения.

1. $v_D(x, y)$ линейно или разлагается на линейные множители.

2. Дивизор $D + P_\infty$ коллинеарный.

3. $v_D(x, y) = a_{20}x^2 + a_{11}xy + a_{10}x + a_{01}y + a_{00}$, где $a_{11}^2 a_{00} + a_{01}^2 a_{20} - a_{11}a_{01}a_{10} = 0$.

Рассмотрим отображение

$$\Phi : \mathcal{D}(2, 4) \to k[x] \times k[x, y] \times k[y],\ D \mapsto \Phi(D) = (u_D(x), v_D(x, y), w_D(y)),$$

где $u_D(x) = \prod_{P_i \in \mathrm{supp}(D)} (x - x_i)$, $w_D(y) = \prod_{P_i \in \mathrm{supp}(D)} (y - y_i)$, $v_D(x, y)$ — интерполирующее коническое сечение D. Отображение Φ не является инъективным. Действительно, пусть $x_1, x_2 \in k$, $p_4(x_1) = p_4(x_2) \neq 0$ и y_0 — корень уравнения $y^3 - p_4(x_1) = 0$. Тогда дивизоры

$$D_1 = (x_1 : y_0 : 1) + (x_1 : \xi y_0 : 1) + (x_2 : y_0 : 1) + (x_2 : \xi^2 y_0 : 1),$$

$$D_1 = (x_1 : y_0 : 1) + (x_1 : \xi^2 y_0 : 1) + (x_2 : y_0 : 1) + (x_2 : \xi y_0 : 1)$$

обладают одинаковыми образами при действии Φ. Однако, если ограничить $\mathcal{D}(2, 4)$ до множества $\mathcal{D}_0(2, 4) = \bigcup_{i=2}^{4} \mathrm{Div}_0^{+,i}(C)$, где

$$\mathrm{Div}_0^{+,i}(C) = \{D \in \mathrm{Div}_C^{+,i} \mid D$$

не содержит две сопряженные точки, $i = 2, 3$ и

$$\mathrm{Div}_0^{+,4}(C) = \{D \in \mathrm{Div}_C^{+,4} \mid D \neq P_1 + \sigma P_1 + P_2 + \sigma P_2\},$$

то мы получим следующий результат.

Лемма 2.5. Сужение отображения Φ на множество $\mathcal{D}_0(2, 4)$ является биекцией на свой образ $\Phi(\mathcal{D}_0(2, 4))$.

3. Алгоритм редукции

Задача редукции. Для заданного аффинного дивизора D необходимо найти аффинный дивизор $D_f \geq 0$ степени $\deg(D_f) \leq 3$, такой, что $D - \deg(D)P_\infty \sim D_f - \deg(D_f)P_\infty$. Алгоритм редукции основан на следующей геометрической идее. Если задан положительный аффинный дивизор $D_0 = P_1 + P_2 + P_3 + P_4$ степени 4 и все его точки коллинеарны, то по лемме **1.5** D_0 лежит в каноническом классе и $D_0 - 4P_\infty \sim 0$. В противном случае для редукции $D_0 - 4P_\infty$ берем интерполирующее коническое сечение v_0 дивизора D_0. Тогда из равенства (1) следует, что v_0 пересекает C максимум в 3 аффинных точках H_1, H_2, H_3. Следовательно, получаем

$$(v_0) = (D_0 - 4P_\infty) + (D_1 - 3P_\infty),\quad D_0 - 4P_\infty \sim -(D_1 - 3P_\infty),$$

где $D_1 = H_1 + H_2 + H_3$.

Теперь рассмотрим коническое сечение v_1 дивизора D_1. Сечение v_1 пересекает C в 3 точках P_1', P_2', P_3'. Следовательно, $D_1 - 3P_\infty \sim -(D_2 - 3P_\infty)$, где $D_2 = P_1' + P_2' + P_3'$. Объединяя предыдущие результаты, получаем $D_0 - 4P_\infty \sim D_2 - 3P_\infty$. В результате дивизор D_2 степени 3 является редукцией дивизора D_0.

Алгоритм 3.1.

1. **if** $\deg(D) \le 3$ **then** D уже редуцирован, $D_f := D$, перейти к шагу 6. **else** взять $D_0 \le D$, $\deg(D_0) = 4$ и положить $D := D - D_0$.

2. Найти интерполирующее коническое сечение v_0 дивизора D_0.

3. Факторизовать $R_y(v_0, C)$ (результант по переменной y), из $\dfrac{R_y(v_0, C)}{u_0}$ получить x-координаты точек из $\mathrm{supp}(D_1)$, затем, используя v_0, вычислить их y-координаты.

4. Зная D_1, найти коническое сечение v_1, затем восстановить D_2 из $\dfrac{R_y(v_1, C)}{u_1}$ и v_1.

5. **if** $\deg(D) \le 4 - \deg(D_2)$ **then** положить $D_f := D + D_2$ и перейти к шагу 6. **else** взять $E_0 \le D$, $\deg(E_0) = 4 - \deg(D_2)$, положить $D := D - E_0$, $D_3 := E_0 + D_2$, $D_0 := D_3$ и перейти к шагу 2.

6. **return** (D_f).

Замечание 3.2. С вычислительной точки зрения алгоритм **3.1** может быть затратным, поскольку в двух его шагах факторизуется многочлен из $k[x]$. Для модификации алгоритма **3.1** отметим следующее.

1. Пусть дивизор D представлен в виде $D = D_0 + E_0 + E_1 + \ldots + E_{N-1}$, где E_j — аффинный и положительный, $j = 1,\ldots, N-1$. Процесс редукции в алгоритме **3.1** дает нам последовательность положительных аффинных дивизоров

$$D_0, D_1, D_2, \ldots, D_{3j}, D_{3j+1}, D_{3j+2}, \ldots, D_{3N}, D_{3N+1}, D_{3N+2}, \tag{2}$$

где

$$D_{3j} := D_{3(j-1)+2} + E_{j-1},\ j = 1,\ldots, N,$$

$$D_{3j} - 4P_\infty \sim -(D_{3j+1} - \deg(D_{3j+1})P_\infty) \sim D_{3j+2} - \deg(D_{3j+2})P_\infty,$$

$$0 \le \deg(D_{3j+1}), \deg(D_{3j+2}) \le 3, \deg(D_{3j}) = 4 \text{ и } \deg(E_{j-1}) = 4 - \deg(D_{3j+2}).$$

Следовательно, $D - \deg(D)P_\infty \sim D_{3N+2} - \deg(D_{3N+2})P_\infty$ и D_{3N+2} — результат редукции D.

2. Если дивизор D_h, $j = 1,\ldots, 3N+2$ лежит в $\mathcal{D}_0(2, 4)$, то найдем его координаты $\overline{D_h} = \Phi(D_h)$. Получим последовательность

$$\overline{D_0}, \overline{D_1}, \overline{D_2}, \ldots, \overline{D_{3j}}, \overline{D_{3j+1}}, \overline{D_{3j+2}}, \ldots, \overline{D_{3N}}, \overline{D_{3N+1}}, \overline{D_{3N+2}}. \tag{3}$$

3. Зная $\overline{D_0}$ (представление D_0), в зависимости от того, $D \in \mathcal{D}_0(2, 4)$ или нет, мы вычисляем $\overline{D_h}$ или D_h, для $h \ge 1$ рекурсивно, исходя из по-

следовательностей (2) и (3). Рекурсивное вычисление $\overline{D_h}$ и D_h в худшем случае будет заключаться в вычислении решения системы линейных уравнений над полем k. В итоге, зная $\overline{D_{3N+2}} = (u_{3N+2}, v_{3N+2}, w_{3N+2})$, по лемме **3.4** мы можем найти точки из $\mathrm{supp}(D_{3N+2})$.

Замечание 3.3. Зная $\overline{D_{3j+1}}$, $\overline{D_{3j+2}}$, можно установить следующие равенства:

$$v_{3j+1} = v_{3j+2}, \qquad u_{3j+2} = \left(\frac{R_y(v_{3j+1}, C)}{u_{3j+1}}\right)^*, \qquad w_{3j+2} = \left(\frac{R_y(w_{3j+1}, C)}{w_{3j+1}}\right)^*,$$

где $(**)^*$ означает деление многочлена ** на коэффициент его старшего одночлена. Вдобавок, если v_{3j+1} явно не зависит от x, то $w_{3j+2} = w_{3j+1}$.

Лемма 3.4. Пусть задан дивизор $D_{3j} \in \mathrm{Div}_C^{+,4}$. Тогда можно вычислить $\overline{D_{3j}}$, если $D_{3j} \in \mathrm{Div}_0^{+,4}(C)$, и $\overline{D_{3j+1}}$ и $\overline{D_{3j+2}}$, если $D_{3j} \notin \mathrm{Div}_0^{+,4}(C)$.

Лемма 3.5. Пусть $D_{3j} \in \mathrm{Div}_0^{+,4}(C)$ и $\overline{D_{3j}} = (u_{3j}, v_{3j}, w_{3j})$. Тогда возможны следующие случаи.

1. Можно вычислить

$$\overline{D_{3j+1}} = (u_{3j+1}, v_{3j+1}, w_{3j+1}) \qquad \text{и} \qquad \overline{D_{3j+2}} = (u_{3j+2}, v_{3j+2}, w_{3j+2}),$$

где v_{3j+1} (следовательно, и v_{3j+2}) зависит от y.

2. Можно вычислить D_{3j+2} в явном виде.

Лемма 3.6. Пусть известны $\overline{D_{3j+1}}$ и $\overline{D_{3j+2}}$ и дивизор E_{j-1}. Тогда возможны следующие случаи.

1. Можно вычислить $\overline{D_{3(j+1)}} = (u_{3(j+1)}, v_{3(j+1)}, w_{3(j+1)})$.

2. Можно вычислить $\overline{D_{3(j+1)+1}}$ и $\overline{D_{3(j+1)+2}}$.

3. Можно вычислить $D_{3(j+1)+2}$ в явном виде, и он k-рационален.

Из **3.3—3.6** получается эффективная версия алгоритма **3.1**.

Алгоритм 3.7.

1. **if** $\deg(D) \le 3$ **then** D уже редуцирован, $D_f := D$, перейти к шагу 6.
2. Положим $D_0 = P_1 + P_2 + P_3 + P_4$.
3. **if** $D_0 \in \mathrm{Div}_0^{+,4}(C)$ **then** вычисляем $\overline{D_0}$.
4. **else** вычисляем $\overline{D_1}$, $\overline{D_2}$, переход к вспомогательному алгоритму **3.8**.
5. Зная $\overline{D_0}$ и применяя лемму **3.5**, находим:

a) D_2 в явном виде. **if** $\deg(D + D_2) < 4$ **then** положим $D_f := D + D_2$, переход к шагу 6. **else** положим $D_0 := D_2 + E_0$, $D := D - E_0$, переход к шагу 3;

b) $\overline{D_1}$, $\overline{D_2}$ в явном виде, переход к вспомогательному алгоритму **3.8**.

6. **return** (D_f).

Вспомогательный алгоритм 3.8.

S1. **if** $\deg(D) + \deg(v_2) < 4$ **then** используя лемму **3.4**, найдем D_2, затем положим $D_f := D + D_2$, переход к шагу 6.

S2. **else** возьмем E_0, $\deg(E_0) + \deg(v_2) = 4$, $E_0 \le D$, положим $D := D - E_0$ и применим лемму **3.6**. Возможно несколько вариантов:

a) найдем $\overline{D_3}$. **then** положим $\overline{D_0} = \overline{D_3}$, переход к шагу 5;

b) найдем $\overline{D_4}$ и $\overline{D_5}$. **then** положим $\overline{D_1} = \overline{D_4}$, $\overline{D_2} = \overline{D_5}$, переход к S1;

c) найдем D_5. **if** $\deg(D + D_5) < 4$ **then** положим $D_f := D + D_5$, переход к шагу 6. **else** положим $D_0 := D_5 + E_0$, $D := D - E_0$, переход к шагу 3.

Предложение 3.9. Пусть имеется дивизор D. Алгоритм **3.7** вычисляет редукцию D, совершая $O(\deg(D))$ операций в поле k и только одну факторизацию многочлена степени, не превышающей 3, из $k[x]$. Более того, если $k = \mathbf{F}_q$, то константа c в выражении $O(\deg(D))$ удовлетворяет неравенству $c \le 2(4 \cdot \log_2 q)^3$.

Пример 3.10. Пусть $k = \mathbf{F}_{7^6}$ и $p_4(x) = x^4 + x^3 + 4x^2 + x$. Найдем редукцию дивизора $D = 6(5:2:1) + (3:0:1) + (1:0:1)$ с помощью алгоритма **3.7**.

Результаты редукции дивизора D представлены в таблице.

Результаты редукции дивизора D

D_i	$\overline{D_i}$	E_j
$D_0 = 3(5:2:1) + (3:0:1)$	$\overline{D_0} = (x^4 + 5x^3 + 6x^2 + 3x + 6, x^2 + 4x + 2y, y^4 + y^3 + 5y^2 + 6y)$	–
$D_1 = ?$	$\overline{D_1} = (x^2 + 4x, x + y, y^2 + 5y)$	–
$D_2 = ?$	$\overline{D_2} = \left(x^2 + 4, x + y, y^2 + 4\right)$	$E_0 = (5:2:1) + (3:0:1)$
$D_3 = ?$	$\overline{D_3} = ?$	–
$D_3 = ?$	$\overline{D_4} = ?$	–
$D_5 = 2(0:0:1) + (1:0:1)$	$\overline{D_5} = ?$	$E_0 = (5:2:1)$
$D_6 = 2(0:0:1) + (1:0:1) + + (5:2:1)$	$\overline{D_6} = (x^4 + x^3 + 5x^2, xy + 3x^2 + 4x, y^4 + 5y^3)$	–
$D_7 = ?$	$\overline{D_7} = (x^3 + 6x^2 + 3x, x^2 + 2x + y, y^3 + 4y^2 + 6y)$	–
$D_8 = ?$	$\overline{D_8} = (x^3 + 3x + 5, x^2 + 2x + y, y^3 + y^2 + 2y + 4)$	$E_0 = (5:2:1)$
$D_9 = ?$	$\overline{D_9} = (x^4 + 2x^3 + 3x^2 + 4x + 3, 3x^2 + 6x + y + xy + 2, y^4 + 6y^3 + 6)$	–
$D_{10} = ?$	$\overline{D_{10}} = (x^3 + x^2 + 6x + 5, x^2 + 4x + + 6y + 3, y^3 + 6y^2 + 4y + 4)$	–
$D_{11} = ?$	$\overline{D_{11}} = (x^3 + 4x^2 + 4x + 4, x^2 + 4x + + 6y + 3, y^3 + 6y^2 + 4y + 4)$	$E_0 = \varnothing$
$D_f = (\omega^{25112} : \omega^{60200} : 1) + + (\omega^{54008} : \omega^{8600} : 1) + + (\omega^{58136} : \omega^{68456} : 1)$	$\overline{D_f} = ?$	–

Список литературы

1. *Barreirol E.R., Sarlabous J.E., Cherdieu J.-P.* Efficient Reduction on the Jacobian Variety of Picard Curves // Coding Theory, Cryptography and Related Areas. 1998. P. 13—28.

2. *Sarlabous J.E., Barreirol E.R., Barceló J.A.P.* On the Jacobian Varieties of Picard Curves: Explicit Addition Law and Algebraic Structure // Mathematische Nachrichten. 1999. №208. P. 149—166.

3. *Flon S., Oyono R.* Fast Arithmetic on Jacobians of Picard Curves // Public Key Cryptography — PKC 2004. 2004. P. 55—68.

4. *Oyono R.* Arithmetik nicht-hyperelliptischer Kurven des Geschlechts 3 und ihre Anwendung in der Kryptographie : PhD Diss. Univ. Duisburg-Essen, 2005.

5. *Handbook* of Elliptic and Hyperelliptic Curve Cryptography / ed. H. Cohen, G. Frey. Chapman & Hall, 2006

6. *Sutherland A.V.* Fast Jacobian Arithmetic for Hyperelliptic Curves of Genus 3 // ANTS XIII. 2019. P. 425—442.

7. *Thakur S.* Abelian varieties in pairing-based cryptography. 2019. aXiv:1812. 11479v2 [math.NT].

Об авторах

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: elliptec@mail.ru

Сергей Владимирович Столярчук — студент, Балтийский федеральный университет им. И. Канта, Россия.
E-mail: s_v_stolyarchuk@mail.ru

Сергей Николаевич Ткаченко — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: tkasergey@yandex.ru

Андрей Алексеевич Шпилевой — канд. физ.-мат. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: ashpilevoi@kantiana.ru

The authors

Dr Sergey I. Aleshnikov, Associate Professor, I. Kant Baltic Federal University, Russia.
E-mail: elliptec@mail.ru

Sergey V. Stolyarchuk, Undergraduate Student, I. Kant Baltic Federal University, Russia.
E-mail: s_v_stolyarchuk@mail.ru

Dr Sergey N. Tkachenko, Associate Professor, I. Kant Baltic Federal University, Russia.
E-mail: tkasergey@yandex.ru

Dr Andrey A. Shpilevoy, Associate Professor, I. Kant Baltic Federal University, Russia.
E-mail: ashpilevoi@kantiana.ru