Дальневосточный математический журнал. 2019. Т. 19. № 1. С. 84–87

УДК 517.583+512.742.72
MSC2010 33E05

© А. В. Устинов[1]

Упрощённое доказательство формулы Ворда для эллиптических последовательностей

Эллиптическая делимостная последовательность — это последовательность целых чисел, удовлетворяющая нелинейному рекуррентному отношению, которое связывает полиномы деления на эллиптических кривых. Эллиптические делимостные последовательности были впервые определены, а их арифметические свойства изучены Морганом Вордом в 1948 г. В частности, он доказал явную формулу для общего члена последовательности в терминах сигма-функции Вейерштрасса. В настоящей статье мы приводим упрощенное доказательство формулы Ворда.

Ключевые слова: *эллиптические делимостные последовательности, эллиптические кривые, эллиптические функции Вейерштрасса.*

Эллиптические делимостные последовательности (elliptic divisibility sequences) были введены Морганом Вордом в работе [1].

Определение. *Эллиптическая последовательность* — это последовательность комплексных чисел $\{h_n\}_{n=-\infty}^{\infty}$, удовлетворяющая рекуррентному соотношению

$$h_{n+m}h_{n-m} = h_{n+1}h_{n-1}h_m^2 - h_n^2 h_{m+1}h_{m-1} \qquad (m, n \in \mathbb{Z}). \tag{1}$$

Если последовательность $\{h_n\}$ состоит из целых чисел и $h_n \mid h_m$ при $n \mid m$, то $\{h_n\}$ называется *эллиптической делимостной последовательностью.*

Из рекуррентного соотношения (1) следует, что $h_{-n} = -h_n$, и, в частности, $h_0 = 0$. Также без ограничения общности можно считать, что $h_1 = 1$. Основной интерес с точки зрения приложений представляют последовательности, для которых $h_2 h_3 \neq 0$. Такие последовательности называются *общими эллиптическими последовательностями.* Полное описание общих эллиптических последовательностей даёт результат, полученный Вордом, см. [1, Theorem 12.1].

[1] Тихоокеанский государственный университет, 680035, г. Хабаровск, ул. Тихоокеанская, 136; Хабаровское отделение Института прикладной математики ДВО РАН, 680000, г. Хабаровск, ул. Дзержинского, 54. Электронная почта: ustinov@iam.khv.ru, ustinov.alexey@gmail.com

Теорема. *Пусть* $\{h_n\}_{n=0}^{\infty}$ *— общая эллиптическая последовательность. Тогда существуют рациональные числа* g_2, g_3 *и комплексное* z *такие, что*

$$h_n = \frac{\sigma(nz)}{\sigma(z)^{n^2}}, \tag{2}$$

где $\sigma(z)=\sigma(z;g_2,g_3)$ *— σ-функция Вейерштрасса, ассоциированная с кривой*

$$y^2 = 4x^3 - g_2x - g_3. \tag{3}$$

Ниже предлагается доказательство, упрощающее оригинальный подход, использованный Вордом.

Замечание 1. При $h_2 = 0$, как показано в [1], последовательность $\{h_n\}$ имеет вид $h_n = \left(\frac{-8}{n}\right)$, где $\left(\frac{d}{n}\right)$ — символ Кронекера, т. е.

$$h_n = \begin{cases} 0, & \text{если } n \text{ чётно;} \\ (-1)^{[n/4]}, & \text{если } n \text{ нечётно.} \end{cases}$$

К этому случаю сводится любая последовательность, в которой для некоторого n_0 выполняется равенство $h_{n_0} = h_{n_0+2} = 0$. Описание случая $h_3 = 0$ см. в [1, Ch. VII].

Замечание 2. Из соотношения (1), вообще говоря, не следует, что эллиптическая делимостная последовательность существует. При $m = 2,\ 3,\ \ldots$ формула (1) превращается в различные рекуррентные соотношения, каждое из которых однозначно задаёт последовательность $\{h_n\}_{n=0}^{\infty}$ (при наличии достаточного числа начальных условий). Согласованность этих рекуррентных соотношений неочевидна. Поэтому будем предполагать, что эллиптическая делимостная последовательность задаётся начальными условиями $h_1 = 1$, h_2, h_3, h_4 и соотношением (1), в котором $m = 2$:

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_n^2h_3h_1 \qquad (n \geqslant 2). \tag{4}$$

Если $h_{n-2}=0$, то формула (4) уже не позволяет вычислить h_{n+2}. В этом случае (см. замечание 2) $h_{n-4}\neq 0$, и значение h_{n+2} можно найти из формулы

$$h_{n+2}h_{n-4} = h_nh_{n-2}h_3^2 - h_{n-1}^2h_2h_4 \qquad (n \geqslant 2), \tag{5}$$

которая получается из (1) подстановкой $m=3$ и заменой n на $n-1$.

Доказательство теоремы. Как и в оригинальном доказательстве из работы [1] подберём параметры кривой (3) и значение z так, чтобы равенство (2) выполнялось при $n = 2, 3, 4$:

$$h_2 = \frac{\sigma(2z)}{\sigma(z)^4}, \quad h_3 = \frac{\sigma(3z)}{\sigma(z)^9}, \quad h_4 = \frac{\sigma(4z)}{\sigma(z)^{16}}. \tag{6}$$

Воспользуемся стандартными формулами, выражающими значения $\sigma(2z)$, $\sigma(3z)$ и $\sigma(4z)$ через $\wp$-функцию Вейерштрасса и её производные, см. [2]:

$$\frac{\sigma(2z)}{\sigma(z)^4} = -\wp'(z), \quad \frac{\sigma(3z)}{\sigma(z)^9} = \wp'(z)^2(\wp(z) - \wp(2z)), \tag{7}$$

$$-\frac{\sigma(4z)}{\sigma(2z)\sigma(z)^{12}} = \wp'(z)^4 + \wp'(z)^2\wp''(z)(\wp(2z) - \wp(z)). \tag{8}$$

Из этих формул можно выразить значения $\wp'(z)$, $\wp(z)-\wp(2z)$ и $\wp''(z)$:

$$\wp'(z) = -h_2, \quad \wp(z)-\wp(2z) = \frac{h_3}{h_2^2}, \quad \wp''(z) = \frac{h_4+h_2^5}{h_2h_3}. \tag{9}$$

Из формулы удвоения

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$$

следует, что

$$\wp(2z)+2\wp(z) = \frac{1}{4}\left(\frac{h_4+h_2^5}{h_2^2h_3}\right)^2.$$

Таким образом,

$$3\wp(z) = \frac{h_3}{h_2^2} + \frac{1}{4}\left(\frac{h_4+h_2^5}{h_2^2h_3}\right)^2.$$

Значение g_2 и а g_3 находится с помощью равенств

$$2\wp''(z) = 12\wp(z)^2 - \mathrm{g}_2, \quad \wp'(z)^2 = 4\wp(z)^3 - \mathrm{g}_2\wp(z) - \mathrm{g}_3.$$

По известной кривой (3) и значениям $\wp(z)$ и $\wp'(z)$ точка z определяется однозначно.

Из равенств (7)–(9) следует, что значения h_2, h_3, h_4, найденные исходя из формул (9), удовлетворяют соотношениям (6). Таким образом имеется взаимно однозначное соответствие между тройками параметров (h_2,h_3,h_4) и $(\mathrm{g}_2,\mathrm{g}_3,z)$.

При $a=nz$, $b=2z$, $c=z$, $d=0$ трёхчленное тождество Вейерштрасса

$$\begin{aligned}\sigma(a+b)\sigma(a-b)\sigma(c+d)\sigma(c-d) = \sigma(a+c)\sigma(a-c)\sigma(b+d)\sigma(b-d) - \\ - \sigma(a+d)\sigma(a-d)\sigma(b+c)\sigma(b-c)\end{aligned}$$

принимает вид

$$\sigma((n+2)z)\sigma((n-2)z)\sigma(z)^2 = \sigma((n+1)z)\sigma((n-1)z)\sigma(2z)^2 - \sigma(nz)^2\sigma(3z)\sigma(z), \tag{10}$$

а при $a=(n-1)z$, $b=3z$, $c=z$, $d=0$ —

$$\begin{aligned}\sigma((n+2)z)\sigma((n-4)z)\sigma(z)^2 = \\ = \sigma(nz)\sigma((n-2)z)\sigma(3z)^2 - \sigma((n-1)z)^2\sigma(2z)\sigma(4z).\end{aligned} \tag{11}$$

При $n\geqslant 5$ равенство (2) доказывается по индукции с помощью рекуррентного соотношения (4) и формул (10), (11) и (6). □

Замечание 3. Из доказанной теоремы следует, что эллиптическая последовательность, первоначально определённая равенством (4), удовлетворяет и осоотношению (1). Таким образом, определение (1) действительно является корректным.

Список литературы

[1] M. Ward, "Memoir on elliptic divisibility sequences", *Amer. J. Math.*, **70**, (1948), 31–74.

[2] Abramowitz, Milton, and Irene A. Stegun., *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, v. 55, Courier Corporation, 1965.

Поступила в редакцию
21 апреля 2019 г.

Исследование выполнено при частичной финансовой поддержке РФФИ (проект № 18-01-00638 А).

Ustinov A. V. A simplified proof of Ward's formula for elliptic sequences. *Far Eastern Mathematical Journal.* 2019. V. 19. No 1. P. 84–87.

ABSTRACT

An elliptic divisibility sequence (EDS) is a sequence of integers satisfying a nonlinear recursion relation arising from division polynomials on elliptic curves. EDS were first defined, and their arithmetic properties studied, by Morgan Ward in the 1948. In particular he has proven an explicit formula for the general term of the sequence in terms of the Weierstrass sigma function. In the present paper we give a simplified proof of Ward's formula.

Key words: *lliptic divisibility sequence, elliptic curves, Weierstrass elliptic functions.*