УДК 511, УДК 003.26

Вывод критерия Корсельта чисел Кармайкла из критерия связи чисел Кармайкла с функцией Кармайкла

Пастухов Ю.Ф., к. ф.-м. н., доц.
Полоцкий государственный университет
Пастухов А.Ю.;
Волосова Н.К., аспирант
Московский государственный технический университета МГТУ им. Н.Э. Баумана
Волосов К.А., профессор, д. ф.-м. н., Волосова А.К. , к. ф.-м. н.
МИИТ, г. Москва
Пастухов Д.Ф., к. ф.-м. н., доц.
Полоцкий государственный университет
Карлов М.И., к. ф.-м. н., доц.
Московский физико-технический институт (национальный исследовательский университет)
Чертков В.М., к. т. н., доц.
Полоцкий государственный университет

Derivation of the Corcelt criterion of Carmichael numbers from the criterion of the connection of Carmichael numbers with the Carmichael function

Pastukhov Y.F., Pastukhov D.F., Pastukhov A.Y., Karlov M.I.,
Volosova N.K., Volosov K.A., Volosova A.K., Chertkov V.M.

1. Введение Новым в данной работе является вывод критерия Корсельта чисел Кармайкла из критерия связи чисел Кармайкла с функцией Кармайкла.

Пусть $\varphi(n)$ - функция Эйлера, $\lambda(n)$ - функция Кармайкла. P - множество простых чисел

$n = p^{\alpha}(p \in P, n \in N)$ - примарное натуральное число (степень простого)

$HOK(a_1, a_2, \dots, a_s)$ - наименьшее общее кратное $a_1, a_2, \dots, a_s$

В работе[16] авторами был сформулирован и доказан следующий критерий:

Теорема 1[16] (критерий связи чисел Кармайкла с функцией Кармайкла). Составное число n является числом Кармайкла тогда и только тогда,

$$\frac{n-1}{\lambda(n)} \in N \quad (1)$$

Теорема 2

$$a_i \in N, \exists i: 1 \le i \le s, a_i \vdots d \Rightarrow HOK(a_1, a_2, \dots, a_s) \vdots d \quad (2)$$

Доказательство. $a_i \vdots d \Rightarrow a_i = dq, q \in N, A = HOK(a_1, a_2, \dots, a_s) \vdots a_i \Rightarrow A = a_i Q = dqQ \Rightarrow A \vdots d$

Теорема 3 (https://ru.wikipedia.org/wiki/Функция_Кармайкла) Для $n = p^{\alpha}(p \in P, n \in N)$

$$\lambda(n) = \begin{cases} \varphi(n), n = p^{\alpha}, (p > 2, \alpha \in \mathrm{N} \text{ или } p = 2, 1 \le \alpha \le 2) \\ \frac{1}{2}\varphi(n), n = p^{\alpha}, (p = 2, \alpha \ge 3) \end{cases} \quad (3)$$

Теорема 4 https://ru.wikipedia.org/wiki/Функция_Кармайкла

Пусть $n \in N \;\; n = \prod_{i=1}^{s} p_i^{\alpha_i}$ тогда

$$\lambda(n) = HOK\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})\right) \quad (4)$$

Теорема 5 (https://ru.wikipedia.org/wiki/Функция_Эйлера)

Пусть $n \in N \;\; n = \prod_{i=1}^{s} p_i^{\alpha_i}$, тогда

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) \quad (5)$$

Теорема 6 Пусть $n \in N \;\; n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Тогда $\lambda(n)$ не делится на $p_i \forall i = \overline{1,s}$

Доказательство. От противного. Пусть $\lambda(n) \vdots p_i$ для некоторого $p_i, 1 \le i \le s \Leftrightarrow \lambda(n) = p_i d_1, d_1 \in N$

Так как $(n-1) \vdots \lambda(n) \Rightarrow (n-1) = \lambda(n) * d_2, d_2 \in N \Rightarrow (n-1) = \lambda(n) * d_2 = p_i d_1 d_2$

Так как $n = \prod_{i=1}^{s} p_i^{\alpha_i}, \alpha_i \ge 1, i = \overline{1,s} \Rightarrow n \vdots p_i \forall i = \overline{1,s} \Rightarrow n = p_i d_3, d_3 \in N$

$n - (n-1) = 1 = p_i d_3 - p_i d_1 d_2 = p_i(d_3 - d_1 d_2) \Rightarrow 1 \vdots p_i$ Противоречие, так как $p_i \ge 2$

Теорема 7 Пусть $n \in N \;\; n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Тогда $p = 2$ не может входить в разложение n более, чем во второй степени, то есть, если $p_i = 2, 1 \le i \le s \Rightarrow 1 \le s_i \le 2$

Доказательство. Пусть это не так: $p_i = 2, 1 \le i \le s \Rightarrow s_i \ge 3$. Тогда по **теоремам 3,5**

$\lambda(p_i^{s_i}) = \frac{1}{2}\varphi(p_i^{s_i}) = \frac{1}{2}\varphi(2^{s_i}) = \frac{1}{2}(2^{s_i} - 2^{s_i - 1}) = \frac{1}{2}(2^{s_i - 1}) = 2^{s_i - 2} \ge 2^1 = 2$ так как по предположению $s_i \ge 3$,то по **теореме 5 формула(5)** $p_i^{\alpha_i} = p_i^{\alpha_i - 1}(p_i - 1) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$

И, значит, $\lambda(p_i^{s_i}) = \lambda(2^{s_i}) = 2^{s_i - 2} \vdots 2$. По **теореме 4** $\lambda(n) = HOK\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})\right)$

Значит, **по теоремам 2,5** так как $\lambda(p_i^{s_i}) = \lambda(2^{s_i}) \vdots 2 \Rightarrow \lambda(n) = HOK\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})\right) \vdots 2$

Но по **теореме 6** $\lambda(n)$ не делится ни на одно p_i, включая $p_i = 2$ Противоречие. **Теорема 7** доказана.

На самом деле, из **теоремы 7** вытекает более сильное чем в **теореме 7** утверждение:

Теорема 8 Пусть $n \in N$ $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Если $p_i = 2$ при некотором $1 \le i \le s$, тогда 1) $s_i = 1$ 2) $\lambda(p_i^{s_i}) = \lambda(2^{s_i}) = \varphi(2^{s_i}) = 2^{s_i - 1}$

Доказательство. Если $p_i = 2$ при некотором $1 \le i \le s$, то по **теореме 7** $s_i \le 2$ **По теореме 3**, так как $s_i \le 2 \Rightarrow \lambda(2^{s_i}) = \varphi(2^{s_i}) = 2^{s_i} - 2^{s_i-1} = 2^{s_i-1} \ge 2^1 = 2$ Значит, по **теоремам 2,3,4,5,если** $s_i = 2$

$$\lambda(p_i^{s_j}) = \lambda(2^{s_i}) = \varphi(2^{s_i}) = 2^{s_i-1} \vdots 2 \Rightarrow \lambda(n) = HOK\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})\right) \vdots 2$$

И так как по условию $(n-1)$: $\lambda(n) \Rightarrow (n-1) \vdots 2$ Но по **теореме 6** $\lambda(n)$ не делится ни на одно p_i, включая $p_i = 2$ Противоречие. **Теорема 8 доказана.** Для $p_i \in P, p_i > 2$ верна

Теорема 9 Пусть $n \in N$ $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Если $p_i > 2, p_i \in P$ при некотором $1 \le i \le s$, тогда

$$1)\ s_i = 1$$
$$2)\ \lambda(p_i^{s_i}) = \varphi(p_i^{s_i}) = p_i^{s_i-1}(p_i - 1) \tag{7}$$

Доказательство. По теореме 3 для $p_i \in P, p_i > 2 \Rightarrow \lambda(p_i^{s_i}) = \varphi(p_i^{s_i}) = p_i^{s_i} - p_i^{s_i-1} = p_i^{s_i-1}(p_i - 1)$

Значит, по **теоремам 3,5 ,если** $s_i \ge 2 \Rightarrow \lambda(p_i^{s_i}) = \varphi(p_i^{s_i}) = p_i^{s_i} - p_i^{s_i-1} = p_i^{s_i-1}(p_i - 1) \vdots p_i$

По **теоремам 2,4** $\lambda(n) = HOK\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})\right) \vdots p_i$ Но по **теореме 6** $\lambda(n)$ не делится ни на одно p_i Противоречие. **Теорема 9 доказана.**

Следствием **теорем 6-9** является

Теорема 10 Пусть $n \in N$ $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Тогда $\alpha_i = 1$ $\forall i = \overline{1,s} \Rightarrow n = \prod_{i=1}^{s} p_i$

Теорема 11 Пусть $n \in N$ $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Тогда $\lambda(n) = HOK(p_1 - 1, p_2 - 1, \dots, p_s - 1)$

Доказательство. По **теореме10** $\lambda(n) = \prod_{i=1}^{s} p_i$ По **теореме 4** $\lambda(n) = HOK\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_s^{\alpha_s})\right) =$ $= HOK\left(\lambda(p_1^1), \lambda(p_2^1), \dots, \lambda(p_s^1)\right)$ По **теореме 3** $HOK\left(\lambda(p_1^1), \lambda(p_2^1), \dots, \lambda(p_s^1)\right) = HOK\left(\varphi(p^1), \varphi(p_2^1), \dots, \varphi(p_s^1)\right) =$ $= HOK\ (p_1 - 1, p_2 - 1, \dots, p_s - 1)$

Теорема 11 доказана.

Теорема 12 Пусть $a, b_1, b_2, \dots, b_n \in N$ Тогда условие $a \vdots b_i$ $\forall i = \overline{1,n} \Leftrightarrow a$: $HOK(b_1, b_2, \dots, b_n)$

Доказательство. $b_i = \prod_{j=1}^{s} p_j^{\alpha_{ij}} i = \overline{1,n} \Rightarrow a \vdots b_i \Leftrightarrow a \vdots p_j^{\max(\alpha_{ij})} 1 \le i \le n$ $\forall j = \overline{1,s} \Leftrightarrow a \vdots HOK(b_1, \dots, b_n)$

Теорема 13 Пусть $n \in N$ $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ - составное $p_i \in P \forall i = \overline{1,s}$ Тогда

$(n-1) \vdots \lambda(n) \Leftrightarrow$ **1)** $n = \prod_{i=1}^{s} p_i$ и **2)** $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$

Доказательство. Достаточность. $(n-1) \vdots \lambda(n)$ По **теореме10** $n = \prod_{i=1}^{s} p_i$ По **теореме 11 и теореме 12**

$\lambda(n) = HOK(p_1 - 1, p_2 - 1, \dots, p_s - 1) \Leftrightarrow \lambda(n) \vdots (p_i - 1) \forall i = \overline{1,s} \Leftrightarrow (n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$

Необходимость. 1) $\prod_{i=1}^{s} p_i$ и **2)** $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$ Из 1) **по теоремам 3,4,5**

$\lambda(n) = HOK(\lambda(p_1), \lambda(p_2), \dots, \lambda(p_s)) = HOK(\varphi(p_1), \varphi(p_2), \dots, \varphi(p_s)) = HOK(p_1 - 1, p_2 - 1, \dots, p_s - 1)$

Из **2)** По **теореме 12** $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s} \Leftrightarrow (n-1) \vdots HOK(p_1 - 1, p_2 - 1, \dots, p_s - 1) = \lambda(n)$

Теорема 14 (Критерий Корсельта чисел Кармайкла) Составное число n является числом Кармайкла тогда и только тогда, когда 1) $n = \prod_{i=1}^{s} p_i$ и 2) $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$

Доказательство. По **теоремам 1,13** Составное число n-число Кармайкла $\Leftrightarrow (n-1) \vdots \lambda(n) \Leftrightarrow$
1) $n = \prod_{i=1}^{s} p_i$ и 2) $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$

Литература:

1. Волосова Н.К., Волосов К.А., Пастухов Д.Ф., Пастухов Ю.Ф. Решение уравнения Пуассона в целых числах по модулю p с кусочно разрывной правой частью // Евразийское Научное Объединение. – 2019. № 1-1 (47). С. 4-9.

2. Пастухов Ю.Ф., Пастухов А.Ю., Карлов М.И., Пастухов Д.Ф., Волосова Н.К., Чернов С.В. Поиск наилучшего приближения в метрике квадратичного отклонения ступенчатыми функциями для обратной функции плотности распределения Лапласа (определение уровней восстановления для плотности распределения Лапласа) // Евразийское Научное Объединение. – 2021. № 1-1 (71). С. 49-54.

3. Волосова Н.К., Басараб М.А., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. О роли профиля скорости на верхнем отрезке в гидродинамической задаче для прямоугольной каверны // Евразийское Научное Объединение. – 2020. № 5-1 (63). С. 11-17.

4. Волосова Н.К., Басараб М.А., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Модифицированное разностное уравнение К.Н. Волкова для уравнения Пуассона на прямоугольнике с четвертым порядком погрешности // Евразийское Научное Объединение. – 2019. № 6-1 (52). С. 4-11.

5. Волосова Н.К., Басараб М.А., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Вычисление поля давления по полю скорости в гидродинамической задаче для прямоугольной каверны // Евразийское Научное Объединение. – 2020. № 9-1 (67). С. 1-8.

6. Волосова Н.К. О нестационарном уравнении диффузии с полной производной по времени на прямоугольнике // Евразийское Научное Объединение. –2021. № 1-1 (71). С. 9-14.

7. Волосова Н.К. О решении уравнения Пуассона на прямоугольнике с шестым порядком погрешности за конечное число элементарных операций // Евразийское Научное Объединение. –2020. № 3-1 (61). С. 20-27.

8. Волосова Н.К. Нестационарная гидродинамическая задача в открытой прямоугольной каверне // Евразийское Научное Объединение. –2021. № 3-1 (73). С. 16-21.

9. Волосова Н.К. Конечные методы решения уравнения Пуассона на произвольном прямоугольнике с краевым условием Дирихле// Евразийское Научное Объединение. –2020. № 5-1 (63). С. 17-28.

10. Волосова Н.К., Волосов К.А., Волосова А.К., Карлов М.И., Пастухов Д.Ф., Пастухов Ю.Ф. Модифицированная формула Ньютона - касательных парабол на комплексной плоскости // Евразийское Научное Объединение. 2021. № 6-1 (76). С. 21-27.

11 Пастухов Ю.Ф., Пастухов Д.Ф., Карлов М.И., Пастухов А.Ю. Тензор многомерного обобщенного 0-импульса 1-ого ранга // Евразийское Научное Объединение. 2021. № 2-1 (72). С. 43-48.

12. Пастухов Ю.Ф., Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов А.Ю. Теорема о связи чисел Кармайкла с функцией Кармайкла // Евразийское Научное Объединение. 2021. № 6-1 (76). С. 50-53.

13. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Вычисление производных дробного порядка явной квадратурной формулой Гаусса с двумя узлами // Евразийское Научное Объединение. 2021. № 1-1 (71). С. 14-19.

14. Волосова Н.К. Мягкие краевые условия в гидродинамической задаче для профиля скорости в открытой прямоугольной каверне // Евразийское Научное Объединение. 2021. № 5-1 (75). С. 9-14.

15. Волосова Н.К., Волосов К.А., Волосова А.К., Карлов М.И., Пастухов Д.Ф., Пастухов Ю.Ф. Модифицированная формула Ньютона - касательных парабол на комплексной плоскости // Евразийское Научное Объединение. 2021. № 6-1 (76). С. 21-27.

16. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Вычисление производных дробного порядка с высокой степенью точности // Евразийское Научное Объединение. 2020. № 11-1 (69). С. 1-9.

17. Пастухов Ю.Ф., Пастухов Д.Ф. Тензор Эйлера-Лагранжа в расслоении (преобразование многомерного обобщенного 0-импульса) // Евразийское Научное Объединение. 2020. № 11-1 (69). С. 27-32.

18. Волосова Н.К., Басараб М.А., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Возможные виды течения в закрытой каверне и противоречия в задаче с подвижной крышкой // Евразийское Научное Объединение. 2020. № 12-1 (70). С. 4-14.

19. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. О Решении уравнения Пуассона на прямоугольнике с четвертым порядком погрешности за конечное число элементарных операций // Евразийское Научное Объединение. 2020. № 2-1 (60). С. 11-17.

20. Пастухов Ю.Ф., Пастухов А.Ю., Пастухов Д.Ф. Наилучшее приближение ступенчатыми функциями в метрике квадратичного отклонения для плотности распределения Лапласа // Евразийское Научное Объединение. 2020. № 3-1 (61). С. 39-44.

21. Пастухов Ю.Ф. Поиск наилучшего приближения в метрике квадратичного отклонения ступенчатыми функциями для распределения Коши // Евразийское Научное Объединение. 2019. № 10-1 (56). С. 10-15.

22. Волосова Н.К. Этап конструирования математической модели аневризмы. Течения в каверне и противоречия в задаче в "закрытой“ кювете. В сборнике: Некоторые актуальные проблемы современной математики и математического образования. Материалы 74-й научной конференции «Герценовские Чтения 2021». Российская Академия Образования; Академия информатизации образования; Российский государственный педагогический университет им. А. И. Герцена, Кафедра математического анализа, Кафедра компьютерной инженерии и программотехники. Санкт-Петербург, 2021. С. 208-213.

23. Пастухов Ю.Ф. “ Необходимые условия в обратной вариационной задаче ”, Фундаментальная и прикладная математика,7:1(2001), 285-288

24. Пастухов Ю.Ф., Пастухов Д.Ф., Чернов С.В., Пастухов А.Ю. Условия сохранения обобщенной энергии на экстремалях системы уравнений Эйлера-Лагранжа /Пастухов Ю.Ф. [и др.]. // Евразийское Научное Объединение. 2020. Т. 1. № 3(61). С. 32- 39.

25. Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф., Сперанская О.А. Геометрический подход для качественного поиска конвективных ячеек по температурному полю // Евразийское Научное Объединение. 2021. № 8-1 (78). С. 10-18.

26. Волосова Н.К., Басараб М.А., Волосов К.А., Волосова А.К., Пастухов Д.Ф., Пастухов Ю.Ф. Обобщенная модель открытой каверны для аневризмы кровеносных сосудов // Евразийское Научное Объединение. 2021. № 8-1 (78). С. 18-23.

27. Пастухов Ю.Ф., Пастухов Д.Ф., Чернов С.В., Карлов М.И., Пастухов А.Ю. Рекуррентные уравнения обобщенных импульсов. Достаточные условия сохранения обобщенных импульсов k-ого порядка на решениях системы уравнений обобщенных импульсов (k-1)-ого порядка // Евразийское Научное Объединение. 2021. № 8-1 (78). С. 34-38.

28. Волосова Н.К. Простейшая математическая модель образования Фибрина в аневризмах кровеносных капилляров // Евразийское Научное Объединение. 2021. № 10-1 (80). С. 17-23.

29. Пастухов Ю.Ф. Поиск наилучшего приближения в метрике квадратичного отклонения ступенчатыми функциями для обратной функции плотности распределения Коши. (Определение уровней восстановления для плотности распределения Коши) // Евразийское Научное Объединение. 2021. № 10-1 (80). С. 29-34.

30. Пастухов Д.Ф. Численные методы. Лекции. Численный практикум // Учебное пособие к лекционным и практическим занятиям для студентов специальности 1-40 01 01 Программное обеспечение информационных технологий 1-98 01 01 Компьютерная безопасность / Новополоцк. Москва, 2021. (3-е изд., дополненное)

31. Пастухов Д.Ф. Построение нестационарных моделей в оболочке Ansys Fluent // учебное пособие / Москва, 2018.

32. Пастухов Ю.Ф. Определение оптимальных уровней восстановления и квантования плотности нормального распределения в метрике квадратичного отклонения для алгоритмов сжатия данных // Евразийское Научное Объединение. 2018. № 11-1 (45). С. 16-21.