УДК 517.584;524.7

Студ. П.С. Дзибук
Науч. рук. доц. Л.Д. Яроцкая (кафедра высшей математики, БГТУ)

ПРИМЕНЕНИЕ ФУНКЦИЙ БЕССЕЛЯ К ЗАДАЧЕ ПОСТРОЕНИЯ КРИВЫХ ВРАЩЕНИЯ КОСМИЧЕСКИХ ОБЪЕКТОВ

Одна из нерешенных в общем виде и вызывающая интерес задача современной астрофизики – задача построения кривой вращения космических объектов. Сложность задачи обусловлена асимметричностью плотности распределения вещества, непостоянной вязкостью и другими факторами, затрудняющими наблюдение. Отметим, что в классической механике задача названа в честь Иоганна Кеплера.

Аналитическое решение краевой задачи в цилиндрических координатах, полученное для дисковых галактик в работе [1] методом разделения переменных, выражается через функции Бесселя первого рода. В работе [2] кривые вращения космических объектов в идеальной среде на основании гидродинамического подхода описаны цилиндрическими функциями $J_1(\beta r)$, где r – расстояние от объекта до оси вращения системы, а β – параметр, зависящий от угловых скоростей и скорости поступательного движения системы. Показано, что случай $\beta >> 1$ соответствует кривым вращения планет и лун и в пределе совпадает с законами Кеплера. Если $\beta < 1$, то имеем кривую вращения галактики.

Функция Бесселя первого рода порядка n для любых значений z определяется как сумма ряда [3]

$$J_n(z) = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!(n+k)!}\left(\frac{z}{2}\right)^{n+2k}, \quad |z| < \infty.$$

Данные функции названы по имени немецкого астронома Фридриха Бесселя, который в работе 1824 года, изучая движение планет вокруг солнца, вывел рекуррентные соотношения, получил для целых порядков интегральные представления, составил первые таблицы. Простейшими функциями рассматриваемого класса являются функции $J_0(z)$ и $J_1(z)$. Отметим, что с законом Кеплера согласуется следующая асимптотическая оценка функции $J_1(z)$ для больших $|z|$:

$$J_1(z) \sim \sqrt{\frac{2}{\pi z}} \cos\left(z - \frac{3\pi}{4}\right).$$

ЛИТЕРАТУРА

1. Меса А., Липовка А.А. Моделирование кривой вращения дисковых галактик // Астрофизический бюллетень. – 2022, Т. 77, №2. – С. 136–146.

2. Kudykina T. Rotation Curves of the Cosmic Objects and Attractive Force in the Universe // Mediterranean Journal of Physics. – 2016, 1(1). – P. 32-36.

3. Бейтмен Г., Эрдейи А. Высшие трансцендентные функции. Функции Бесселя, функции параболического цилиндра, ортогональные многочлены. – М., «Наука». 1974. – 296 с.

УДК 511.2/.3

Студ. Н.М. Гулевич, Т.И. Гулешов
Науч. рук. доц. Е.И. Ловенецкая (кафедра высшей математики, БГТУ)

ФАКТОРИЗАЦИЯ НАТУРАЛЬНЫХ ЧИСЕЛ

Факторизация натуральных чисел – одна из ключевых задач теории чисел, заключающаяся в разложении числа на простые множители. Эта задача имеет важное значение в криптографии, в частности в алгоритме RSA, где безопасность основана на вычислительной сложности факторизации больших чисел. Алгоритм RSA использует пару ключей: открытый для шифрования и закрытый для расшифровки, причем нахождение закрытого ключа по открытому требует факторизации произведения двух больших простых чисел.

В данной работе рассмотрены три алгоритма факторизации: метод перебора делителей, алгоритм Ферма и ρ-метод Полларда. Метод перебора делителей проверяет все возможные делители до квадратного корня числа. Алгоритм Ферма использует представление числа как разности квадратов. Метод Полларда основан на вероятностном подходе, эффективность зависит от выбранной функции. Были реализованы указанные алгоритмы, проведено сравнение их производительности на числах разной величины и структуры. Метод перебора делителей наиболее эффективен для относительно небольших чисел. Алгоритм Ферма эффективен, когда число можно представить как разность квадратов двух чисел, близких по значению. ρ-метод Полларда, будучи вероятностным, показывает высокую эффективность для чисел с умеренно большими множителями. Изучались также некоторые модификации алгоритмов: метод Ферма получил обратную реализацию, метод Полларда – множество реализаций с различными внутренними функциями. Результатом работы является программа на языке Python, позволяющая выполнять факторизацию натуральных чисел с использованием алгоритма перебора (до 10 000), далее применяющая алгоритмы Ферма и Полларда параллельно, что позволяет пользоваться преимуществами всех алгоритмов для поиска делителей одновременно.

ЛИТЕРАТУРА

1. Кнут, Д.Э. Искусство программирования. Том 2: Получисленные алгоритмы / Д.Э. Кнут. – М.: Вильямс, 2018.