УДК 511.2: 519.6

Теорема о связи чисел Кармайкла с функцией Кармайкла

Пастухов Ю.Ф., к. ф.-м. н., доц.
Полоцкий государственный университет
Волосова Н.К., аспирант
Московский государственный технический университет 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
Пастухов А.Ю.

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

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

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. Рассмотрим задачу о связи чисел Кармайкла и функции Кармайкла.

Определение 1. Составное число m называется числом Кармайкла, если

$\forall a \in Z|\text{НОД}(a,m) = 1 \Rightarrow a^{m-1} \equiv 1(modm)$(Wikipedia.org).

Пример 1. Обозначим множество остатков $Z_m = \{1,2,\dots,m-1\}$ числа m, а $z \in {}^{*}_{Z_m}|\text{НОД}(z,m) \equiv 1, m = 4$, $m-1 = 3|_{Z_m^*} = \{1,3\}. 1^3 \equiv 1(mod4), 3^3 = 27 \equiv 3(mod4)$- то есть, составное число 4 не является числом Кармайкла. Известно, что среди натурального ряда чисел Кармайкла меньше простых чисел, не превышающего заданного целого. Доказано, что это множество чисел Кармайкла бесконечно[1]. Минимальное число Кармайкла равно 561.

Пример 2. Докажем, что $m = 561$- число Кармайкла, используя критерий Корсельта: составное число m является числом Кармайкла, если и только если $(m-1)/(p_i - 1) \in N$, где $p_i = \{3,11,17\}$- только простые делители первой степени числа $m = 561$.

$$m = 561 = 3 \cdot 11 \cdot 17, m-1 = 560, p_i - 1 = \{2,10,16\}, (m-1)/(p_i - 1) = \{560/2, 560/10, 560/16\} \in N.$$

Числа Кармайкла иначе называют псевдопростыми числами, поскольку они удовлетворяют теореме Ферма (упрощенному варианту теоремы Эйлера – Ферма[2]): $\forall a \in Z|\text{НОД}(a,p) = 1 \Rightarrow a^{\varphi(p)} \equiv 1(modp)$, $\varphi(p) = p - 1 \Leftrightarrow p \in P$, если число p – простое. При этом выполнение условия $\forall a|1 < a < p$: $\text{НОД}(a,p) = 1$ очевидно.

Определение 2. Функцией Кармайкла целого числа n называется минимальная степень (натуральное число) $\lambda(n)$, такая, что для всех целых чисел a взаимно простых с n: $\forall a \in Z|\text{НОД}(a,n) = 1 \Rightarrow a^{\lambda(n)} \equiv 1(modn)$ (Wikipedia.org).

Замечание. Функция Кармайкла вычисляется для любого целого числа, независимо от того является ли оно числом Кармайкла или не является. Чтобы пояснить сказанное рассмотрим пример 3:

Пример 3. $n = 4, Z_4^* = \{1,3\}, \lambda(4) = 2 \Leftrightarrow 1^2 \equiv 1(mod4), 3^2 = 9 \equiv 1(mod4)$, но $3^1 = 3 \neq 1(mod4)$.

Запишем из справочника в **таблицу 1** 9 первых чисел m Кармайкла, $m-1$, их функции Кармайкла $\lambda(m)$. В последнем столбце вычислим значения $(m-1)/\lambda(m)$.

Таблица 1. **Связь чисел Кармайкла с функцией Кармайкла**

m	$m-1$	$\lambda(m)$	$(m-1)/\lambda(m)$
561	560	80	7
1105	1104	48	23
1729	1728	36	48
2425	2424	112	22
2821	2820	60	47
6601	6600	1320	5
8911	8910	198	45
41041	41040	120	342
825265	825264	144	5731

Видно, что во всех случаях числа $(m-1)/\lambda(m)$ целые. Это наводит на мысль о глубокой связи между числами Кармайкла и функции Кармайкла и в справедливости **Теоремы 1.**

Теорема 1 (*критерий связи между числом и функцией Кармайкла*). Составное число m является числом Кармайкла тогда и только тогда, когда $(m-1)/\lambda(m) \in N$.

Необходимость. Используем формулу логики $(A \Rightarrow B) \Leftrightarrow (\overline{B} \Rightarrow \overline{A})$. А доказательство необходимости проведем от противного $(\overline{B} \Rightarrow A)$, то есть, предположим, что если $(m-1)/\lambda(m) \notin N \Rightarrow$ составное число m является числом Кармайкла. Тогда $m = 1 + \lambda(m) \cdot k + r, k \in Z, r \in Z_{\lambda(m)} (0 < r < \lambda(m))$.

Рассмотрим произвольные целые числа a взаимно простые с m $a \in Z | \text{НОД}(a,m) = 1$, тогда по определению числа Кармайкла имеем

$$a^{m-1} \overset{01}{\equiv} 1(modm) \Leftrightarrow a^{1+\lambda(m)k+r-1} \equiv 1(modm) \Leftrightarrow a^r \cdot (a^{\lambda(m)})^k \equiv 1(modm) \overset{02}{\Leftrightarrow} a^r \equiv 1(modm), 1 \le r < \lambda(m)\ .$$

Но полученное неравенство $a^r \equiv 1(modm), 1 \le r < \lambda(m)$ противоречит **Определению 2** функции Кармайкла, так как нашлось другое число $r < \lambda(m)$ меньшее функции Кармайкла такое, что $a^r \equiv 1(modm)$,. То есть, число $\lambda(m)$ уже не является минимальным. Получили противоречие. Следовательно, справедливы формулы логики $(\overline{B} \Rightarrow \overline{A}) \Leftrightarrow (A \Rightarrow B)$. То есть, из того, что составное число m является числом Кармайкла следует

$$(m-1)/\lambda(m) \in N.$$

Достаточность. Пусть верно $(m-1)/\lambda(m) \in N$. Тогда $\exists k \in Z: m = 1 + \lambda(m) \cdot k$

$a^{m-1} = a^{\lambda(m)\cdot k} = (a^{\lambda(m)})^k \overset{02}{\equiv} 1^k(modm) \Leftrightarrow a^{m-1} \equiv 1(modm)$ - доказано, что составное число m удовлетворяет **Определению 1** для чисел Кармайкла.

Теорема 1 доказана.

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

Литература:

1. W.R. Alfond, A. Granville, C. Pomeramce. There are infinitely Many Carmichael Numberes//Annals of Mathematics: jornal. – 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., Синица П.Р. Шифрование данных на базе эллиптических кривых. Новополоцк. 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 р 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”. QIPA 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.