ISBN 978-5-901722-87-9

УДК 621.398

ГЕНЕРАЦИЯ ПОСЛЕДОВАТЕЛЬНОСТИ РЯДОВ ФАРЕЯ НА ОСНОВЕ МЕТОДА СРАВНЕНИЯ ДЛЯ ПОСТРОЕНИЯ КАНАЛА ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ ОБЪЕКТАМИ

Кораблев Егор Денисович[1], заведующий лабораторией, ассистент кафедры Систем информационной безопасности управления и коммуникаций
e-mail: graravar@gmail.com
Крит Андрей Александрович[1], заведующий лабораторией, ассистент кафедры Систем информационной безопасности управления и коммуникаций
e-mail: qgc89092850880@gmail.com
Федосенко Юрий Семёнович[1], доктор технических наук, профессор, заведующий кафедрой Систем информационной безопасности управления и коммуникаций
e-mail: fds1707@mail.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия

Аннотация. Рассмотрен метод генерации рядов Фарея на основе расчета сравнения для соседних дробей. Данный метод отличается высокой скоростью работы по сравнению с методом медиантой, однако не позволяет рассчитать заданный набор рядов за один запуск цикла, в отличие от алгоритма медианты, что препятствует решению узконаправленных задач. Рассматриваемый алгоритм может применяться для получения ряда большого порядка для решения конкретных задач, как например решение диофантовых уравнений или решение задачи поиска пораженных частот, или оценки криптостойкости алгоритмов на основе RSA.

Ключевые слова: криптография, пораженные частоты, ряды Фарей, сравнения, теория чисел, медианта, цепные дроби, математика, алгоритмизация, оптимизация, диофантовы уравнения, RSA.

FAREY SERIES SEQUENCE GENERATION BASED ON THE MEDIANT METHOD FOR APPLICATION IN UNMANNED CONTROL OF MOBILE OBJECTS

Korablev Egor Denisovich[1], Head of the Laboratory, Assistant of the Department of Information Security Management and Communications Systems
e-mail: graravar@gmail.com
Krit Andrei Aleksandrovich[1], Head of the Laboratory, Assistant of the Department of Information Security Management and Communications Systems
e-mail: qgc89092850880@gmail.com
Fedosenko Iurii Semenovich[1], Doctor of Mathematical Sciences, Professor, Head of the Department of Information Security Management and Communications Systems
e-mail: fds1707@mail.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia

Abstract. The method of Farey sequence generation based on the calculation of median for neighbouring fractions is considered. This method is not characterised by high speed of work in comparison with the method of comparison solution, but it allows to calculate a given set of series in one run of the cycle, unlike the algorithm of comparison solution, which greatly compensates for the low speed of work. The considered algorithm can be used to obtain a large amount of data for different range of problems, such as solving Diophantine equations, or solving the problem of searching for affected frequencies, or evaluating the cryptographic stability of RSA-based algorithms.

Keywords: cryptography, affected frequencies, Farey sequences, comparisons, number theory, median, chain fractions, mathematics, algorithmisation, optimisation, Diophantine equations, RSA.

Введение

Ряды Фарея представляют собой последовательности рациональных чисел, которые охватывают все положительные рациональные числа в интервале от 0 до 1. Они получаются путем вычисления и упорядочивания всех дробей с заданным ограничением на числитель и знаменатель.

Метод сравнения основан на использовании предыдущего элемента ряда для расчета последующего элемента ряда.

Данная методика позволяет получить заданный ряд Фарея при определенном коэффициенте, представляемого литерой «n», то есть ряд обозначается как «Φ_n».

Данный ряд может применяться для моделирования номограммы пораженных частот приемного устройства, что в свою очередь позволит спроектировать качественный фильтр промежуточной частоты (ФПЧ) для радиоприемного тракта. Благодаря свойству рядов Фарея к приближению действительных чисел, появляется возможность промоделировать распределение комбинационных частот с высокой (заданной) точностью. Данная возможность увеличивает вероятность доставки телеметрического (или иного) сообщения для дистанционного управления подвижным объектом, за счет уменьшения появляющихся в смесителе помех (комбинационных частот).

Ряд Фарея

Приближения действительных чисел рациональными, в основном изучалось с помощью аппарата цепных дробей. Эти приближения исследуются также с помощью, так называемых последовательностей Фарея, имеющих большое значение и при рассмотрении других вопросов теории чисел [1]. Введем определение фареевых дробей. Последовательностью Фарея «Φ_n» называют множество несократимых рациональных чисел a/b со знаменателем $b \leq n$, принадлежащих сегменту [0; 1] и расположенных в порядке их возрастания. Фареевы последовательности названы по имени английского ученого Дж. Фарея, опубликовавшего в 1816 году некоторые свойства этих последовательностей [1].

Рассмотрим один из алгоритмов генерации подобного ряда. Данный алгоритм является решением сравнения первой степени по модулю с одним неизвестным вида $yx \equiv -1 \bmod (z)$. Существует несколько методов решения сравнения данного вида, мы обратимся к методу прямого перебора.

Разберем на примере. Существует элемент ряда 3/7. Необходимо в ряде десятого порядка Φ_{10} следующую за ней. Для чего необходимо решить сравнение $yy_0 \equiv -1 \bmod (z)$. Подставим коэффициенты: y = 3, z = 7. Получаем тождественное уравнение: $3y_0 \equiv -1 \bmod (7)$. Для его решения воспользуемся вышеуказанным методом прямого перебора. Начинаем к коэффициенту -1 прибавлять подмодульное значение z до тех пор, пока коэффициент не будет кратен значению коэффициента y. При первой же итерации получаем уравнение вида:

$3y_0 \equiv (-1+7) \bmod (7) \Rightarrow 3y_0 \equiv 6 \bmod (7) \Rightarrow y_0 \equiv 2 \bmod (7)$. Затем, как следует из теоремы 253 [1], для нахождения знаменателя рассчитываемой дроби y_0, необходимо к полученному коэффициенту 2 прибавить подмодульное значение 7 до тех пор, пока следующая итерация сложения не превысит порядок ряда. Как только оно превысит, следует взять предыдущее значение коэффициента. Продолжим пример: $y_0 \equiv (2+7) \bmod (7) \Rightarrow y_0 \equiv 9 \bmod (7)$. Если прибавим еще раз, то 9 + 7 = 16, что превышает порядок ряда равный 10. Тем самым, получаем, что знаменатель $y_0 = 9$. Согласно теореме 253 [1], формула для расчета числителя выглядит следующим образом:

$$x_0 = \frac{y * y_0 + 1}{b},$$

где y – числитель предыдущего элемента;

y_0 – знаменатель нового элемента;

b – знаменатель предыдущего элемента.

Приведем выведенный полный алгоритм расчета:

$$\begin{cases} z = b - 1 \\ x \equiv \left(\frac{(\sum_{i=1}^{N} z_i) + z}{a}\right) mod\ b; N = z\ mod\ a; z_{i+1} = z + b \\ y_0 = x + \sum_{y_0 \le n} b \\ x_0 = \frac{a * y_0 + 1}{b} \end{cases}$$

Итак, при подстановке коэффициентов, x_0 будет равен 4. Тем самым следующим элементом в ряде Φ_{10} является 4/9.

За счет того, что происходит быстрая генерация одного конкретного ряда, можно аппроксимировать позиции комбинационных помех как можно более точно за короткий срок. Отношение скорости генерации набора рядов методом медианты к методу решения сравнений стремится к 8%, что означает, что процесс генерации набора рядов методом медианты на 92% быстрее, чем методом решения сравнения. Однако, когда идет речь о задаче аппроксимации по одному ряду, то метод решения сравнения работает быстрее, чем метод медианты. Благодаря этому, можно быстро сгенерировать один конкретный ряд, и в последующем вычислить приближенный набор комбинационных частот (для повышения помехозащищенности).

Был написан алгоритм на языке Visual Basic .NET, позволяющий рассчитать ряд Фарея любого заданного порядка на основании вышеизложенной методики. На рисунке 1 приведен интерфейс разработанного ПО для ряда с порядком 10.

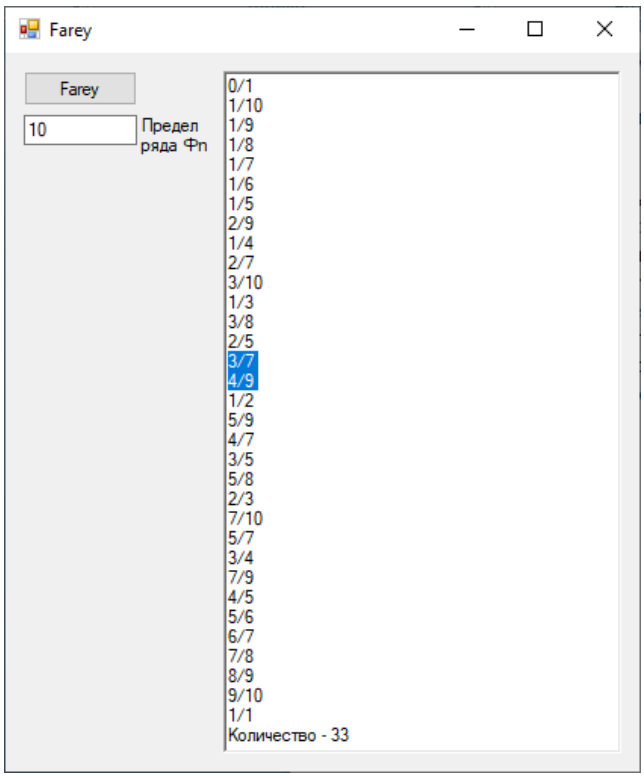

Рисунок 1 – Интерфейс ПО

На рисунке 1, в текстовом поле справа выделена пара приведенных в примере элементов.

Приведем ниже, в таблице 1, примеры рассчитанных рядов:

Таблица 1

Примеры рассчитанных рядов Фарея

Номер ряда	Определение ряда	Ряд
1	$Ф_1$	0/1, 1/1
5	$Ф_{10}$	0/1, 1/10, 1/9, 1/8, 1/7, 1/6, 1/5, 2/9, 1/4, 2/7, 3/10, 1/3, 3/8, 2/5, 3/7, 4/9, 1/2, 5/9, 4/7, 3/5, 5/8, 2/3, 7/10, 5/7, 3/4, 7/9, 4/5, 5/6, 6/7, 7/8, 8/9, 9/10, 1/1
6	$Ф_{20}$	0/1, 1/20, 1/19, 1/18, 1/17, 1/16, 1/15, 1/14, 1/13, 1/12, 1/11, 1/10, 2/19, 1/9, 2/17, 1/8, 2/15, 1/7, 3/20, 2/13, 3/19, 1/6, 3/17, 2/11, 3/16, 1/5, 4/19, 3/14, 2/9, 3/13, 4/17, 1/4, 5/19, 4/15, 3/11, 5/18, 2/7, 5/17, 3/10, 4/13, 5/16, 6/19, 1/3, 7/20, 6/17, 5/14, 4/11, 7/19, 3/8, 5/13, 7/18, 2/5, 7/17, 5/12, 8/19, 3/7, 7/16, 4/9, 9/20, 5/11, 6/13, 7/15, 8/17, 9/19, 1/2, 10/19, 9/17, 8/15, 7/13, 6/11, 11/20, 5/9, 9/16, 4/7, 11/19, 7/12, 10/17, 3/5, 11/18, 8/13, 5/8, 12/19, 7/11, 9/14, 11/17, 13/20, 2/3, 13/19, 11/16, 9/13, 7/10, 12/17, 5/7, 13/18, 8/11, 11/15, 14/19, 3/4, 13/17, 10/13, 7/9, 11/14, 15/19, 4/5, 13/16, 9/11, 14/17, 5/6, 16/19, 11/13, 17/20, 6/7, 13/15, 7/8, 15/17, 8/9, 17/19, 9/10, 10/11, 11/12, 12/13, 13/14, 14/15, 15/16, 16/17, 17/18, 18/19, 19/20, 1/1

Как видно, количество элементов растет нелинейно, для первого рада это количество равно двум, для второго – 3, для третьего – 5, для четвертого – 7, для пятого – 11, для десятого – 33. Из этого можно сделать вывод, что в случае, когда будет необходимо воссоздать ряд большого порядка, потребуется большая вычислительная мощность. Приведем в таблице 2 количество элементов для рядов от 1 до 20 порядка.

Таблица 2

Зависимость количества членов ряда Фарея от номера ряда Фарея

№	Количество
1	2
10	33
20	129
25	201
50	775
75	1737
100	3045
125	4797
150	6859
175	9371
200	12233
225	15429
250	19025
275	23083
300	27399

Вывод

В данной статье был рассмотрен метод генерации набора последовательностей Фарея, воссоздаваемый с помощью алгоритма решения сравнений. Данный алгоритм позволяет в ограниченное время сгенерировать ряд заданного порядка. Что в свою очередь позволяет давать оценку сверхбольшим рядам Фарея (более 2^{128}) как для дальнейшей оценки криптостойкости алгоритмов на основе RSA [2], так и для расчёта пораженных частот приёмного радиотракта, что в свою очередь позволит проектировать высококачественные ФПЧ.

Список литературы:

1. Бухштаб, А.А. Теория чисел [Текст] / А.А. Бухштаб – Москва : издательство «Просвещение», 1966. – 384 с.

2. Новичков, М.Д. Применение недвоичных систем счисления для организации высокоточных вычислений [Текст] /М.Д. Новичков, Д.А. Орлов// Вестник Воронежского государственного технического университета. Т. 17. №3. – Воронеж, 2021. – С. 32 – 45.