

УДК 511.2: 519.6

ТЕОРЕМА О СВЯЗИ ЧИСЕЛ КАРМАЙКЛА С ФУНКЦИЕЙ КАРМАЙКЛА

Ю.Ф. Пастухов, к. ф.-м. н., доц.

(Полоцкий государственный университет)

*Н.К. Волосова (аспирант Московского государственного технического
университета МГТУ им. Н.Э. Баумана);*

*К.А. Волосов, профессор, д.ф. - м.н., А.К. Волосова, к.ф.- м.н. (МИИТ) г.
Москва;*

Д.Ф. Пастухов, к. ф.-м. н., доц.

(Полоцкий государственный университет)

А.Ю. Пастухов

Аннотация: В работе рассмотрены примеры поиска чисел и функции Кармайкла. Доказана теорема (критерий) о связи числа Кармайкла и функции Кармайкла. Приведена таблица для первых девяти чисел Кармайкла и функции Кармайкла, подтверждающая утверждение теоремы.

Ключевые слова: теория чисел, численные методы, функция Эйлера, функция Кармайкла, криптография.

A THEOREM ON THE CONNECTION OF THE CARMICHAEL NUMBERS WITH THE CARMICHAEL FUNCTION

YU.F. Pastuhov, N.K. Volosova, K.A. Volosov, A.K. Volosova, D.F. Pastuhov,
A.Y. Pastuhov

Введение. История чисел Кармайкла связана с именами математиков Алвина Корсельта, Джона Черника, Эрдеша, Карла Померанса, которые применяются в криптографии. Для проверки является ли выбранное натуральное число числом Кармайкла, часто используется критерий Корсельта. В данной работе впервые приведен и доказан другой критерий для чисел Кармайкла, связывающий два определения для числа и функции Кармайкла. Полученные результаты могут быть применены в работах по криптографии [3],[4],[5],[6],[7],[8],[9],[10],[11],[12].

Постановка задачи. Данная работа написана для Российской научной библиотеки eLibrary.ru. Поэтому полный текст работы можно прочитать и (или) скопировать в eLibrary.ru, которому присвоен идентификационный номер eLIBRARY ID: 46338920.

Результаты полученной теоремы можно использовать в алгоритмах проверки целых чисел на простоту.

Литература

1. W.R. Alford, A. Granville, C. Pomerance. There are infinitely Many Carmichael Numbers//Annals of Mathematics: journal. – 1994/ - Vol/ 139/ - P. 703-722/- doi:102307/2118576.
2. Лидовский В.В. Теория информации: Учебное пособие. – М.: Компания Спутник+.2004. – 111 с. – ISBN 5-93406-661-7.
3. Раткин Л.С. Система распределенных стенографических реестров для управления и обеспечения кибербезопасности транспортного комплекса//Транспорт: наука, техника, управление. Научный информационный сборник. 2020. № 5. С. 62-65.
4. Раткин Л.С. Квантовые стеганографические телекоммуникационные комплексы с технологией распределенных скрытых реестров для единой системы мониторинга движения транспортных средств// Транспорт: наука, техника, управление. Научный информационный сборник. 2020. № 9. С. 64-66.
5. Вакуленко С.П., Волосова Н.К., Пастухов Д.Ф. Способы передачи QR-кода в стеганографии/ С.П. Вакуленко, Н.К. Волосова, Д.Ф. Пастухов //Мир транспорта. – 2018. Т.16. № 5(78). С. 14-25.
6. Пастухов Д.Ф., Волосова Н.К., Волосова А.К. Некоторые методы передачи QR-кода в стеганографии/ Д.Ф. Пастухов, Н.К. Волосова, А.К. Волосова //Мир транспорта. – 2019. Т.17. № 3(82). С. 16-39.
7. Пастухов Д.Ф., Пастухов Ю.Ф., Сеница П.Р. Шифрование данных на базе эллиптических кривых. Новополюцк. Изд-во ПГУ. 2016:72 с.
8. Волосова Н.К., Малыгина А.Д., Вакуленко С.П., Пастухов Д.Ф. Эффективная итерационная формула для краевой задачи уравнения Пуассона со сложно распределенными источниками. В сборнике: Некоторые актуальные проблемы современной математики и математического образования. Герценовские чтения – 2019. Материалы научной конференции. 2019. С. 201-208.
9. 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.
10. Афанасьев А.И., Князев В.Н. Разработка беспроводной системы управления на основе концепции интернет вещей//Моделирование, оптимизация и информационные технологии. 2020. Т. 8. №1(28). С. 8-9.
 11. 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.
 12. Богуш Р.П., Захарова И.Ю., Пастухов Ю.Ф., Пастухов Д.Ф., Наумович Н.М. Моделирование сжатия радиолокационных данных дистанционного зондирования земли на основе блочного адаптивного квантования// Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. 2019. № 4. С. 7-15.
 13. 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.
 14. Волосова Н.К. Возможные виды течения в закрытой каверне и противоречия в задаче с подвижной крышкой// Евразийское Научное Объединение. – 2020. № 12-1 (70). С. 4-14.
 15. Кристалинский В.Р., Кристалинский Р.Е. О решении задач математической физики в системе WOLFRAM MATHEMATICA//Современные информационные технологии и ИТ-образование. Т 15. № 4. 2019. С. 981-991.
 16. 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.
 17. 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.
 18. Волосов К.А., Данилов В.Г., Колобов Н.А., Маслов В.П. Доклады академии наук СССР. 1986. Т.33. С. 517.
 19. Volosov K.A., Danilov V.G., Maslov V.P. Structure of a weak discontinuity of solutions of quasilinear degenerate parabolic equations// Mathematical Notes. 1988. Т.43. №6. С. 479-485.
 20. Волосов К.А. Одевание решений для некоторых неинтегрируемых задач и некоторые инвариантные свойства анзаца метода Хироты//Дифференциальные уравнения. 2005. Т 41.№ 11.С. 1572-1575.

21. Волосов К.А. О собственных функциях структур, описываемых моделью “мелкой воды” на плоскости// *Фундаментальная и прикладная математика*. 2006. Т. 12. № 6. С. 17-32.
22. Волосов К.А. Построение решений квазилинейных параболических уравнений в параметрическом виде// *Дифференциальные уравнения*, 2007, Т.43, №.4., С.492-497.
23. Волосов К.А. Новый метод построения решений уравнений с частными производными в параметрической форме// *Известия Российского государственного педагогического университета им. А.И. Герцена*. 2007. Т.7. № 26. С. 13-20.
24. Волосов К.А. Конструкция решений квазилинейных уравнений с частными производными// *Сибирский журнал индустриальной математики* 2008, т.11, н.2(34), С. 29-39 .
25. В.П. Маслов, В.Г. Данилов, К.А. Волосов. Математическое моделирование процессов тепломассопереноса (эволюция диссипативных структур). С добавлением Н.А. Колобова, - М.:Наука, 1987, 352 с.
26. Волосова Н.К. О нестационарном уравнении диффузии с полной производной по времени на прямоугольнике// *Евразийское Научное Объединение*. –2021. № 1-1 (71). С. 9-14.
27. Волосова Н.К., Пастухов Д.Ф., Волосов К.А. Методы расширения области применения методов математической физики//*Международная конференция “Квазилинейные уравнения и обратные задачи”. QIPR conference handbook and proceedings*. – М.: МФТИ, 2018. – С 20.
28. 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.
29. The role of aeration in forming the thermal regime of a geothermal lake. Anisimova E.P., Pastukhov D.F., Speranskaya A.A., Speranskaya O.A.// *Izvestiya. Atmospheric and Oceanic Physics*. 1996. Т 32. № 2. С. 268-272.
30. Волосова Н.К. Нестационарная гидродинамическая задача в открытой прямоугольной каверне// *Евразийское Научное Объединение*. –2021. № 3-1 (73). С. 16-21.
31. 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.