МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Московский государственный технический университет им. Н.Э. Баумана

Российский Университет Транспорта

Министерство образования Республики Беларусь

Полоцкий государственный университет имени Евфросинии Полоцкой

ПАСТУХОВ Ю.Ф.
(Полоцкий университет имени Евфросинии Полоцкой)

ВОЛОСОВА Н.К.
(Московский государственный технический университет им. Н.Э. Баумана – Национальный исследовательский университет);

ВОЛОСОВ К.А., ВОЛОСОВА А.К.
(Московский государственный университет путей сообщения Императора Николая || (Москва));

ПАСТУХОВ Д.Ф.
(Полоцкий университет имени Евфросинии Полоцкой)

НЕСКОЛЬКО ТЕОРЕМ О ЧИСЛАХ КАРМАЙКЛА

Учебное пособие к лекционным и практическим занятиям
для студентов специальности
1-98 01 01 Компьютерная безопасность

Москва
2023

УДК 511:512:519.6

Рецензенты:
Михаил Иванович Карлов, защитил диссертацию кандидата физико-математических наук на Механико-математическом факультете МГУ им. М.В. Ломоносова

Пастухов Ю.Ф., Волосова Н.К., Волосов К.А., Волосова А.К., Пастухов Д.Ф.
Несколько теорем о числах Кармайкла: Учебное пособие. – Москва. 2023.-33 с.

Учебное пособие содержит две работы о свойствах чисел Кармайкла, функции Кармайкла, функции Эйлера из пятнадцати теорем. Доказан критерий связи чисел Кармайкла и функции Кармайкла. Доказана эквивалентность полученного критерия и критерия Корсельта для чисел Кармайкла. Написана основная программа и подпрограммы, а также графический модуль на языке Visual Fortran 6.6 с учетом полученного критерия. Программой получены первые числа Кармайкла до 100 миллионов и занесены в таблицу.

Для студентов педагогических, технических университетов, преподавателей, инженеров, программистов использующих в своей практической деятельности эффективные методы и простые алгоритмы поиска простых чисел.

УДК 511:512:519.6

Введение

Числа Кармайкла впервые упоминаются с работы Алвина Корсельта, доказавшему в 1899 году теорему о целых составных числах, которые могут удовлетворять малой теореме Ферма. С тех пор числа Кармайкла называют псевдопростыми числами. Поскольку существование таких составных чисел сильно затрудняют поиск простых чисел, используя простой алгоритм Ферма.

В первой части доказан критерий связи чисел Кармайкла и функции Кармайкла.

Вторая часть содержит 15 теорем о свойствах чисел Кармайкла и их связи со свойствами функций Эйлера, Кармайкла. Три из 15 теорем доказаны и приведены на сайте Wikipedia.org. Во второй работе доказана эквивалентность критерия связи чисел и функции Кармайкла и критерия Корсельта.

На основе полученных теорем написана программа и графический интерфейс на языке Visual Fortran 6.6 с применением специальной библиотеки Xeffort 1.2.24. С помощью программы сведены в таблицу все числа Кармайкла, величина которых не превышает 100 миллионов.

Авторы читали студентам 2-3 курсов предметы Основы информационной безопасности, Математические основы криптологии, Безопасность в компьютерных сетях, Криптотехнологии (магистратура) с учетом сведений о числах Кармайкла, используя материал из данного пособия для теоретических и практических занятий. Основные программы и подпрограммы написаны на языке FORTRAN, который редко используется, но незаменим с математической точки зрения, поэтому программа на данном языке может также принести студентам пользу.

ОГЛАВЛЕНИЕ

УДК 511.2:512: 519.6

ТЕОРЕМА О СВЯЗИ ЧИСЕЛ КАРМАЙКЛА С ФУНКЦИЕЙ КАРМАЙКЛА

Пастухов Юрий Феликсович
(Полоцкий государственный университет);
Волосова Наталья Константиновна
(Московский государственный технический университета МГТУ им. Н.Э. Баумана);
Волосова Александра Константиновна
(Московский Университет Транспорта, г. Москва);
Волосов Константин Александрович
(Московский Университет Транспорта, г. Москва);
Пастухов Дмитрий Феликсович
(Полоцкий государственный университет.

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

Введение. История чисел Кармайкла связана с именами математиков Алвина Корсельта, Джона Черника, Эрдеша, Карла Померанса, которые применяются в криптографии [1],[2],[3],[4],[5],[6]. 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 связаны с результатами, полученными авторами в работах по криптографии [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36].

Постановка задачи. Рассмотрим задачу о связи чисел Кармайкла и функции Кармайкла.

Определение 1. Составное число m называется числом Кармайкла, если $\forall a \in Z \left| НОД(a,m) = 1 \right. \Rightarrow a^{m-1} \equiv 1 (\mathrm{mod}\, m)$ (Wikipedia.org).

Пример 1. Обозначим множество остатков $Z_m = \{1,2,...,m-1\}$ числа m, а $z \in Z_m^* \left| НОД(z,m) \equiv 1 \right.$,

$1) m = 4, m-1 = 3 \mid \overset{*}{Z}_m = \{1,3\}. 1^3 \equiv 1 (\mathrm{mod}\ 4), 3^3 = 27 \equiv 3 (\mathrm{mod}\ 4)$- то есть, составное число 4 не является числом Кармайкла. Известно, что среди натурального ряда чисел Кармайкла меньше числа простых чисел, не превышающих 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]):

$\forall a \in Z \mid НОД(a, p) = 1 \Rightarrow a^{\varphi(p)} \equiv 1 (\mathrm{mod}\ p),$ где - функция Эйлера целого числа p

$\varphi(p) = p - 1 \Leftrightarrow p \in P$ если число p – простое. Для простого числа p выполнение условия $\forall a \mid 1 < a < p : НОД(a, p) = 1$ 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 $n : \forall a \in Z \mid НОД(a, n) = 1 \Rightarrow a^{\lambda(n)} \equiv 1 (\mathrm{mod}\ n)$ (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. $n = 4, \overset{*}{Z}_4 = \{1,3\}, \lambda(4) = 2 \Leftrightarrow 1^2 \equiv 1 (\mathrm{mod}\ 4), 3^2 = 9 \equiv 1 (\mathrm{mod}\ 4)$, но $3^1 = 3 \neq 1 (\mathrm{mod}\ 4)$.

Запишем из справочника в **таблицу 1** 9 первых чисел m Кармайкла, $m-1$, обозначим 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
2465	2464	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 $a \in Z | НОД(a,m) = 1$,тогда по определению числа Кармайкла имеем $a^{m-1} \overset{O1}{\equiv} 1 (\mathrm{mod}\, m) \Leftrightarrow a^{1+\lambda(m)\cdot k+r-1} \equiv 1 (\mathrm{mod}\, m) \Leftrightarrow a^r \cdot \left(a^{\lambda(m)}\right)^k \equiv 1 (\mathrm{mod}\, m) \overset{O2}{\Leftrightarrow} a^r \equiv 1 (\mathrm{mod}\, m), 1 \le r < \lambda(m)$.

Но полученное неравенство $a^r \equiv 1 (\mathrm{mod}\, m), 1 \le r < \lambda(m)$ противоречит **Определению 2** функции Кармайкла, так как нашлось другое число $r < \lambda(m)$ меньшее функции Кармайкла такое, что $\forall a : НОД(a,m) = 1 \Rightarrow a^r \equiv 1 (\mathrm{mod}\, m)$. 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 $\exists k \in Z : m = 1 + \lambda(m) \cdot k$. Далее выберем такие остатки a числа m, для которых $a \in Z | НОД(a,m) = 1$, имеем

$a^{m-1} = a^{\lambda(m)\cdot k} = \left(a^{\lambda(m)}\right)^k \overset{O2}{\equiv} 1^k (\mathrm{mod}\, m) \Leftrightarrow \forall a \in Z | НОД(a,m) = 1,\ a^{m-1} \equiv 1 (\mathrm{mod}\, m)$ - доказано, что составное число m удовлетворяет **Определению 1** для числа 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. Лидовский В.В. Теория информации: Учебное пособие. – М.: Компания Спутник +,2004. – 111 с. –ISSN 5-93406-661-7.
2. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. — Казань: КФУ, 2011. — 190 с.
3. 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.
4. Вывод критерия Корсельта чисел Кармайкла из критерия связи чисел Кармайкла с функцией Кармайкла / Ю. Ф. Пастухов, А. Ю. Пастухов,

Н. К. Волосова [и др.] // Евразийское Научное Объединение. – 2021. – № 12-1(82). – С. 31-34. – EDN GDLERY.

5. Теорема о связи чисел Кармайкла с функцией Кармайкла / Ю. Ф. Пастухов, Н. К. Волосова, К. А. Волосов [и др.] // Евразийское Научное Объединение. – 2021. – № 6-1(76). – С. 50-53. – EDN HTIQST.
6. 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.
7. 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.
8. Мурашов, Д. И. Социальный генетический алгоритм / Д. И. Мурашов, Л. Н. Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2006. – № 4(4). – С. 53-60. – EDN YMWFVB.
9. Гладкий, С. Л. Верификация численных расчетов методом фиктивных канонических областей / С. Л. Гладкий, Н. Ф. Таланцев, Л. Н. Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2006. – № 4(4). – С. 18-27. – EDN YMWFVJ.
10. Филиппов, Н. А. Математический путь к лучшей количественной информационной технике / Н. А. Филиппов // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 71-83. – EDN MNIHZT.
11. Плаксин, М. А. Механизмы сокращения нагрузки на эксперта при применении метода анализа иерархий / М. А. Плаксин // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 64-70. – EDN MNIHZJ.
12. Городилов, А. Ю. Криптоанализ перестановочного шифра с помощью генетического алгоритма / А. Ю. Городилов // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 44-49. – EDN MNIHYF.
13. Остапенко, Е. Н. Профессор Владимир Владимирович Маланин / Е. Н. Остапенко // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 222-226. – EDN MNIIHL.
14. Айдаров, Ю. Р. Новый алгоритм анализа протоколов информационной безопасности и оценка его вычислительной сложности / Ю. Р. Айдаров // Вестник Пермского университета. Математика. Механика. Информатика. – 2008. – № 4(20). – С. 165-168. – EDN MNLKGR.
15. Фирсов, А. Н. Оценка эффективности некоторых оптимизаций протоколов надежной и атомарной групповой рассылки / А. Н. Фирсов // Вестник Пермского университета. Математика. Механика. Информатика. – 2009. – № 3(29). – С. 161-168. – EDN KHNUXV.

16. Малых, А. Е. Андрей Николаевич Колмогоров / А. Е. Малых, В. И. Данилова // Вестник Пермского университета. Математика. Механика. Информатика. – 2009. – № 3(29). – С. 216-224. – EDN KHNVAN.
17. Данилова, Е. Ю. Сравнение генетических алгоритмов на примере задачи коммивояжера / Е. Ю. Данилова, А. Ю. Городилов // Вестник Пермского университета. Математика. Механика. Информатика. – 2009. – № 3(29). – С. 49-53. – EDN KHNUQN.
18. Пенский, О. Г. Профессор Леонид Нахимович Ясницкий / О. Г. Пенский // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 1(1). – С. 6-8. – EDN LGKJNP.
19. Морозенко, В. В. Генетический алгоритм для криптоанализа шифра Виженера / В. В. Морозенко, Г. О. Елисеев // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 1(1). – С. 75-80. – EDN LGKJRL.
20. Тарунин, Е. Л. Возможности вычислительных методов в проблемах теории чисел / Е. Л. Тарунин // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 2(2). – С. 15-28. – EDN MNLKJT.
21. Малых, А. Е. Об историческом процессе развития теории латинских квадратов и некоторых их приложениях / А. Е. Малых, В. И. Данилова // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 4(4). – С. 95-104. – EDN NDXQYZ.
22. Черномордик, И. В. Об одном алгоритме восстановления в задаче распознавания изображения / И. В. Черномордик // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 4(4). – С. 50-53. – EDN NDXQVX.
23. Тарунин, Е. Л. Уточнения формул распределения простых чисел / Е. Л. Тарунин // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 1(5). – С. 10-19. – EDN NTUHTV.
24. Ермакова, Л. М. Методы классификации текстов и определения качества контента / Л. М. Ермакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 3(7). – С. 47-53. – EDN OIVSGR.
25. Толюпа, Е. А. Доверенная цифровая подпись на базе алгоритма ЭЦП ГОСТ Р 34.10-94 / Е. А. Толюпа // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 3(7). – С. 63-66. – EDN OIVSHV.
26. Городилов, А. Ю. Криптоанализ тригонометрического шифра с помощью генетического алгоритма / А. Ю. Городилов, А. А. Митраков // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 4(8). – С. 75-82. – EDN PDBIQB.
27. Замятина, Е. Б. Построение синтаксически и семантически правильной Queue Network-модели в Triad.Net / Е. Б. Замятина, А. В. Шафранов //

Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 4(8). – С. 83-91. – EDN PDBIQL.
28. Полищук, В. И. Подход к созданию автоматизированной информационно-аналитической системы мониторинга безопасности г. Перми / В. И. Полищук // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 4(4). – С. 75-79. – EDN NDXQXV.
29. Ермакова, Л. М. Методы обнаружения писем-трансформеров / Л. М. Ермакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 2(6). – С. 77-85. – EDN OIVSCL.
30. Ермакова, Л. М. Методы извлечения информации из текста / Л. М. Ермакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2012. – № 1(9). – С. 77-84. – EDN PCVJRF.
31. Макеев, Н. Н. Выдающееся открытие XIX века (к 200-летию со дня рождения Эвариста Галуа) / Н. Н. Макеев // Вестник Пермского университета. Математика. Механика. Информатика. – 2012. – № 2(10). – С. 68-75. – EDN PCRVKT.
32. Чуприна, С. И. Разработка подхода к индексации смыслового содержания графической информации на принципах онтологического инжиниринга / С. И. Чуприна, В. А. Никифоров // Вестник Пермского университета. Математика. Механика. Информатика. – 2013. – № 3(22). – С. 111-118. – EDN RPSSZV.
33. Шафер, А. Е. Двухфакторная аутентификация с использованием СМС-сервиса / А. Е. Шафер, А. В. Черников // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – № 1(28). – С. 79-85. – EDN UHSZBX.
34. Тюрин, С. Ф. Восстановитель информации в двухканальной самосинхронной схеме / С. Ф. Тюрин, А. Н. Каменских // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – № 4(31). – С. 105-109. – EDN VHLGIL.
35. Шабуров, А. С. Обнаружение компьютерных атак на основе функционального подхода / А. С. Шабуров, А. А. Миронова // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – № 4(31). – С. 110-115. – EDN VHLGIV.
36. Климов, А. А. Определение авторства произведений изобразительного искусства на основе частотного анализа цветов и энтропии цифровых отпечатков / А. А. Климов, Е. В. Овчинникова, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2016. – № 4(35). – С. 43-52. – DOI 10.17072/1993-0550-2016-4-43-52. – EDN XUXJJZ.

УДК 511.2:512: 519.6

ВЫВОД КРИТЕРИЯ КОРСЕЛЬТА ДЛЯ ЧИСЕЛ КАРМАЙКЛА ИЗ КРИТЕРИЯ СВЯЗИ ЧИСЕЛ КАРМАЙКЛА С ФУНКЦИЕЙ КАРМАЙКЛА

Пастухов Юрий Феликсович
(Полоцкий государственный университет);
Волосова Наталья Константиновна
(Московский государственный технический университета МГТУ им. Н.Э. Баумана);
Волосова Александра Константиновна
(Московский Университет Транспорта, г. Москва);
Волосов Константин Александрович
(Московский Университет Транспорта, г. Москва);
Пастухов Дмитрий Феликсович
(Полоцкий государственный университет.

DERIVATION OF THE CORSELT CRITERION FOR CARMICHAEL NUMBERS FROM THE CRITERION FOR THE RELATIONSHIP BETWEEN CARMICHAEL NUMBERS WITH CARMICHAEL FUNCTION

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

Аннотация: *В работе рассмотрено несколько утверждений о свойствах чисел Кармайкла. Используя свойства чисел Кармайкла, функции Кармайкла и фуннкции Эйлера доказана эквивалентность двух критериев. А именно, эквивалентность критерия Корсельта для поиска чисел критерию связи чисел Кармайкла с функцией Кармайкла. Простые доказательства одиннадцати теорем опираются на три ранее известные факты-теоремы.*
Ключевые слова*: теория чисел, численные методы, функция Эйлера, функция Кармайкла, криптография.*

Введение. В данной работе впервые получен вывод критерия Корсельта чисел Кармайкла из критерия связи чисел Кармайкла с функцией Кармайкла. В предыдущей работе был доказан критерий связи функции Кармайкла с числами Кармайкла. Вторая статья учебного пособия посвящена эквивалентности двух критериев - критерия Корсельта и критерия связи чисел Кармайкла с функцией Кармайкла.

Постановка задачи и основные доказанные утверждения

Для удобства введем обозначения:

$\varphi(n)$ - функция Эйлера,

$\lambda(n)$ - функция Кармайкла,

P - Множество простых чисел, N - множество натуральных чисел,

$n = p^{\alpha}(p \in P, n \in N, \alpha \in N)$[4] - примарное натуральное число (степень простого числа),

$A = \text{НОК}(a_1, a_2, ..., a_s)$-наименьшее общее кратное чисел $a_1, a_2, ..., a_s$.

В работе**[1]** авторами был доказан следующий критерий:

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

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

Теорема 2. $$a_i \in N, \exists i : 1 \le i \le s, a_i \vdots d \Rightarrow \text{НОК}(a_1, a_2, ..., a_s) \vdots d \quad (2)$$

Замечание 1. Здесь и далее используется общепринятое обозначение $a_i \vdots d$ - означает, что число a_i делится нацело на число d.

Доказательство.

$$a_i \vdots d \Rightarrow a_i = dq_i, q_i \in N, d \in N, A = \text{НОК}(a_1, a_2, ..., a_s) \vdots a_i \Rightarrow A = a_i Q_i = dq_i Q_i \Rightarrow A \vdots d(Q_i \in N)$$

Теорема 2 доказана.

Теорема 3. (https://ru.wikipedia.org/wiki/Функция_Кармайкла)

(ссылка на теорему без доказательства). Для $n = p^{\alpha}(p \in P, n \in N, \alpha \in N)$

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

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

(ссылка на теорему без доказательства).

Пусть $n \in N, n = \prod_{i=1}^{s} p_i^{\alpha_i}, p_i \ge 2$ тогда $\lambda(n) = \text{НОК}\left(\lambda\left(p_1^{\alpha_1}\right), \lambda\left(p_2^{\alpha_2}\right), ..., \lambda\left(p_s^{\alpha_s}\right)\right)$ (4)

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

(ссылка на теорему без доказательства).

Пусть $n \in N, n = \prod_{i=1}^{s} p_i^{\alpha_i}$, тогда $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) = n\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1)$ (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 любой элементарный делитель $p_i \ge 2\left(i = \overline{1,s}\right)$ числа n.

Доказательство Теоремы 6 проведем от противного. Пусть $\lambda(n) \vdots p_i$ для некоторого $p_i, 1 \le i \le s \Leftrightarrow \lambda(n) = p_i d_i, d_i \in N, p_i \in N$.

Так как по условию **Теоремы 6** $(n-1) \vdots \lambda(n) \Rightarrow (n-1) = \lambda(n) \cdot d_0 = d_0 p_i d_i, d_0 \in N \Rightarrow (n-1) \vdots p_i$

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

Однако, $n - (n-1) = 1 = p_i d_3 - d_0 p_i d_i = p_i(d_3 - d_0 d_i) \Rightarrow 1 \vdots p_i$ получили противоречие, так как $p_i \ge 2$ (**Теорема 4**). **Теорема 6** доказана.

Теорема 7. Пусть $n \in N, n = \prod_{i=1}^{s} p_i^{\alpha_i}$ и $(n-1) \vdots \lambda(n)$. Тогда $p_i=2$ может входить в разложение n только во второй степени или в первой степени $\alpha_i \le 2$. То есть, если $p_i=2$, то следует, что $\alpha_i \in \{1,2\}$.

Доказательство Теоремы 7 проведем от противного. Пусть это не так: $p_i = 2, 1 \le i \le s \Rightarrow \alpha_i \ge 3$. Тогда по **Теореме 3** имеем

$$\lambda\left(p_i^{\alpha_i}\right) = \frac{1}{2}\varphi\left(p_i^{\alpha_i}\right) = \frac{1}{2}\varphi\left(2^{\alpha_i}\right) = \frac{1}{2}\left(2^{\alpha_i} - 2^{\alpha_i - 1}\right) = \frac{1}{2}\left(2^{\alpha_i - 1}\right) = 2^{\alpha_i - 2} \ge 2^1 = 2$$

так как по предположению $\alpha_i \ge 3$.

Другими словами, $\lambda\left(p_i^{\alpha_i}\right) = \frac{1}{2}\varphi\left(p_i^{\alpha_i}\right) = 2^{\alpha_i - 1} \vdots 2 (\lambda_i \ge 3)$, а функция Кармайкла делится нацело на два.

С учетом полученного результата $\lambda\left(p_i^{\alpha_i}\right) = 2^{\alpha_i - 1} \vdots 2 (p_i = 2, \alpha_i \ge 3)$, **Теоремы 4** и **Теоремы 2** $\lambda(n) = \text{НОК}\left(\lambda\left(\text{p}_1^{\alpha_1}\right), \lambda\left(\text{p}_2^{\alpha_2}\right), ..., \lambda\left(\text{p}_\text{s}^{\alpha_\text{s}}\right)\right)$ имеем, что $\lambda(n) = \text{НОК}\left(\lambda\left(\text{p}_1^{\alpha_1}\right), \lambda\left(\text{p}_2^{\alpha_2}\right), ..., \lambda\left(\text{p}_\text{s}^{\alpha_\text{s}}\right)\right) \vdots 2$

Но по доказанной **Теореме 6** $\lambda(n)$ не делится ни на одно p_i, включая $p_i = 2$. Полученное противоречие доказывает **Теорему 7**.

Оказывается, что из **Теоремы 7** вытекает более сильное 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 индексе $i = \overline{1,s}$, тогда верны два утверждения

1) $\alpha_i = 1$ 2) $\lambda(p_i^{\alpha_i}) = \lambda(2^{\alpha_i}) = \varphi(2^{\alpha_i}) = 2^{\alpha_i - 1}$ (6)

Доказательство теоремы проведем конструктивно. Если $p_i = 2$ при некотором индексе $i = \overline{1,s}$, то по **Теореме 7** $\alpha_i \le 2$. **По теореме 3** имеем

$\alpha_i \le 2 \Rightarrow \lambda\left(2^{\alpha_i}\right) = \varphi\left(2^{\alpha_i}\right) = 2^{\alpha_i} - 2^{\alpha_i - 1} = 2^{\alpha_i - 1} \le 2$. Значит, **теоремам 2,5, если** $s_i = 2$

По **Теореме 3** для случая $\alpha_i = 2$ получим

$$\lambda\left(p_i^{\alpha_i}\right) = \lambda\left(2^{\alpha_i}\right) = \varphi\left(2^{\alpha_i}\right) = 2^{\alpha_i} - 2^{\alpha_i - 1} = 2^{\alpha_i - 1} = 2$$

По **Теореме 2** и по **Теореме 4** имеем $\lambda(n) = \text{НОК}\left(\lambda\left(\text{p}_1^{\alpha_1}\right), \lambda\left(\text{p}_2^{\alpha_2}\right), ..., \lambda\left(\text{p}_\text{s}^{\alpha_\text{s}}\right)\right) \vdots 2$

Согласно условию **Теоремы 8** $(n-1) \vdots \lambda(n) \Rightarrow (n-1) \vdots 2$. Но по **Теореме 6** $\lambda(n)$ не делится ни на одно p_i, включая $p_i = 2$ Полученное противоречие доказывает **Теорему 8.**

Для $p_i \in P, p_i > 2$ верна следующая теорема

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

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

Доказательство. Согласно результату **Теоремы 3** для $p_i \in P, p_i > 2 \Rightarrow \lambda\left(p_i^{\alpha_i}\right) = \varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i - 1}(p_i - 1)$.

Тогда если $p_i > 2$, то $\lambda\left(p_i^{\alpha_i}\right) = \varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i - 1}(p_i - 1) \vdots p_i (p_i > 2)$.

По **Теореме 2** $\lambda(n) = \text{НОК}\left(\lambda\left(\text{p}_1^{\alpha_1}\right), \lambda\left(\text{p}_2^{\alpha_2}\right), ..., \lambda\left(\text{p}_\text{s}^{\alpha_\text{s}}\right)\right) \vdots p_i$. Но по **Теореме 6** $\lambda(n)$ не делится ни на одно $p_i \ge 2$, в частности на $p_i > 2$. Полученное противоречие доказывает **Теорему 9.**

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 справедливо утверждение $\alpha_i = 1 \forall i = \overline{1,s} \Rightarrow n = \prod_{i=1}^{s} p_i$. Другими словами, в разложении натурального числа n примарные делители p_i числа n могут входить только в первой степени.

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

Тогда $\lambda(n) = \text{НОК}(p_1 - 1, p_2 - 1, ..., p_s - 1)$.

Доказательство. По **Теореме 10** $n = \prod_{i=1}^{s} p_i$. Последовательно, используя **Теоремы 4,10,3,5,** получим цепочку преобразований

$$\lambda(n) \overset{T4}{=} \text{НОК}\left(\lambda\left(p_1^{\alpha_1}\right), \lambda\left(p_2^{\alpha_2}\right), ..., \lambda\left(p_s^{\alpha_s}\right)\right) \overset{T10}{=} \text{НОК}\left(\lambda\left(p_1^1\right), \lambda\left(p_2^1\right), ..., \lambda\left(p_s^1\right)\right) \overset{T3}{=} \text{НОК}\left(\varphi\left(p_1^1\right), \varphi\left(p_2^1\right), ..., \varphi\left(p_s^1\right)\right) \overset{T5}{=} \text{НОК}(p_1 - 1, p_2 - 1, ..., p_s - 1)$$

Таким образом, **Теорема 11** доказана.

Теорема 12. Пусть $a, b_1, b_2, ..., b_n \in N$. И пусть $a \vdots b_i \forall i = \overline{1,n}$. Тогда справедлив критерий

$a \vdots b_i \forall i = \overline{1,n} \Leftrightarrow a \vdots \text{НОК}(b_1, b_2, ..., b_n)$.

Доказательство. В силу единственности разложения произвольного целого числа b_i на примарные множители $p_j, j = \overline{1,s}$ получим $b_i = \prod_{j=1}^{s} p_j^{\alpha_{i,j}}, i = \overline{1,n}$. По условию теоремы $a \vdots b_i \forall i = \overline{1,n} \Leftrightarrow a \vdots p_j^{\max\limits_{i=1,n}(\alpha_{i,j})} \forall j = \overline{1,s} \Leftrightarrow a \vdots \text{НОК}(b_1, b_2, ..., b_n)$.

Теорема 12 доказана.

Теорема 13. Пусть $n \in N, n = \prod_{i=1}^{s} p_i^{\alpha_i}$, $p_i \in P \ \forall i = \overline{1,s}$ - составное. Тогда условие $(n-1) \vdots \lambda(n)$ равносильно двум таким условиям

$1) n = \prod_{i=1}^{s} p_i \quad 2) (n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$.

Доказательство.

Достаточность. Пусть $(n-1) \vdots \lambda(n)$. По **Теореме 10** $n = \prod_{i=1}^{s} p_i$.

По **Теореме 11** и по **Теореме 12** получим

$\lambda(n) = \text{НОК}(p_1 - 1, p_2 - 1, ..., p_s - 1) \Leftrightarrow \lambda(n) \vdots (p_i - 1) \ \forall i = \overline{1,s} \Rightarrow (n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$

Достаточность доказана.

Необходимость. Пусть $1) n = \prod_{i=1}^{s} p_i \quad 2) (n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$.

Из первого условия $n = \prod_{i=1}^{s} p_i$ по **Теоремам 3,4** имеем

$$\lambda(n) \overset{T10}{=} \text{НОК}(\lambda(p_1), \lambda(p_2), ..., \lambda(p_s)) \overset{T3}{=} \text{НОК}(\varphi(p_1), \varphi(p_2), ..., \varphi(p_s)) \overset{T5}{=} \text{НОК}(p_1 - 1, p_2 - 1, ..., p_s - 1)$$

Из второго условия $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$ получим по **Теореме 12**

$$(n-1) \vdots (p_i - 1) \forall i = \overline{1,s} \overset{T12}{\Rightarrow} (n-1) \vdots \text{НОК}(p_1 - 1, p_2 - 1, ..., p_s - 1) \overset{T11}{=} \lambda(n)$$

Достаточность доказана.

Теорема 14 (Критерий Корсельта для 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.

Необходимость. Пусть n-число Кармайкла. По **Теореме 1** это равносильно $(n-1) \vdots \lambda(n)$. По **Теореме 13** это равносильно выполнению 2-х условий $n = \prod_{i=1}^{s} p_i$ и $(n-1) \vdots (p_i - 1) \forall i = \overline{1,s}$. Необходимость доказана.

Достаточность. Пусть выполнены условия $n=\prod_{i=1}^{s} p_i$ и $(n-1):(p_i-1)\forall i=\overline{1,s}$. Из **Теоремы 13** следует, что $(n-1):\lambda(n)$. А из **Теоремы 1** следует, что n – число Кармайкла.

Теорема 15. Числа Кармайкла нечетны.

Доказательство теоремы проведем от противного. Пусть сотавное число Кармайкла n четно. Тогда число n-1 нечетно. Следовательно, число n-1 раскладывается только на нечетные делители. По Теореме 1 $(n-1):\lambda(n)$. По **Теореме 11** $\lambda(n)=\text{НОК}(p_1-1,p_2-1,...,p_s-1)$. Следовательно, $(n-1):(p_1-1),(n-1):(p_2-1),...,(n-1):(p_s-1)$. Но $(p_1-1)=2k_1+1,(p_2-1)=2k_2+1,...,(p_s-1)=2k+1_s$, $k_1,k_2,...,k_s\in N$. Тогда каждый делитель $p_1,p_2,...,p_s$ числа Кармайкла n $p_1=2k_1+2,p_2=2k_2+2,...,(p_s-1)p_s=2k_s+2,n=\prod_{i=1}^{s} p_i$ является четным числом. Но число Кармайкла составное, имеет не менее двух делителей не меньших 2. По доказанному здесь каждый делитель $p_1,p_2,...,p_s$ четный, поэтому оно (n) делится на два в степени s, что противоречит **Теореме 14**, так как делитель числа n $p_k=2^s,s\geq 2,s\in N$ не является примарным. **Теорема 15** доказана.

Замечание 2. Два условия $n=\prod_{i=1}^{s} p_i$ и $(n-1):(p_i-1)\forall i=\overline{1,s}$, которые используются для поиска чисел Кармайкла, называют алгоритмом Корсельта.

Разделы математической теории криптографии и теории компьютерной безопасности используют известные таблицы простых чисел, а также генерируют новые большие по величине простые числа на базе известных небольших простых чисел ускоренными (комбинированными алгоритмами). Некоторые алгоритмы отбора простых чисел среди всех целых используют теорему Эйлера – Ферма. Среди возможных найденных чисел нужно отбросить числа Кармайкла. Поэтому эффективные алгоритмы поиска чисел Кармайкла поспособствуют открытию новых больших простых чисел. Авторы учебного пособия будут рады, если приведенные здесь теоремы о свойствах чисел Кармайкла, функции Кармайкла, функции Эйлера и их связи дадут пользу для алгоритмов поиска новых чисел Кармайкла и простых чисел.

Полученные в двух работах результаты можно использовать для поиска простых чисел в криптографии и компьютерной безопасности. Отметим важные результаты в криптографии, компьютерной безопасности, теории чисел, полученные Уральской школой математиков и криптографов [5], [6], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49]. Отметим, что будущий академик Иван Матвеевич Виноградов начинал работать в стенах Пермского Государственного Университета, специалист в математической теории чисел. Также известно, что Механико-математический факультет Пермского Государственного Университета

(Пермский Государственный Национальный Исследовательский Университет) стал пятым мехматом на территории России в 1916 году.

Литература

1. Лидовский В.В. Теория информации: Учебное пособие. – М.: Компания Спутник +,2004. – 111 с. –ISSN 5-93406-661-7.
2. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. — Казань: КФУ, 2011. — 190 с.
3. 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.
4. Вывод критерия Корсельта чисел Кармайкла из критерия связи чисел Кармайкла с функцией Кармайкла / Ю. Ф. Пастухов, А. Ю. Пастухов, Н. К. Волосова [и др.] // Евразийское Научное Объединение. – 2021. – № 12-1(82). – С. 31-34. – EDN GDLERY.
5. Теорема о связи чисел Кармайкла с функцией Кармайкла / Ю. Ф. Пастухов, Н. К. Волосова, К. А. Волосов [и др.] // Евразийское Научное Объединение. – 2021. – № 6-1(76). – С. 50-53. – EDN HTIQST.
6. Шабуров, А. С. Обнаружение компьютерных атак на основе функционального подхода / А. С. Шабуров, А. А. Миронова // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – № 4(31). – С. 110-115. – EDN VHLGIV.
7. Климов, А. А. Определение авторства произведений изобразительного искусства на основе частотного анализа цветов и энтропии цифровых отпечатков / А. А. Климов, Е. В. Овчинникова, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2016. – № 4(35). – С. 43-52. – DOI 10.17072/1993-0550-2016-4-43-52. – EDN XUXJJZ.
8. Бортников, А. Ю. Семантические фильтры входных данных для системы научной визуализации SciVi / А. Ю. Бортников // Вестник Пермского университета. Математика. Механика. Информатика. – 2016. – № 4(35). – С. 37-42. – DOI 10.17072/1993-0550-2016-4-37-42. – EDN XUXJJP.
9. Бахтин, В. В. Математическая модель поиска коэффициента памяти компьютера, инфицированного вирусом, и собственных параметров компьютерных вирусов в аспекте теории вычислителей с неабсолютной памятью / В. В. Бахтин // Вестник Пермского университета. Математика. Механика. Информатика. – 2017. – № 4(39). – С. 79-85. – DOI 10.17072/1993-0550-2017-4-79-85. – EDN ZXNXKZ.
10. Пермский международный форум "Наука и глобальные вызовы XXI века" / М. М. Бузмакова, Е. Ю. Никитина, А. В. Черников, Л. Н.

Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 5-8. – EDN WUMBNC.
11. Черников, А. В. Одна из возможных реализаций модели менеджера паролей для ОС Андроид / А. В. Черников // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 1(56). – С. 38-47. – DOI 10.17072/1993-0550-2022-1-38-47. – EDN PNSEAY.
12. Чернов, П. К. Создание интегрированной модели данных из разнородных источников, содержащих цифровые следы / П. К. Чернов, Е. А. Рабчевский // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 2(57). – С. 81-87. – DOI 10.17072/1993-0550-2022-2-81-87. – EDN UYUSGT.
13. Разработка специальной классификации информационных активов в сфере информационной безопасности / А. В. Манжосов, И. П. Болодурина, В. С. Сабуров, Н. А. Долгушев // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 54-60. – DOI 10.17072/1993-0550-2022-4-54-60. – EDN ZHZWNB.
14. Нехорошева, Э. А. Построение модели протокола электронного голосования с возможностью проверки результата избирателями / Э. А. Нехорошева, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 61-67. – DOI 10.17072/1993-0550-2022-4-61-67. – EDN QAMNYK.
15. Поторочина, К. Л. Безопасность применения IoT в сфере здравоохранения / К. Л. Поторочина, Е. Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 68-81. – DOI 10.17072/1993-0550-2022-4-68-81. – EDN FBHTIG.
16. Рабчевский, А. Н. Выявление признаков информационных операций на основе анализа начальной частоты публикации дубликатов / А. Н. Рабчевский, М. Ю. Карпов, Е. Г. Ашихмин // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 82-88. – DOI 10.17072/1993-0550-2022-4-82-88. – EDN TYPKBC.
17. Горячев, С. Н. Построение инструментальной модели для исследования системы "Компьютерный вирус-переносчик-автоматизированное рабочее место-локальная вычислительная сеть" / С. Н. Горячев, Н. С. Кобяков, С. Н. Костарев // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 1(52). – С. 53-56. – DOI 10.17072/1993-0550-2021-1-53-56. – EDN MCYXZQ.
18. Импортозамещение в сфере телекоммуникаций и IT-технологий / В. Л. Осипов, И. В. Жигалов, А. С. Лубянков [и др.] // Вестник Пермского

университета. Математика. Механика. Информатика. – 2021. – № 1(52). – С. 70-74. – DOI 10.17072/1993-0550-2021-1-70-74. – EDN ZHKBOL.
19. Чернов, П. К. Модификация алгоритма на основе сети Фейстеля с добавлением элемента случайности в ключ шифрования / П. К. Чернов, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 1(52). – С. 81-88. – DOI 10.17072/1993-0550-2021-1-81-88. – EDN MGBPSA.
20. Половицкий, Я. Д. Пермская алгебраическая школа С.Н. Черникова и ее предшественники / Я. Д. Половицкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 3(54). – С. 68-73. – DOI 10.17072/1993-0550-2021-3-68-73. – EDN PDKKGF.
21. Черников, А. В. Рекомендации по разработке менеджеров паролей для ОС Андроид / А. В. Черников // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 4(55). – С. 49-57. – DOI 10.17072/1993-0550-2021-4-49-57. – EDN HWPILN.
22. Ронзин, В. И. Разработка программного модуля поиска нарушений для интегрированной системы безопасности / В. И. Ронзин, Е. Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. – 2020. – № 1(48). – С. 69-73. – DOI 10.17072/1993-0550-2020-1-69-73. – EDN MSQOTG.
23. Тюрин, С. Ф. Три квантора / С. Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. – 2020. – № 1(48). – С. 87-91. – DOI 10.17072/1993-0550-2020-1-87-91. – EDN MZNRKB.
24. Шимановская, М. В. Многопоточность на платформе.NET. Обзор средств / М. В. Шимановская, И. А. Муфтеев, Е. И. Илларионова // Вестник Пермского университета. Математика. Механика. Информатика. – 2020. – № 2(49). – С. 69-75. – DOI 10.17072/1993-0550-2020-2-69-75. – EDN CLCJAF.
25. Разработка элементов криптопроцессора с использованием отечественной САПР "Ковчег" / О. А. Зобнина, А. Н. Каменских, Г. К. Королев, С. Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. – 2019. – № 2(45). – С. 60-66. – DOI 10.17072/1993-0550-2019-2-60-66. – EDN IYZAXK.
26. Боков, К. А. Компьютерное моделирование перколяции k-меров на квадратной решетке / К. А. Боков, М. М. Бузмакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 1(40). – С. 51-55. – DOI 10.17072/1993-0550-2018-1-51-55. – EDN XMHXWP.

27. Александрова, Е. И. Модификация алгоритмов на основе сети Фейстеля посредством внесения избыточности с помощью кодов Хэмминга / Е. И. Александрова, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 3(42). – С. 95-103. – DOI 10.17072/1993-0550-2018-3-95-103. – EDN VKVNHZ.
28. Разработка программного обеспечения для выявления источников общественноопасной информации в социальной сети " ВКонтакте" / А. А. Березин, Э. Ф. Гайнутдинов, А. С. Максимов, Е. Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 3(42). – С. 104-110. – DOI 10.17072/1993-0550-2018-3-104-110. – EDN VKVNIG.
29. Мустакимова, Я. Р. Создание базы данных и разработка архитектуры системы для выявления участников "групп смерти" / Я. Р. Мустакимова, Е. Ю. Никитина, А. Д. Турпанова // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 3(42). – С. 117-123. – DOI 10.17072/1993-0550-2018-3-117-123. – EDN YMJSYX.
30. Евстафьев, Е. О. Алгоритм динамической обфускации информации с ограничением количества попыток расшифровки, исполнения и просмотра на web-клиенте / Е. О. Евстафьев, С. Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 4(43). – С. 56-59. – DOI 10.17072/1993-0550-2018-4-56-59. – EDN YRJEDJ.
31. 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.
32. 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.
33. 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.
34. Волосов К.А. О собственных функциях структур, описываемых моделью “мелкой воды” на плоскости// Фундаментальная и прикладная математика. 2006. Т. 12.№ 6. С. 17-32.

35. Волосов К.А. Построение решений квазилинейных параболических уравнений в параметрическом виде// Дифференциальные уравнения, 2007, Т.43, №.4., С.492-497.
36. 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.
37. Волосов К.А. Конструкция решений квазилинейных уравнений с частными производными// Сибирский журнал индустриальной математики 2008, т.11, н.2(34), С. 29-39 .
38. Шифрование данных на базе эллиптических кривых: Учебное пособие / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.]. – Москва: Российская открытая академия транспорта федерального государственного бюджетного образовательного учреждения высшего образования "Российский университет транспорта" (МИИТ), 2023. – 52 с. – EDN RPATBZ.
39. Сборник статей по гидродинамике / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.]. – 2-е издание. – Москва: Московский государственный университет путей сообщения Императора Николая II, 2023. – 231 с. – EDN UDVEDI.
40. Алгебраические методы шифрования: Учебное пособие / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.]. – четвёртое издание. – Москва: Российская открытая академия транспорта федерального государственного бюджетного образовательного учреждения высшего образования "Российский университет транспорта" (МИИТ), 2023. – 52 с. – EDN QZKSJC.
41. Пастухов, Ю. Ф. Вычисление наилучшего приближения в метрике квадратичного отклонения ступенчатыми функциями для функции плотности распределения Госсета / Ю. Ф. Пастухов, Д. Ф. Пастухов // Краевые задачи и математическое моделирование: Тематический сборник научных статей / Под общей редакцией Е.А. Вячкиной. – Новокузнецк : Кузбасский гуманитарно-педагогический институт федерального государственного бюджетного образовательного учреждения высшего образования "Кемеровский государственный университет", 2023. – С. 84-86. – EDN NQENGD.
42. Обобщение метода Петрова-Галеркина для решения системы интегральных уравнений Фредгольма второго рода / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.] // Вестник Пермского университета. Математика. Механика. Информатика. – 2023. – № 1(60). – С. 5-14. – DOI 10.17072/1993-0550-2023-1-5-14. – EDN KQEIXG.
43. Пастухов Ю.Ф. Необходимые условия в обратной вариационной задаче// Фундаментальная и прикладная математика,7:1(2001), 285-288.
44. Сравнение методов прогонки столбцов и строк неизвестной матрицы для решения уравнения Пуассона в переменных функция тока-вихрь в

гидродинамической задаче для закрытой прямоугольной каверны / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.] // Тенденции развития науки и образования. – 2022. – № 87-2. – С. 48-56. – DOI 10.18411/trnio-07-2022-48. – EDN AOYFJY.

45. Моделирование систем. Лекции. Лабораторный практикум / Д. Ф. Пастухов, Ю. Ф. Пастухов, Н. К. Волосова [и др.]. – 3-е дополненное. – Новополоцк : Учреждение образования «Полоцкий государственный университет имени Евфросинии Полоцкой», 2022. – 142 с. – EDN PYJINB.
46. Численные методы. Лекции. Численный практикум / Д. Ф. Пастухов, Ю. Ф. Пастухов, Н. К. Волосова [и др.]. – 3-е издание, дополненное. – Новополоцк. Москва : Учреждение образования «Полоцкий государственный университет», 2021. – 237 с. – EDN CLJJLX.
47. 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.

48. 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.

49. Этап конструирования математической модели аневризмы. Течения в каверне и противоречия в задаче в "закрытой“ кювете / Н. К. Волосова, М. А. Басараб, А. К. Волосова [и др.] // Некоторые Актуальные проблемы современной математикии математического образования : Материалы 74-й научной КОНФЕРЕНЦИИ«ГЕРЦЕНОВСКИЕ ЧТЕНИЯ 2021», Санкт-Петербург, 05–10 апреля 2021 года / Российская Академия Образования; Академия информатизации образования; Российский государственный педагогический университет им. А. И. Герцена, Кафедра математического анализа, Кафедра компьютерной инженерии и программотехники. – Санкт-Петербург: ООО "Издательство ВВМ", 2021. – С. 208-213. – EDN HREUQK.

Числа Кармайкла до 100000000. Программа поиска чисел Кармайкла.

Согласно алгоритмам Теорем 1 и 14 написана программа для поска чисел Кармайкла. Оригинальный код программы написан на языке Visual Fortran , интерфейс программы позволяет находить числа Кармайкла в заданном диапазоне целых чисел, как показано на рисунках 4. Это связано с тем, что при больших значений чисел требуется значительно больше времени, чем при малых значениях. Например, в диапазоне от 1 до 100000 программе требуется всего 4 секуды для отскания всех чисел Кармайкла (Рис.2). В то время как в диапазоне от 80 ло 100 миллионов программа затрачивает 1,63 часа (Рис.4). Поэтому для поиска чисел Кармайкла за конечное время с большими значениями приходится сужать исследуемый диапазон.

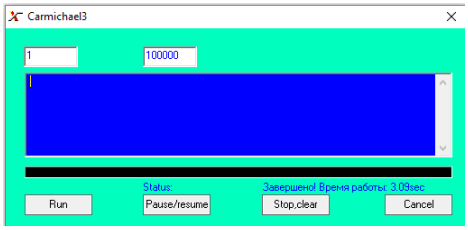

Рис.1. Интерфейс программы для поиска чисел Кармайкла не превышающих 10000(исходное состояние)

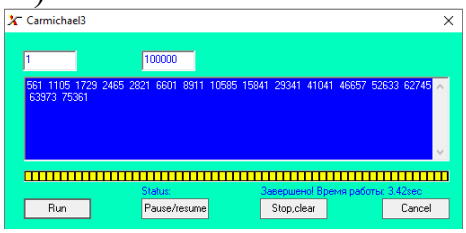

Рис.2. Числа Кармайкла не превышающие 100000(после запуска программы кнопкой run).

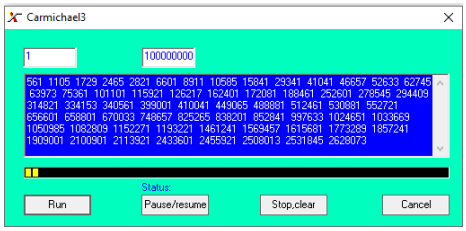

Рис.3. Числа Кармайкла не превышающие 100000000.

Таблица 1. Множество чисел Кармайкла не превышающих 100000000.

К= {561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 334153, 340561, 399001, 410041, 449065, 488881, 512461, 530881, 552721, 656601, 658801, 670033, 748657, 825265, 838201, 852841, 997633, 1024651, 1033669, 1050985, 1082809, 1152271, 1193221, 1461241, 1569457, 1615681, 1773289, 1857241, 1909001, 2100901, 2113921, 2433601, 2455921, 2508013, 2531845, 2628073, 2704801, 3057601, 3146221, 3224065, 3581761, 3664585, 3828001, 4335241,

4463641, 4767841, 4903921, 4909177, 5031181, 5049001, 5148001, 5310721, 5444489, 5481451, 5632705, 5968873, 6049681, 6054985, 6189121, 6313681, 6733693, 6840001, 6868261, 7207201, 7519441, 7995169, 8134561, 8341201, 8355841, 8719309, 8719921, 8830801, 8927101, 9439201, 9494101, 9582145, 9585541, 9613297, 9890881, 10024561, 10267951, 10402561, 10606681, 10837321, 10877581, 11119105, 11205601, 11921001, 11972017, 12261061, 12262321, 12490201, 12945745, 13187665, 13696033, 13992265, 14469841, 14676481, 14913991, 15247621, 15403285, 15829633, 15888313, 16046641, 16778881, 17098369, 17236801, 17316001, 17586361, 17812081, 18162001, 18307381, 18900973, 19384289, 19683001, 20964961, 21584305, 22665505, 23382529, 25603201, 26280073, 26474581, 26719701, 26921089, 26932081, 27062101, 27336673, 27402481, 28787185, 29020321, 29111881, 31146661, 31405501, 31692805, 32914441, 33302401, 33596641, 34196401, 34657141, 34901461, 35571601, 35703361, 36121345, 36765901, 37167361, 37280881, 37354465, 37964809, 38151361, 39353665, 40160737, 40430401, 40622401, 40917241, 41298985, 41341321, 41471521, 42490801, 43286881, 43331401, 43584481, 43620409, 44238481, 45318561, 45877861, 45890209, 6483633, 47006785, 48321001, 48628801, 49333201, 50201089, 53245921, 53711113, 54767881, 55462177, 56052361, 58489201, 60112885, 60957361, 62756641, 64377991, 64774081, 65037817, 65241793, 67371265, 67653433, 67902031, 67994641, 68154001, 69331969, 70561921, 72108421, 72286501, 74165065, 75151441, 75681541, 75765313, 76595761 77826001, 78091201, 7812000, 7941120, 79624621, 80282161, 80927821, 81638401, 81926461, 82929001, 83099521, 83966401, 84311569, 84350561, 84417985, 87318001, 88689601, 90698401, 92625121, 93030145, 93614521, 93614521, 93869665, 94536001, 96895441, 99036001, 99830641, 99861985}.

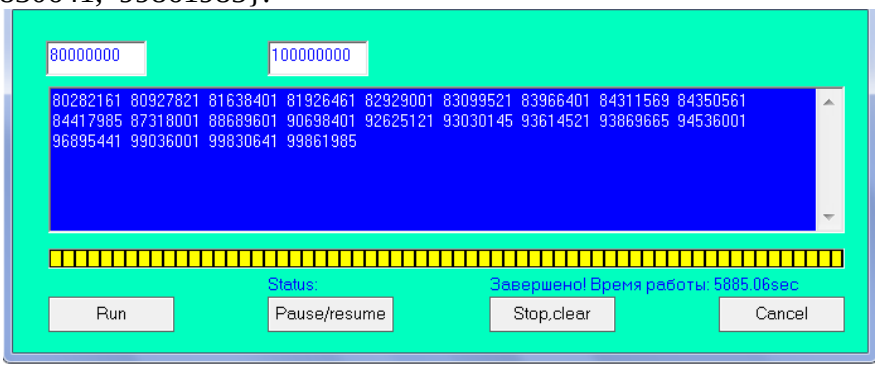

Рис.4. Числа Кармайкла от 80000000 до 100000000. Время работы программы 1,63 часа.

В таблицу 1 программой записаны все числа Кармайкла в диапазоне от 1 до 100 миллионов.

Код программы и графический интерфейс принадлежат Пастухову Юрию Феликсовичу.

Литература (общий список):

1. Лидовский В.В. Теория информации: Учебное пособие. – М.: Компания Спутник +,2004. – 111 с. –ISSN 5-93406-661-7.
2. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. — Казань: КФУ, 2011. — 190 с.
3. 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.
4. Вывод критерия Корсельта чисел Кармайкла из критерия связи чисел Кармайкла с функцией Кармайкла / Ю. Ф. Пастухов, А. Ю. Пастухов, Н. К. Волосова [и др.] // Евразийское Научное Объединение. – 2021. – № 12-1(82). – С. 31-34. – EDN GDLERY.
5. Теорема о связи чисел Кармайкла с функцией Кармайкла / Ю. Ф. Пастухов, Н. К. Волосова, К. А. Волосов [и др.] // Евразийское Научное Объединение. – 2021. – № 6-1(76). – С. 50-53. – EDN HTIQST.
6. 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.
7. 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.
8. Мурашов, Д. И. Социальный генетический алгоритм / Д. И. Мурашов, Л. Н. Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2006. – № 4(4). – С. 53-60. – EDN YMWFVB.
9. Гладкий, С. Л. Верификация численных расчетов методом фиктивных канонических областей / С. Л. Гладкий, Н. Ф. Таланцев, Л. Н. Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2006. – № 4(4). – С. 18-27. – EDN YMWFVJ.
10. Филиппов, Н. А. Математический путь к лучшей количественной информационной технике / Н. А. Филиппов // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 71-83. – EDN MNIHZT.
11. Плаксин, М. А. Механизмы сокращения нагрузки на эксперта при применении метода анализа иерархий / М. А. Плаксин // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 64-70. – EDN MNIHZJ.
12. Городилов, А. Ю. Криптоанализ перестановочного шифра с помощью генетического алгоритма / А. Ю. Городилов // Вестник Пермского

университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 44-49. – EDN MNIHYF.
13. Остапенко, Е. Н. Профессор Владимир Владимирович Маланин / Е. Н. Остапенко // Вестник Пермского университета. Математика. Механика. Информатика. – 2007. – № 7(12). – С. 222-226. – EDN MNIIHL.
14. Айдаров, Ю. Р. Новый алгоритм анализа протоколов информационной безопасности и оценка его вычислительной сложности / Ю. Р. Айдаров // Вестник Пермского университета. Математика. Механика. Информатика. – 2008. – № 4(20). – С. 165-168. – EDN MNLKGR.
15. Фирсов, А. Н. Оценка эффективности некоторых оптимизаций протоколов надежной и атомарной групповой рассылки / А. Н. Фирсов // Вестник Пермского университета. Математика. Механика. Информатика. – 2009. – № 3(29). – С. 161-168. – EDN KHNUXV.
16. Малых, А. Е. Андрей Николаевич Колмогоров / А. Е. Малых, В. И. Данилова // Вестник Пермского университета. Математика. Механика. Информатика. – 2009. – № 3(29). – С. 216-224. – EDN KHNVAN.
17. Данилова, Е. Ю. Сравнение генетических алгоритмов на примере задачи коммивояжера / Е. Ю. Данилова, А. Ю. Городилов // Вестник Пермского университета. Математика. Механика. Информатика. – 2009. – № 3(29). – С. 49-53. – EDN KHNUQN.
18. Пенский, О. Г. Профессор Леонид Нахимович Ясницкий / О. Г. Пенский // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 1(1). – С. 6-8. – EDN LGKJNP.
19. Морозенко, В. В. Генетический алгоритм для криптоанализа шифра Виженера / В. В. Морозенко, Г. О. Елисеев // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 1(1). – С. 75-80. – EDN LGKJRL.
20. Тарунин, Е. Л. Возможности вычислительных методов в проблемах теории чисел / Е. Л. Тарунин // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 2(2). – С. 15-28. – EDN MNLKJT.
21. Малых, А. Е. Об историческом процессе развития теории латинских квадратов и некоторых их приложениях / А. Е. Малых, В. И. Данилова // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 4(4). – С. 95-104. – EDN NDXQYZ.
22. Черномордик, И. В. Об одном алгоритме восстановления в задаче распознавания изображения / И. В. Черномордик // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 4(4). – С. 50-53. – EDN NDXQVX.
23. Тарунин, Е. Л. Уточнения формул распределения простых чисел / Е. Л. Тарунин // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 1(5). – С. 10-19. – EDN NTUHTV.
24. Ермакова, Л. М. Методы классификации текстов и определения качества контента / Л. М. Ермакова // Вестник Пермского

университета. Математика. Механика. Информатика. – 2011. – № 3(7). – С. 47-53. – EDN OIVSGR.
25. Толюпа, Е. А. Доверенная цифровая подпись на базе алгоритма ЭЦП ГОСТ Р 34.10-94 / Е. А. Толюпа // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 3(7). – С. 63-66. – EDN OIVSHV.
26. Городилов, А. Ю. Криптоанализ тригонометрического шифра с помощью генетического алгоритма / А. Ю. Городилов, А. А. Митраков // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 4(8). – С. 75-82. – EDN PDBIQB.
27. Замятина, Е. Б. Построение синтаксически и семантически правильной Queue Network-модели в Triad.Net / Е. Б. Замятина, А. В. Шафранов // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 4(8). – С. 83-91. – EDN PDBIQL.
28. Полищук, В. И. Подход к созданию автоматизированной информационно-аналитической системы мониторинга безопасности г. Перми / В. И. Полищук // Вестник Пермского университета. Математика. Механика. Информатика. – 2010. – № 4(4). – С. 75-79. – EDN NDXQXV.
29. Ермакова, Л. М. Методы обнаружения писем-трансформеров / Л. М. Ермакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 2(6). – С. 77-85. – EDN OIVSCL.
30. Ермакова, Л. М. Методы извлечения информации из текста / Л. М. Ермакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2012. – № 1(9). – С. 77-84. – EDN PCVJRF.
31. Макеев, Н. Н. Выдающееся открытие XIX века (к 200-летию со дня рождения Эвариста Галуа) / Н. Н. Макеев // Вестник Пермского университета. Математика. Механика. Информатика. – 2012. – № 2(10). – С. 68-75. – EDN PCRVKT.
32. Чуприна, С. И. Разработка подхода к индексации смыслового содержания графической информации на принципах онтологического инжиниринга / С. И. Чуприна, В. А. Никифоров // Вестник Пермского университета. Математика. Механика. Информатика. – 2013. – № 3(22). – С. 111-118. – EDN RPSSZV.
33. Шафер, А. Е. Двухфакторная аутентификация с использованием СМС-сервиса / А. Е. Шафер, А. В. Черников // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – № 1(28). – С. 79-85. – EDN UHSZBX.
34. Тюрин, С. Ф. Восстановитель информации в двухканальной самосинхронной схеме / С. Ф. Тюрин, А. Н. Каменских // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – № 4(31). – С. 105-109. – EDN VHLGIL.
35. Шабуров, А. С. Обнаружение компьютерных атак на основе функционального подхода / А. С. Шабуров, А. А. Миронова // Вестник

Пермского университета. Математика. Механика. Информатика. – 2015. – № 4(31). – С. 110-115. – EDN VHLGIV.
36. Климов, А. А. Определение авторства произведений изобразительного искусства на основе частотного анализа цветов и энтропии цифровых отпечатков / А. А. Климов, Е. В. Овчинникова, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2016. – № 4(35). – С. 43-52. – DOI 10.17072/1993-0550-2016-4-43-52. – EDN XUXJJZ.
37. Бортников, А. Ю. Семантические фильтры входных данных для системы научной визуализации SciVi / А. Ю. Бортников // Вестник Пермского университета. Математика. Механика. Информатика. – 2016. – № 4(35). – С. 37-42. – DOI 10.17072/1993-0550-2016-4-37-42. – EDN XUXJJP.
38. Бахтин, В. В. Математическая модель поиска коэффициента памяти компьютера, инфицированного вирусом, и собственных параметров компьютерных вирусов в аспекте теории вычислителей с неабсолютной памятью / В. В. Бахтин // Вестник Пермского университета. Математика. Механика. Информатика. – 2017. – № 4(39). – С. 79-85. – DOI 10.17072/1993-0550-2017-4-79-85. – EDN ZXNXKZ.
39. Пермский международный форум "Наука и глобальные вызовы XXI века" / М. М. Бузмакова, Е. Ю. Никитина, А. В. Черников, Л. Н. Ясницкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 5-8. – EDN WUMBNC.
40. Черников, А. В. Одна из возможных реализаций модели менеджера паролей для ОС Андроид / А. В. Черников // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 1(56). – С. 38-47. – DOI 10.17072/1993-0550-2022-1-38-47. – EDN PNSEAY.
41. Чернов, П. К. Создание интегрированной модели данных из разнородных источников, содержащих цифровые следы / П. К. Чернов, Е. А. Рабчевский // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 2(57). – С. 81-87. – DOI 10.17072/1993-0550-2022-2-81-87. – EDN UYUSGT.
42. Разработка специальной классификации информационных активов в сфере информационной безопасности / А. В. Манжосов, И. П. Болодурина, В. С. Сабуров, Н. А. Долгушев // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 54-60. – DOI 10.17072/1993-0550-2022-4-54-60. – EDN ZHZWNB.
43. Нехорошева, Э. А. Построение модели протокола электронного голосования с возможностью проверки результата избирателями / Э. А. Нехорошева, А. П. Шкарапута // Вестник Пермского университета.

Математика. Механика. Информатика. – 2022. – № 4(59). – С. 61-67. – DOI 10.17072/1993-0550-2022-4-61-67. – EDN QAMNYK.
44. Поторочина, К. Л. Безопасность применения IoT в сфере здравоохранения / К. Л. Поторочина, Е. Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 68-81. – DOI 10.17072/1993-0550-2022-4-68-81. – EDN FBHTIG.
45. Рабчевский, А. Н. Выявление признаков информационных операций на основе анализа начальной частоты публикации дубликатов / А. Н. Рабчевский, М. Ю. Карпов, Е. Г. Ашихмин // Вестник Пермского университета. Математика. Механика. Информатика. – 2022. – № 4(59). – С. 82-88. – DOI 10.17072/1993-0550-2022-4-82-88. – EDN TYPKBC.
46. Горячев, С. Н. Построение инструментальной модели для исследования системы "Компьютерный вирус-переносчик-автоматизированное рабочее место-локальная вычислительная сеть" / С. Н. Горячев, Н. С. Кобяков, С. Н. Костарев // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 1(52). – С. 53-56. – DOI 10.17072/1993-0550-2021-1-53-56. – EDN MCYXZQ.
47. Импортозамещение в сфере телекоммуникаций и IT-технологий / В. Л. Осипов, И. В. Жигалов, А. С. Лубянков [и др.] // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 1(52). – С. 70-74. – DOI 10.17072/1993-0550-2021-1-70-74. – EDN ZHKBOL.
48. Чернов, П. К. Модификация алгоритма на основе сети Фейстеля с добавлением элемента случайности в ключ шифрования / П. К. Чернов, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 1(52). – С. 81-88. – DOI 10.17072/1993-0550-2021-1-81-88. – EDN MGBPSA.
49. Половицкий, Я. Д. Пермская алгебраическая школа С.Н. Черникова и ее предшественники / Я. Д. Половицкий // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 3(54). – С. 68-73. – DOI 10.17072/1993-0550-2021-3-68-73. – EDN PDKKGF.
50. Черников, А. В. Рекомендации по разработке менеджеров паролей для ОС Андроид / А. В. Черников // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 4(55). – С. 49-57. – DOI 10.17072/1993-0550-2021-4-49-57. – EDN HWPILN.
51. Ронзин, В. И. Разработка программного модуля поиска нарушений для интегрированной системы безопасности / В. И. Ронзин, Е. Ю. Никитина // Вестник Пермского университета. Математика. Механика.

Информатика. – 2020. – № 1(48). – С. 69-73. – DOI 10.17072/1993-0550-2020-1-69-73. – EDN MSQOTG.
52. Тюрин, С. Ф. Три квантора / С. Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. – 2020. – № 1(48). – С. 87-91. – DOI 10.17072/1993-0550-2020-1-87-91. – EDN MZNRKB.
53. Шимановская, М. В. Многопоточность на платформе.NET. Обзор средств / М. В. Шимановская, И. А. Муфтеев, Е. И. Илларионова // Вестник Пермского университета. Математика. Механика. Информатика. – 2020. – № 2(49). – С. 69-75. – DOI 10.17072/1993-0550-2020-2-69-75. – EDN CLCJAF.
54. Разработка элементов криптопроцессора с использованием отечественной САПР "Ковчег" / О. А. Зобнина, А. Н. Каменских, Г. К. Королев, С. Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. – 2019. – № 2(45). – С. 60-66. – DOI 10.17072/1993-0550-2019-2-60-66. – EDN IYZAXK.
55. Боков, К. А. Компьютерное моделирование перколяции k-меров на квадратной решетке / К. А. Боков, М. М. Бузмакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 1(40). – С. 51-55. – DOI 10.17072/1993-0550-2018-1-51-55. – EDN XMHXWP.
56. Александрова, Е. И. Модификация алгоритмов на основе сети Фейстеля посредством внесения избыточности с помощью кодов Хэмминга / Е. И. Александрова, А. П. Шкарапута // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 3(42). – С. 95-103. – DOI 10.17072/1993-0550-2018-3-95-103. – EDN VKVNHZ.
57. Разработка программного обеспечения для выявления источников общественноопасной информации в социальной сети " ВКонтакте" / А. А. Березин, Э. Ф. Гайнутдинов, А. С. Максимов, Е. Ю. Никитина // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 3(42). – С. 104-110. – DOI 10.17072/1993-0550-2018-3-104-110. – EDN VKVNIG.
58. Мустакимова, Я. Р. Создание базы данных и разработка архитектуры системы для выявления участников "групп смерти" / Я. Р. Мустакимова, Е. Ю. Никитина, А. Д. Турпанова // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 3(42). – С. 117-123. – DOI 10.17072/1993-0550-2018-3-117-123. – EDN YMJSYX.

59. Евстафьев, Е. О. Алгоритм динамической обфускации информации с ограничением количества попыток расшифровки, исполнения и просмотра на web-клиенте / Е. О. Евстафьев, С. Ф. Тюрин // Вестник Пермского университета. Математика. Механика. Информатика. – 2018. – № 4(43). – С. 56-59. – DOI 10.17072/1993-0550-2018-4-56-59. – EDN YRJEDJ.
60. 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.
61. 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.
62. 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.
63. Волосов К.А. О собственных функциях структур, описываемых моделью “мелкой воды” на плоскости// Фундаментальная и прикладная математика. 2006. Т. 12.№ 6. С. 17-32.
64. Волосов К.А. Построение решений квазилинейных параболических уравнений в параметрическом виде// Дифференциальные уравнения, 2007, Т.43, №.4., С.492-497.
65. 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.
66. Волосов К.А. Конструкция решений квазилинейных уравнений с частными производными// Сибирский журнал индустриальной математики 2008, т.11, н.2(34), С. 29-39 .
67. Шифрование данных на базе эллиптических кривых : Учебное пособие / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.]. – Москва : Российская открытая академия транспорта федерального государственного бюджетного образовательного учреждения высшего образования "Российский университет транспорта" (МИИТ), 2023. – 52 с. – EDN RPATBZ.
68. Сборник статей по гидродинамике / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.]. – 2-е издание. – Москва : Московский государственный университет путей сообщения Императора Николая II, 2023. – 231 с. – EDN UDVEDI.
69. Алгебраические методы шифрования : Учебное пособие / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.]. – четвёртое издание. –

Москва : Российская открытая академия транспорта федерального государственного бюджетного образовательного учреждения высшего образования "Российский университет транспорта" (МИИТ), 2023. – 52 с. – EDN QZKSJC.
70. Пастухов, Ю. Ф. Вычисление наилучшего приближения в метрике квадратичного отклонения ступенчатыми функциями для функции плотности распределения Госсета / Ю. Ф. Пастухов, Д. Ф. Пастухов // Краевые задачи и математическое моделирование : Тематический сборник научных статей / Под общей редакцией Е.А. Вячкиной. – Новокузнецк : Кузбасский гуманитарно-педагогический институт федерального государственного бюджетного образовательного учреждения высшего образования "Кемеровский государственный университет", 2023. – С. 84-86. – EDN NQENGD.
71. Обобщение метода Петрова-Галеркина для решения системы интегральных уравнений Фредгольма второго рода / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.] // Вестник Пермского университета. Математика. Механика. Информатика. – 2023. – № 1(60). – С. 5-14. – DOI 10.17072/1993-0550-2023-1-5-14. – EDN KQEIXG.
72. Пастухов Ю.Ф. Необходимые условия в обратной вариационной задаче// Фундаментальная и прикладная математика,7:1(2001), 285-288.
73. Сравнение методов прогонки столбцов и строк неизвестной матрицы для решения уравнения Пуассона в переменных функция тока-вихрь в гидродинамической задаче для закрытой прямоугольной каверны / Н. К. Волосова, К. А. Волосов, А. К. Волосова [и др.] // Тенденции развития науки и образования. – 2022. – № 87-2. – С. 48-56. – DOI 10.18411/trnio-07-2022-48. – EDN AOYFJY.
74. Моделирование систем. Лекции. Лабораторный практикум / Д. Ф. Пастухов, Ю. Ф. Пастухов, Н. К. Волосова [и др.]. – 3-е дополненное. – Новополоцк : Учреждение образования «Полоцкий государственный университет имени Евфросинии Полоцкой», 2022. – 142 с. – EDN PYJINB.
75. Численные методы. Лекции. Численный практикум / Д. Ф. Пастухов, Ю. Ф. Пастухов, Н. К. Волосова [и др.]. – 3-е издание, дополненное. – Новополоцк. Москва : Учреждение образования «Полоцкий государственный университет», 2021. – 237 с. – EDN CLJJLX.
76. 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.
77. 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.

78. Этап конструирования математической модели аневризмы. Течения в каверне и противоречия в задаче в "закрытой“ кювете / Н. К. Волосова, М. А. Басараб, А. К. Волосова [и др.] // Некоторые Актуальные проблемы современной математикии математического образования : Материалы 74-й научной КОНФЕРЕНЦИИ«ГЕРЦЕНОВСКИЕ ЧТЕНИЯ 2021», Санкт-Петербург, 05–10 апреля 2021 года / Российская Академия Образования; Академия информатизации образования; Российский государственный педагогический университет им. А. И. Герцена, Кафедра математического анализа, Кафедра компьютерной инженерии и программотехники. – Санкт-Петербург: ООО "Издательство ВВМ", 2021. – С. 208-213. – EDN HREUQK.

НЕСКОЛЬКО ТЕОРЕМ О ЧИСЛАХ КАРМАЙКЛА

Пастухов Юрий Феликсович

Волосова Наталья Константиновна

Волосов Константин Александрович

Волосова Александра Константиновна

Пастухов Дмитрий Феликсович

Москва 2023